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

RECOMENDAÇÕES PARA A CONSTRUÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD) NO PROCESSO DE ENGENHARIA DE REQUISITOS

LUCAS MONTEIRO SILVA

GOIÂNIA
2022

LUCAS MONTEIRO SILVA

RECOMENDAÇÕES PARA A CONSTRUÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD) NO PROCESSO DE ENGENHARIA DE REQUISITOS

Projeto de pesquisa apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para aprovação da disciplina de Trabalho de Conclusão de Curso II– CMP1072 – A27.

Orientador(a): Prof.ª. Ma. Adriana Silveira de Souza.

GOIÂNIA

2022

LUCAS MONTEIRO SILVA

RECOMENDAÇÕES PARA A CONSTRUÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD) NO PROCESSO DE ENGENHARIA DE REQUISITOS

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Engenharia da Computação, e aprovado em sua forma final pela escola Politécnica, da Pontifícia Universidade Católica de Goiás em _____/_____/_____.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientadora: Prof.ª. Ma. Adriana Silveira de Souza

_____

Prof. Me. Joriver Rodrigues Canedo

_____

Prof. Ma. Solange da Silva

GOIÂNIA

2022

Dedico este trabalho a minha mãe,
meu pai, meus irmãos, meus maiores exemplos de inspiração.

AGRADECIMENTOS

A Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Aos meus pais e irmãos, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

A minha orientadora acadêmica, professora Adriana Silveira de Souza, pelo apoio e confiança no desenvolvimento deste trabalho.

Sou grato a todo o corpo docente, à direção e administração desta universidade.
Sou grato a todos que participaram desta banca.

RESUMO

O presente trabalho tem como objetivo apresentar um estudo sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) que é um documento fundamental na prevenção de riscos a privacidade dos dados pessoais. Este trabalho vai apresentar recomendações para a construção de um RIPD em um processo de Engenharia de Requisitos, seguindo os padrões da Lei Geral de Proteção de Dados Pessoais (LGPD). A RIPD traz uma grande contribuição para o processo de engenharia de requisitos tendo em vista a prevenção e mitigação de riscos em todos os processos de tratamento de dados, reforçando a conformidade com os requisitos de segurança.

Palavra-chave: RIPD. Riscos. LGPD. Proteção de dados pessoais.

ABSTRACT

The present work aims to present a study on the Data Protection Impact Report (RIPD) which is a fundamental document in the prevention of risks to the privacy of personal data. This work will present recommendations for the construction of a RIPD in a Requirements Engineering process, following the standards of the General Law for the Protection of Personal Data (LGPD). RIPD makes a great contribution to the requirements engineering process with a view to preventing and mitigating risks in all data processing processes, reinforcing compliance with security requirements.

Keyword: RIPD. Risks General Data Protection Law (LGDP). Personal data protection.

LISTA DE FIGURAS

LISTA DE QUADRO

LISTA DE ABREVIATURAS E SIGLAS

AIP	Avaliação de Impacto à Privacidade ou *Privacy Impact Assessment*
ABNT	Associação Brasileira de Normas Técnicas ou *Brazilian Association of Technical Standards*
ANPD	Autoridade Nacional de Proteção de Dados ou *National Data Protection Authority*
BPMN	Notação de modelagem de processos de negócios ou *Business Process Modeling Notation*
DP	Dados Pessoais ou *Personal data*
ES	Engenharia de Software ou *Software Engineering*
GDPR	Regulamento Geral de Proteção de Dados ou *General Data Protection Regulation*
ISO	Organização Internacional de Normalização ou *International Organization for Standardization*
IEC	Comissão Eletrotécnica Internacional ou *International Electrotechnical Commission*
IDC	Corporação de Dados Internacional ou *International Data Corporation*
LGPD	Lei Geral de Proteção de Dados Pessoais ou *General Personal Data Protection Law*
NBR	Norma Brasileira ou *Brazilian Standard*
NFR	Requisito Não Funcional ou *Nonfunctional Requirement*
RG	Registro Geral ou *General Registry*
SRS	Especificação de Requisitos de Software ou *Software Requirements Specification*
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas ou *Brazilian Micro and Small Business Support Service*
UML	Linguagem de modelagem unificada ou *Unified modeling language*

SUMÁRIO

1. Introdução

Com o desenvolvimento da tecnologia da informação e intensificação dos fluxos de informação por meios digitais, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais.

Uma delas são as mídias sociais que transitam milhares de informações por sites e aplicativos que permitem conexão e interação entre os usuários. Também conhecidas como redes sociais, as mídias sociais mais populares atualmente são Facebook, Youtube, Instagram e WhatsApp.

A frase "dados são o novo petróleo", foi criada por Clive Humby, um matemático britânico especializado em dados. Humby (2006) afirma que o dado é muito valioso, mas para ter um melhor uso precisa ser bem refinado e analisado.

Um dado "bem trabalhado" permite que as empresas desenvolvam produtos personalizados para seus consumidores, criem soluções que atendam perfis únicos de clientes, entendam o comportamento de um determinado segmento da população. Assim possibilitando criar soluções inovadoras que atendam às necessidades, consigam diagnosticar e avaliar potenciais riscos antes que se concretizem.

As possibilidades são infinitas e trazem um universo de alternativas para a criação de um "futuro melhor" graças ao desenvolvimento tecnológico através do uso de dados.

Pode-se dizer que os dados são um patrimônio da empresa. Em muitos casos, eles são até mais importantes do que o próprio patrimônio físico da companhia. Por isso, a proteção desses dados é fundamental. (NÉGOCIO SEGURO, 2021)

Diante desse cenário, iniciou-se uma discussão global acerca de como evitar "abusos", por parte das empresas, na coleta e utilização desses dados. Como proposta de solução surgiu a ideia de regulamentação do uso de dados pessoais através de leis e regulamentos específicos em cada país, sendo que o Brasil um dos países que desenvolveu uma legislação específica com essa finalidade (NASCIMENTO, 2021).

Inspirado no movimento global de privacidade e proteção de dados, bem como em leis já existentes em outros países, como a *General Data Protection Regulation* (GDPR), em 14 de agosto de 2018 foi sancionada a Lei n º 13.709 ou Lei Geral de Proteção de Dados Pessoais (LGPD). (NASCIMENTO, 2021).

A Lei estabelece uma estrutura legal de direitos dos(as) titulares de dados pessoais. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais realizado pelo órgão ou entidade. (BRASIL, 2021).

A LGPD tem o intuito de proteger e minimizar os impactos causados pelos tratamentos de dados pessoais. Assim, a própria Lei determinou, no art. 5º, inciso XVII, a elaboração do relatório de impacto de proteção de dados pessoais (RIPD).

O RIPD é documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

O RIPD deve ser elaborado, preferencialmente, na fase inicial do programa ou projeto que incluirá o tratamento de dados. Isto é, deve ele ser realizado desde a fase de concepção de um novo projeto, processo, produto ou serviço.

Esse tema foi escolhido por ser uma prática que toda a organização que trabalha com a criação de um software, processo ou serviço que utiliza dados pessoais deve se preocupar.

Toda a organização desenvolvedora de software, quando vai construir um novo produto, pela LGPD, tem de relatar como os dados pessoais serão tratados. Em especial, na etapa de engenharia de requisitos tem-se início a construção da RIPD e devem dar início a esse relatório.

O objetivo principal desse trabalho é identificar em que aspectos do processo engenharia de requisitos impactam na construção do RIPD.

Este trabalho está organizado da seguinte forma: No capítulo 2 apresenta uma abordagem sobre os processos de engenharia de requisitos. O capítulo 3 uma análise sobre o relatório de impacto a proteção de dados pessoais. O capítulo 4 exibe recomendações para a construção relatório de impacto a proteção de dados pessoais para o processo de engenharia de requisitos. E capítulo 5, demonstra as principais conclusões e sugestões de trabalhos futuros.

2. Objetivos

2.1. Objetivo geral

- Desenvolver recomendações para a construção de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em um processo de Engenharia de Requisitos, seguindo os padrões da Lei Geral de Proteção de Dados Pessoais (LGPD).

2.2. Objetivos específicos

- Analisar processos de Engenharia de Requisitos que trate dados pessoais.
- Analisar processos de negócios.
- Avaliar impactos e riscos no tratamento de dados.
- Analisar modelos de Relatórios de Impacto a Proteção de Dados Pessoais (RIPD).

3. Método

A natureza dessa pesquisa e um resumo de assunto, pois busca orientar e entender como elaborar e implementar recomendações para a construção da RIPD em um processo de Engenharia de Requisitos e está fortemente ligada a computação. O resumo de assunto propõe-se a organizar uma área de conhecimento, no qual indica sua evolução histórica e seu estado da arte, ou seja, adequado para os cursos de graduação (WAZLAWICK, 2014).

Segundo seus objetivos esta pesquisa é explicativa, pois busca alcançar dados consistentes para implementar um RIPD em um processo de Engenharia de Requisitos, seguindo os padrões e as necessidades da Lei Geral de Proteção de Dados (LGPD) de acordo com a lei nº 13.709, de forma pratica, segura e econômica, visando impactos na segurança dos dados e em sua aplicação. (GERHARDT, 2009).

A pesquisa bibliográfica envolve o estudo de artigos, teses, livros e outras publicações que geralmente são fornecidos e indexados por editoras. A pesquisa bibliográfica é qualquer trabalho científico, mas não produz nenhum novo conhecimento, ela apenas ajuda o pesquisador a ter informações relevantes e públicas que ele ainda não possuía (WAZLAWICK, 2014).

E segundo seus procedimentos técnicos, esta pesquisa é bibliográfica, quantitativa e documental, pois pretende propor recomendações para construção da RIPD no processo de Engenharia de Requisitos, levando em consideração os processos de tratamento de dados pessoais. Analisando documentos e avaliando potenciais impactos na fase inicial do tratamento de dados. Wazlawick (2014) sugere que a pesquisa bibliográfica deve seguir os seguintes passos:

a) Listar os títulos de periódicos e eventos relevantes para o tema de pesquisa e os títulos de periódicos gerais em computação que eventualmente possam ter algum artigo na área do tema de pesquisa.

b) Obter a lista e todos os artigos publicados nos últimos cinco anos (ou mais) nesses veículos.

c) Selecionar desta lista aqueles títulos que tenham relação com o tema de pesquisa.

d) Ler o abstract desses artigos e, em função da leitura, classificá-los como relevância “alta”, “média” ou “baixa”.

e) Ler artigos de alta relevância e fazer fichas de leitura anotando os principais conceitos e ideias aprendidos. Anotar também títulos de outros artigos possivelmente mencionados na bibliografia de cada artigo (mesmo que com mais de cinco anos) e que pareçam relevantes para o trabalho de pesquisa. Incluir esses artigos na lista dos que devem ser lidos (inicialmente o abstract e, se for relevante, o artigo todo).

f) Dependendo do caso, ler também os artigos de relevância média e baixa, mas iniciando sempre pelos de alta relevância.

g) Se já tem material suficiente para elaborar uma ideia de pesquisa consistente.

h) Se precisa expandir a pesquisa examinando artigos mais antigos (expandindo o passo b) ou periódicos menos relevantes (expandindo o passo a).

Para Gil (2017) a pesquisa documental é utilizada em praticamente todas as ciências sociais e constitui um dos delineamentos mais importantes no campo da História e da Economia. Como delineamento, apresenta muitos pontos de semelhança com a pesquisa bibliográfica, posto que nas duas modalidades utilizam-se dados já existentes. A principal diferença está na natureza das fontes.

A pesquisa bibliográfica fundamenta-se em material elaborado por autores com o propósito específico de ser lido por públicos específicos. Já a pesquisa documental vale-se de toda sorte de documentos, elaborados com finalidades diversas, tais como assentamento, autorização, comunicação etc. Mas há fontes que ora são consideradas bibliográficas, ora documentais. Por exemplo, relatos de pesquisas, relatórios e boletins e jornais de empresas, atos jurídicos, compilações estatísticas etc. Assim, recomenda-se que seja considerada fonte documental quando o material consultado é interno à organização, e fonte bibliográfica quando for obtido em bibliotecas ou bases de dados.

A pesquisa quantitativa é um método que busca mensurar os dados adquiridos e analisá-los de forma estatística para verificar a validade de uma hipótese. Assim, como seu nome sugere, ela tem como finalidade definir a quantidade de algo. (JR CONSULTORIA, 2021)

Através desta metodologia, as informações obtidas são traduzidas em números e porcentagens. Dessa forma, é possível medir as preferências do cliente, a importância de um produto, dentre outras alternativas.

4. Processo de engenharia de requisitos

O processo engenharia de requisitos é conhecido por definir, documentar e especificar o que um software deve fazer. Os requisitos refletem as necessidades dos clientes para um sistema que serve a uma finalidade determinada, como controlar um dispositivo ou encontrar informações.

De acordo com Nardi e Falbo (2006) obter os requisitos corretos em um projeto de software é a parte mais importante e difícil na construção de software. A deficiência no tratamento de requisitos tem sido apontada como a principal causa de fracassos de projetos de software.

A engenharia de requisitos fornece atividades, técnicas e ferramentas apropriadas para entender o que o cliente deseja. Para isso analisa as necessidades, avalia a viabilidade, negocia uma solução razoável, especifica a solução sem ambiguidades, validando a especificação e gerenciando as necessidades à medida que são transformadas em um software. (PRESSMAN, 2011).

Esse capítulo apresenta o processo de engenharia de requisitos com a finalidade de fornecer uma perspectiva de como esse processo pode influenciar a construção do relatório de impacto. Este processo é composto por cinco atividades: Levantamento de requisitos, análise e modelagem, especificação, verificação e validação e gerência de requisitos.

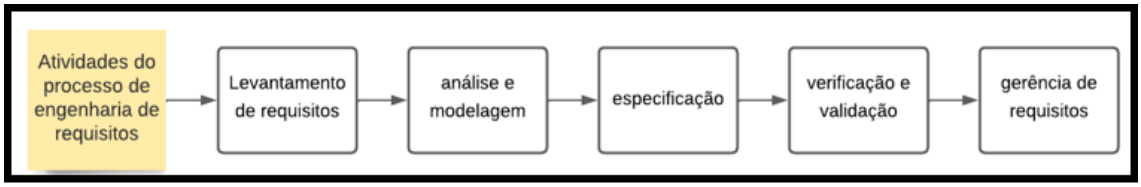
As atividades são utilizadas para se gerar uma documentação formal de requisitos. Essa documentação será a base para a construção subsequente do produto.

Os requisitos de software são sentenças que expressam as necessidades dos clientes e que condicionam a qualidade do software, ou especificações de serviços que o sistema deve prover, restrições no sistema e conhecimentos necessários para desenvolvê-lo.

Considerando que os requisitos são o foco do processo da engenharia de requisitos (ER), é interessante que se tenha uma compreensão clara do que vem a ser um requisito e de como ele se relaciona com outros elementos do processo de software. (NARDI; FALBO, 2006).

A Figura 1 mostra as atividades que compõem a engenharia de requisitos.

Figura 1 – Atividades do processo de engenharia de requisitos



Fonte: Autoria própria.

A seguir são apresentadas as atividades que compõem o processo de engenharia de requisitos.

4.1 Levantamento de requisitos

O levantamento de requisitos é um uma das partes mais importantes do processo que resultará no desenvolvimento de um sistema. Consiste no entendimento daquilo que o cliente deseja ou o que o cliente acredita que precisa, constituído pelas regras do negócio ou processos de negócio. (VERÍSSIMO, 2022).

Segundo Almeida (2018), o processo de negócios é o conjunto de atividades ou tarefas que são estruturadas e giram em torno da produção de um resultado de valor para o cliente.

O processo de negócio implementa a entrega de um serviço ou desenvolvimento de um produto. Ele mostra o que deve ser realizado, como deve ser realizado e quem é o responsável.

Por exemplo se um cliente compra um produto de uma loja virtual, automaticamente gera a necessidade de entrega, isso é um processo de negócio. Ouve uma necessidade e gerou um processo de negócio entre venda e entrega.

Deste modo, o processo de negócio determina como o trabalho será feito na organização e traz a sequência lógica das atividades. É importante ressaltar que:

- Um processo de negócio envolve pessoas, equipamentos, procedimentos e informações.
- O processo de negócio deve agregar valor ao cliente ou agregar valor a outros processos.
- Todo processo de negócio possui uma entrada (*input*) e pelo menos uma saída (*output*).

- No processo de negócio, os insumos (materiais, conhecimento etc.) são transformados em resultados (produtos e serviços).

Muitas são as técnicas para que os requisitos sejam levantados. Elas podem incluir entrevistas e questionários entre os interessados, observação do ambiente de trabalho em que ele será aplicado, simulações junto aos usuários finais etc. (MONITORA, 2020).

Na entrevista a equipe de engenharia de requisitos se reúne com um ou mais envolvidos para entender melhor suas necessidades, motivações, cultura de trabalho e questões do processo de negócio. Requisitos surgem a partir das respostas a essas perguntas.

Um questionário de requisitos é uma lista de perguntas sobre os requisitos do projeto. Normalmente, as perguntas são organizadas (ou requisito de negócios ou objetivo do projeto). Essencialmente, cada requisito de alto nível do seu documento de escopo deve ter uma lista de perguntas para refinar ainda mais sua compreensão. (FERNANDA, 2018).

Investir tempo em um questionário de requisitos ajudará a garantir que você não apenas reunirá requisitos, mas também que você descubra requisitos não sonhados.

Observar o ambiente de trabalho é uma forma que a equipe de engenharia de requisitos se insere no ambiente de trabalho, observa e anota as tarefas reais que o sistema será utilizado.

Utilizando-se essa técnica, é possível capturar o que realmente é feito e qual tipo de suporte computacional é realmente necessário. Ajuda a confirmar ou refutar informações obtidas com outras técnicas e ajuda a identificar tarefas que podem ser automatizadas e que não foram identificadas pelos interessados.

A simulação é uma forma de validar requisitos, simulando um protótipo para o usuário final.

Um protótipo é uma versão preliminar do sistema, muitas vezes não operacional e descartável, que é apresentada ao usuário para capturar informações específicas sobre seus requisitos de informação, observar reações iniciais e obter sugestões, inovações e informações para estabelecer prioridades e redirecionar planos.

4.2 Análise de requisitos

De acordo com Monitora (2020), depois que os requisitos são levantados, eles precisam ser analisados para se ter clareza sobre como eles serão utilizados na modelagem do software.

Pode afirmar que a análise de requisitos consiste em uma modelagem conceitual do software, em que meios de análise são desenvolvidos para se obter uma melhor compreensão e especificação do sistema que será criado.

As representações da modelagem servem para melhor demonstrar os processos da organização, os problemas que precisam ser resolvidos e, com base nisso, os melhores meios para o desenvolvimento do sistema.

- **Requisitos Funcionais**

Os requisitos funcionais de um sistema descrevem o que ele deve fazer. Eles dependem do tipo de software a ser desenvolvido, de quem são seus possíveis usuários e da abordagem geral adotada pela organização ao escrever os requisitos. Quando expressos como requisitos de usuário, os requisitos funcionais são normalmente descritos de forma abstrata, para serem compreendidos pelos usuários do sistema. No entanto, requisitos de sistema funcionais mais específicos descrevem em detalhes as funções do sistema, suas entradas e saídas, exceções etc. (SOMMERVILLE, 2011).

- **Requisitos não funcionais**

Segundo PRESSMAN (2016), um requisito não funcional (NFR, *nonfunctional requirement*) pode ser descrito como um atributo de qualidade, de desempenho, de segurança ou como uma restrição geral em um sistema.

Os requisitos não funcionais têm origem nas necessidades dos usuários, em restrições de orçamento, em políticas organizacionais, em necessidades de interoperabilidade com outros sistemas de software ou hardware ou em fatores externos como regulamentos e legislações (SOMMERVILLE, 2007).

Um exemplo é a definição sobre qual plataforma o software deverá rodar. Trata-se de um requisito não funcional, pois não existe uma regra de negócio nessa definição. Entretanto, é um requisito necessário para fazer outras definições para o desenvolvimento do sistema, como a escolha da linguagem de programação, do banco de dados que será utilizado etc. (NOLETO, 2020).

- **Requisitos de segurança**

Segundo Braz (2012) os requisitos de segurança de software são o conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização.

De acordo com a ISO/IEC 25010:2011 os requisitos de segurança representam o grau em que um produto ou sistema protege as informações e os dados para que as pessoas ou outros produtos ou sistemas tenham o grau de acesso aos dados adequado aos seus tipos.

- **Confidencialidade**

Grau para o qual um produto ou sistema garante que os dados sejam acessíveis somente aquelas pessoas autorizadas a terem acesso.

Sem a confidencialidade, as empresas ficam vulneráveis a ciberataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros. Por exemplo, alguém pode deixar de proteger sua senha, seja para uma estação de trabalho ou para fazer login em uma área restrita. Os usuários podem compartilhar suas credenciais com outra pessoa ou permitir que alguém veja seu login ao inseri-lo. (SERVICE, 2021).

- **Integridade**

Grau para o qual um sistema, produto ou componente impede o acesso não autorizado ou a modificação de programas de computador ou dados.

O princípio de integridade refere-se à manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas. Ou seja, a informação mantém sua origem e ela não pode ser alterada, assim somente pessoas autorizadas poderão acessar e modificar os dados do sistema.

Existem diversos fatores que podem afetar a integridade dos dados armazenados. Os mais comuns são:

- Erro humano: quando os usuários inserem informações incorretas, duplicam ou excluem dados e, ainda, não seguem os protocolos estipulados pela empresa;
- Erros de transferência: ocorre quando os dados não são transferidos com êxito de um banco para o outro;
- Bugs e vírus: malwares e outros programas mal-intencionados podem invadir um computador e alterar, excluir ou roubar dados;

- Hardware comprometido: falhas súbitas no computador ou servidor e problemas de funcionamento de algum dispositivo são exemplos que podem comprometer o hardware.

- **Não repúdio**

Grau em que ações ou eventos podem ser provados como tendo ocorrido, de modo que os eventos ou ações não possam ser rejeitadas ou recusadas mais tarde.

O não repúdio é importante no comércio eletrônico para prevenir que as partes integrantes de uma transação venham a contestar ou negar uma transação após sua realização. O primeiro objetivo de um sistema de não repúdio é provar quem foi o autor de determinada ação e manter as necessárias evidências de tal informação para resolver eventuais disputas ou auditorias. (VERAS, 2018).

- **Prestação de contas**

Grau para o qual as ações de uma entidade podem ser rastreadas exclusivamente para a entidade.

- **Autenticidade**

Grau em que a identidade de um sujeito ou recurso pode ser provada como sendo aquela reivindicada.

Segundo Pereira (2019) esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação.

Todos esses métodos são importantes para garantir a segurança das informações corporativas das possíveis ameaças, que podem ter origens tanto externas quanto internas. Elas podem ser uma pessoa, um evento ou uma ideia capaz de causar danos ao sistema.

As ameaças externas são tentativas de ataque ou desvio de informações vindas de fora da empresa, normalmente originadas por pessoas com a intenção de prejudicar a corporação.

As internas podem ser causadas por colaboradores de forma intencional. Essas ameaças podem causar pequenos incidentes e até prejuízos graves, por isso também devem ser levados em conta na hora do planejamento dos processos de segurança da

empresa. O incidente é uma ocorrência inesperada mais branda, que não causa consequência para nenhuma das partes, nem para o trabalhador, nem para a empresa.

É importante que o Profissional de Sistemas de Informação (SI) mantenha sempre em alta a importância da segurança dos dados corporativos entre todos os usuários. Há diversas formas de manter a proteção da informação e não apenas criando mecanismos que realizam esse trabalho, mas desenvolver projetos que envolvam os usuários para conscientizá-los.

4.3 Modelagem

A modelagem é uma das principais atividades que levam à implementação de um bom software. Construímos modelos para comunicar a estrutura e o comportamento desejados do sistema, visualizar e controlar a arquitetura do mesmo e compreender melhor o sistema que estamos elaborando. Os modelos expressam os requisitos descritos no documento de requisitos, possibilitando um maior entendimento do domínio da aplicação, servindo para determinar se a especificação está completa, consistente e precisa, fornecendo uma transição para a fase de projeto. (TURINE; MASIERO, 1996).

Nesta etapa pode-se criar modelos de protótipo, UML, BPMN e diagrama de casos de uso para verificar e validar os requisitos levantados e analisados anteriormente.

Um protótipo é um modelo simulado do sistema que pode ser usado desde as primeiras etapas do desenvolvimento para ajudar a elucidar e validar requisitos de um sistema.

O uso de protótipos possibilita mostrar a interface, o processo de interação com funcionalidades e botões, de uma maneira fácil de se compreender. Por meio dessa informação concreta o usuário poderá não apenas entender, mas também contribuir com segurança, expressando o que gostou ou não, quais são as funcionalidades fáceis e eficazes de se utilizar etc. (DIAS, 2019).

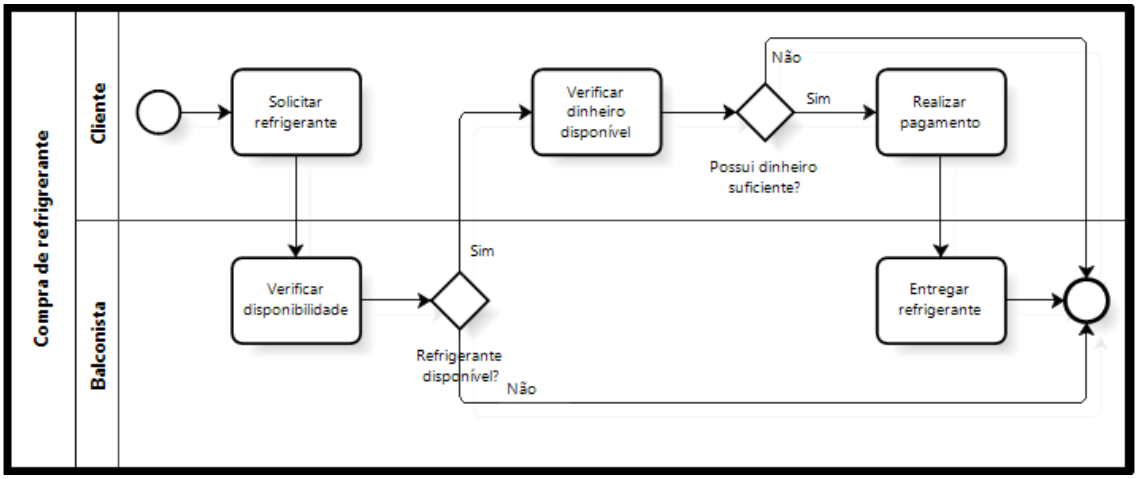
O protótipo evita que suposições ruins avancem no desenvolvimento do produto, diminuindo o custo da correção, mas também traz ideias mais refinadas, não concebidas inicialmente.

A UML é a linguagem mais utilizada quando o assunto é modelagem de software. Definida de forma simples como um conjunto de diagramas que representam elementos, características e comportamentos de um software. (DEVMEDIA, 2022).

BPMN (*Business Process Model and Notation*) é uma notação gráfica que tem por objetivo prover uma gramática de símbolos para mapear, de maneira padrão, todos os processos de negócio de uma organização.

A BPMN é utilizada para facilitar o entendimento desses processos e visualizar seu início, meio e fim, desenhando o fluxo do processo etapa a etapa. A Figura 2 apresenta um exemplo de processo de negócio modelado em BPMN.

Figura 2 - Exemplo de um processo mapeado utilizando BPMN

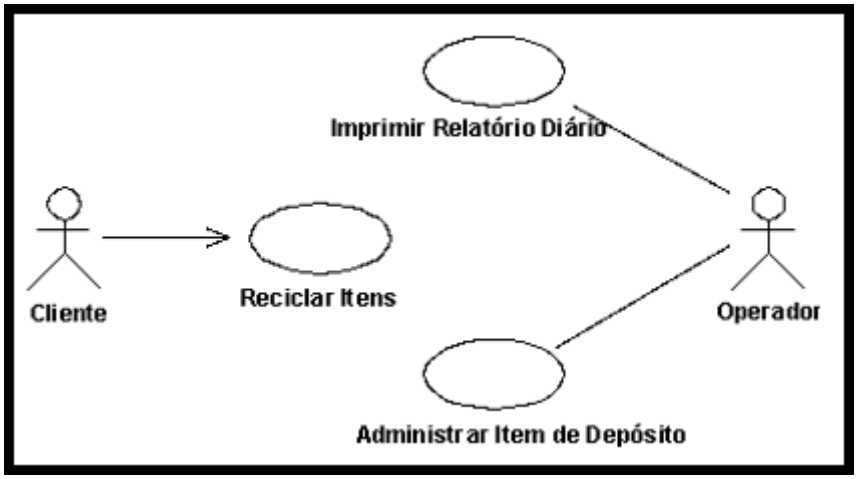


Fonte: Sganderla (2012)

Em BPMN, um processo de negócio é representado através do encadeamento de eventos e atividades, ligados através de conectores que demonstram a sequência em que eles são realizados. Além de eventos e atividades, outros elementos de controle de fluxo podem ser utilizados na modelagem para permitir a criação ou unificação de fluxos paralelos que ocorram no decorrer de um mesmo processo de negócio. (SGANDERLA, 2012).

Um modelo de caso de uso é um modelo que descreve como diferentes tipos de usuários interagem com o sistema para resolver um problema. A figura abaixo representa um modelo de caso de uso.

Figura 3 - Modelo de caso de uso



Fonte: UFPE (2006)

A Figura 3 mostra uma parte de um modelo de casos de uso para o Sistema da Máquina de Reciclagem. É representado por uma sequência de ações executadas pelo sistema que geram um resultado de valor observável para um ator em particular.

4.4 Especificação

Uma especificação de requisitos de software (*software requirements specification*, SRS) é um documento criado quando uma descrição detalhada de todos os aspectos do software a ser construído deve ser especificada antes de o projeto começar. (PRESSMAN, 2011).

Silva (2022) define a especificação como uma descrição sistemática e abstrata do que o software deve fazer a partir daquilo que foi analisado anteriormente. Ela apresenta a solução de como os problemas levantados na análise devem ser resolvidos pelo software em desenvolvimento.

Um SRS geralmente contém requisitos funcionais e não funcionais. Os requisitos funcionais descrevem a função de um sistema de software e seus componentes. Enquanto os requisitos não funcionais descrevem as características de desempenho do sistema de software e seus componentes como segurança ou serviço disponibilidade. Uma especificação de requisito de software fornece uma descrição abrangente de um produto de software a ser desenvolvido. (VISURE, 2022).

4.5 Verificação e Validação

Validação de software ou, mais genericamente, verificação e validação, tem a intenção de mostrar que um software se adequa a suas especificações ao mesmo tempo que satisfaz as especificações do cliente do sistema. (SOMMERVILLE, 2011).

O objetivo da verificação é analisar se o software atende aos requisitos funcionais e não funcionais. O objetivo da validação é garantir que o software atenda às expectativas do cliente.

> Segundo Vazquez (2016) a validação de requisitos é um trabalho de garantia de qualidade na Engenharia de Requisitos que busca assegurar que todos os requisitos especificados estejam alinhados com os requisitos de negócio. Ou seja, procurar garantir que todas as necessidades de negócio das partes interessadas no escopo do projeto serão satisfeitas. (VAZQUEZ, 2016 p305).

O processo de verificação e validação é estabelecer a confiança de que o software é "adequado para o propósito" a ele destinado. Isso significa que o sistema deve atender os critérios estabelecidos especificados na fase anterior.

4.6 Gerência de requisitos

A gerência de requisitos é um modelo sistemático para encontrar, documentar, organizar e rastrear os requisitos variáveis de um sistema.

Durante o processo de desenvolvimento e operação de um sistema de software é natural o surgimento de novos requisitos e a necessidade de mudanças nos requisitos existentes. Este processo, também conhecido como evolução de sistemas, acontece como resultado de mudanças no meio ambiente onde o próprio sistema de software está inserido (LEHMAN, 1996).

Segundo Sommerville (1997), as principais atividades ligadas à gerência de requisitos são relacionadas a:

1. Gerenciar as mudanças em requisitos existentes (pertencentes a especificação);
2. Gerenciar o relacionamento entre os requisitos;
3. Gerenciar as dependências entre o documento de requisitos e outros documentos produzidos durante o desenvolvimento de software;

Para implementar uma gerência de requisitos eficaz é necessário, de antemão, definir um conjunto de políticas para gerenciar os requisitos. É necessário definir um

conjunto de objetivos para o processo de gerência. Estes objetivos devem ser claros e transmitidos para todos os integrantes da equipe. Todos os artefatos (documentos) produzidos durante o desenvolvimento do software devem tornar a gerência dos requisitos visível e transparente. Estes documentos devem ser gerados levando-se em contas padrões externos e corporativos, de modo a assegurar consistência e uniformidade das informações. Políticas bem definidas para a gerência de configuração, controle de mudanças e rastreabilidade e garantia da qualidade precisam ser colocadas em prática de modo a viabilizar um processo dinâmico e eficaz de gerência de requisitos.

Todos os processos da engenharia de requisitos devem estar em conformidade com a LGPD, levando em consideração os requisitos levantados, especificados e documentados, neles devem estar contidos os agentes envolvidos no tratamento de dados, políticas de segurança e os requisitos que descrevem a segurança.

5. Lei Geral de Proteção de Dados Pessoais (LGPD)

A LGPD estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. Ela foi inspirada na GDPR (*General Data Protection Regulation*), que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores. (SEBRAE, 2020).

Antes de mais nada, é preciso entender que a legislação se aplica no meio físico e eletrônico, mas que o assunto se tornou iminente em face da maior facilidade de captação de dados no meio eletrônico. (ALVES, 2021)

No Brasil, a lei entrou em vigor em 18 de setembro de 2020, representando um passo importante para o Brasil. Com isso, passamos a fazer parte de um grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos. Diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países. (SEBRAE, 2020).

Segundo Nascimento (2021) a lei regula o tratamento de dados pessoais, por pessoa jurídica ou por pessoa natural, com o objetivo de proteger os direitos fundamentais e a privacidade dos indivíduos. Dessa forma, ela traz uma transformação cultural e organizacional para as empresas, exigindo uma série de medidas e procedimentos para garantia de conformidade.

A LGPD exige que as empresas que tratam dados garantam um nível de segurança adequado ao risco envolvido em projetos e atividades específicos. Na qual podem cumprir esse requisito identificando primeiro o risco, antes de implementar o nível apropriado de medidas técnicas e organizacionais para mitigá-lo. (ALVES, 2021).

Esta lei dispõe do tratamento de três tipos de dados, que são muito importantes. O dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável, ou seja, são as informações básicas de um determinado individuo: Nome e sobrenome, data e local de nascimento, Registro Geral (RG), Cadastro de Pessoas Físicas (CPF), retrato em fotografia, endereço residencial, endereço de e-mail, número de cartão bancário, renda, histórico de pagamentos, hábitos de consumo, dados de localização, como por exemplo, a função de dados de localização no celular, endereço de protocolo de internet (IP), testemunhos de conexão (*cookies*), número de telefone.

Da mesma forma, fragmentos de informação que, juntos, permitam identificar uma pessoa física também são considerados dados pessoais.

Dentre os dados pessoais, há aqueles que exigem maior atenção no tratamento, aqueles relacionados a crianças e adolescentes, e os sensíveis, que são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

Quando o dado corresponder a menores de idade, é imprescindível obter o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal e se limitar a pedir apenas o conteúdo estritamente necessário, sem repasse a terceiros. (ALVES, 2021).

Sobre os dados sensíveis, o tratamento depende do consentimento explícito do(a) titular dos dados e para um fim definido. De acordo com Brasil (2021) caso o titular dos dados ou seu responsável não dê o consentimento, o tratamento poderá ser realizado nas hipóteses em que for indispensável:

- A empresa controladora cumprir alguma obrigação disposta em lei ou regulação;
- Execução pela administração pública de políticas públicas previstas em leis ou regulamentos;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiros.

- Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Os dados anonimizados já se difere um pouco em relação aos anteriores, são aqueles que não permitem a identificação, direta ou indireta, de seu titular e, portanto, estão fora do escopo de proteção da LGPD. Contudo se o processo de anonimização de dados puder ser revertido, a lei será sim aplicável.

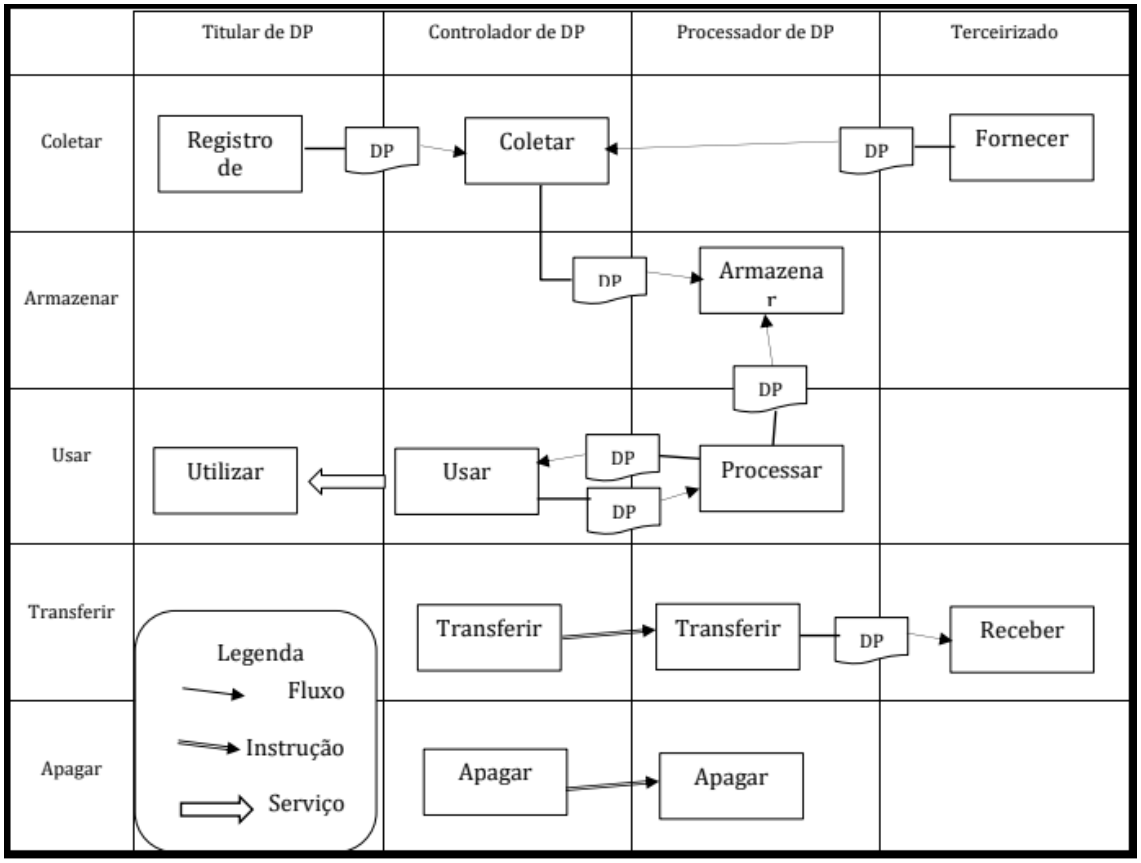
O tratamento de dados pessoais na LGPD são todas as operações realizadas com informações de pessoas naturais, inclusive nos meios digitais, por outras pessoas naturais ou pessoas jurídicas, tanto de direito privado quanto de direito público.

Mas para saber tudo sobre o que é tratamento de dados, é importante compreender quem é o "dono" desses dados. O titular de dados "é toda pessoa natural a quem se referem os dados que são objeto de tratamento".

Assim, compreende-se como atividades pertinentes ao tratamento dessas informações:

- Coleta: incluindo coleta, produção e recepção;
- Retenção: armazenamento e arquivamento;
- Processamento: utilização, classificação, reprodução, controle, avaliação, modificação e extração;
- Compartilhamento: comunicação, distribuição, transmissão, difusão e transferência;
- Eliminação: finalização do tratamento de dados.

Figura 4 – Diagrama de Fluxo do tratamento de DP



Fonte: ABNT NBR ISO/IEC 29134, 2020. 18

A Figura 4 mostra um exemplo de acordo com a ABNT NBR ISO/IEC 29134, de como o fluxo de informações de DP ou dados pessoais pode ser visualizado, em um tratamento de dados pessoais. O seu uso, pode incluir fluxos aprovados de compartilhamento para outras partes, a organização descreverá o fluxo de informações da maneira mais detalhada possível para ajudar a identificar os possíveis riscos de privacidade.

Para resguardar o tratamento dos dados pessoais dos titulares, a Lei traz em seu Capítulo III seus direitos e garantias. Esses direitos trazem o “empoderamento” ao titular sobre seus dados, por meio de uma série de garantias que buscam resguardar o livre acesso e decisão sobre os dados pessoais.

Além disso, a lei deixa clara que os dados pertencem ao indivíduo, e não à empresa que controla ou opera esses dados.

Conforme o art. 18 da LGPD, ao(à) titular estão garantidos os direitos de (BRASIL, 2021):

- Confirmação da existência de tratamento;

- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da Autoridade Nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do(a) titular, exceto nas hipóteses previstas no art. 16 da Lei;
- Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre consequências da negativa;
- Revogação do consentimento.

Para que o controle dos tratamentos seja feito de forma adequada, as empresas precisam contar com a figura do controlador e o operador. Os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado.

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais (BRASIL, 2021).

O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada.

Ou seja, o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador (BRASIL, 2021).

Com o objetivo de criar um canal de comunicação entre o controlador, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados, bem como um responsável direto pelo tema da privacidade e proteção de dados pessoais, a LGPD criou a figura do Encarregado, o qual terá como atividades:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;

- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A fiscalização e a regulação da LGPD ficarão a cargo da ANPD. Essas são tarefas essenciais para que a autoridade nacional atue como um órgão a serviço do cidadão. A autoridade será ainda um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões, denúncias ligadas à LGPD para apuração. (SERPRO, 2020).

Também tem a função de informar e fazer com que a população tenha conhecimento das políticas de proteção aos dados, das práticas e dos direitos sobre os dados, bem como estimular o entendimento das normas pelas empresas que fazem uso dos dados e informações pessoais. (ALVES, 2021).

Contudo, esta lei não se aplica quando se trata da coleta de dados realizada por pessoa natural para fins particulares. Também não se aplica a fins exclusivos, como (BRASIL, 2018):

- Jornalísticos e artísticos;
- Segurança pública;
- Defesa nacional;
- Segurança do Estado;
- Investigação e repressão de infrações penais;
- Particulares sem fins econômicos;
- Dados de fora do Brasil e que não sejam objeto de transferência internacional.

A LGPD está em vigor desde o final de 2020, entretanto, as sanções administrativas entraram em vigor em 01 de agosto de 2021. Os artigos 52, 53 e 54 da lei são os que tratam destas sanções, sendo assim, os que passam a valer integralmente a partir de agora. (BRASIL, 2021).

A aplicação das sanções irá depender de cada caso, pois será validado se a empresa em questão tem uma política de boas práticas e governança em relação ao vazamento de dados, se as medidas corretivas foram adotadas, além de levar em consideração a gravidade das infrações, condições econômicas e grau do dano, por exemplo.

A ANPD é o único órgão com autorização para aplicar as sanções administrativas da LGPD, embora já estejam agindo em parceria com outras entidades e órgãos da administração pública para exercer a fiscalização, como a Secretaria Nacional do

Consumidor – SENACON e o Conselho Administrativo de Defesa Econômica – CADE. (SOFTWALL, 2021).

Conforme o art. 52 da LGPD, a ANPD pode aplicar as seguintes sanções administrativas. (BRASIL, 2021):

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Multa diária, observado o limite total a que se refere o inciso II;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções administrativas mais graves, como proibição total do exercício das atividades da empresa, serão aplicadas apenas depois de penalizações menos intensas, como multas diárias ou divulgação pública da infração.

As sanções e multas só serão aplicadas depois do procedimento administrativo que permita uma ampla defesa e irá considerar os seguintes parâmetros e critérios de gravidade:

- A natureza das infrações e dos direitos pessoais afetados;
- A boa-fé;
- A vantagem auferida ou pretendida;
- A condição econômica do infrator;
- A reincidência;
- O grau do dano;

- A cooperação do infrator e adoção reiterada;
- A demonstração de mecanismos e procedimentos internos capazes de minimizar o dano e de medidas corretivas;
- A adoção de política de boas práticas e governança;
- A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

6. Relatório de Impacto a Proteção de Dados Pessoais (RIPD)

A LGPD (Lei Geral de Proteção de Dados) estabelece uma série de exigências e critérios às empresas que tratam dados pessoais. Dentre eles, está a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). (GETPRIVACY, 2022).

O Relatório de Impacto à Proteção de Dados Pessoais é um documento que visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018).

O RIPD deve ser elaborado, preferencialmente, na fase inicial do programa ou projeto que incluirá o tratamento de dados. Isto é, deve ele ser realizado desde a fase de concepção de um novo projeto, processo, produto ou serviço.

Existem muitas recomendações para a construção da RIPD e uma das mais importantes e a documentação da avaliação de impacto à privacidade (AIP).

Segundo a norma ISO/IEC 29134:2017, AIP é um instrumento para avaliar os potenciais impactos na privacidade de um processo, sistema de informação, programa, módulo de software, dispositivo ou outra iniciativa que trate dados pessoais (DP) e, em consulta às partes interessadas, para tomar ações necessárias para tratar risco à privacidade.

A AIP é mais que uma ferramenta: é um processo que começa nos estágios mais iniciais de uma iniciativa, quando ainda há oportunidades para influenciar seu resultado e, consequentemente, garantir *privacy by design*. É um processo que continua até, e mesmo após, o projeto ter sido entregue.

A descrição da AIP é a base para a construção da RIPD, pois fornece orientação que pode ser adaptada a uma ampla extensão de situações nas quais dados pessoais são tratados. Entretanto, em geral, uma AIP pode ser realizada para:

- identificar impactos à privacidade, riscos à privacidade e responsabilidades;

- fornecer entradas para a concepção de proteção de dados (às vezes chamada *privacy by design*);
- Revisar os riscos à privacidade de um novo sistema de informações e avaliar seu impacto e probabilidade;
- Fornece a base para a provisão de informações de privacidade aos titulares de dados pessoais em qualquer ação recomendada de mitigação de titulares de dados pessoais;
- Manter atualizações ou upgrades posteriores com funcionalidade adicional suscetível a impactar os dados pessoais que sejam manipulados;
- Compartilhar e mitigar riscos à privacidade com partes interessadas, ou fornecer evidências relacionadas ao *compliance*.

A AIP é um instrumento que contribui com evidências que suportam a conformidade com os requisitos legais aplicáveis. Pode fornecer evidências do cuidado devido adotado pela organização em caso de violação, não conformidade, reclamação etc.

De acordo com a Lei 13.709/2018 (LGPD), o Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais. (BRASIL, 2018). A lei define alguns critérios para a elaboração da RIPD são eles:

- Identificação dos agentes de tratamento e do encarregado
- Necessidade de elaborar o relatório
- Descrição do tratamento
- Natureza do tratamento
- Escopo do tratamento
- Contexto do tratamento
- Finalidade do tratamento
- Necessidade e proporcionalidade
- Identificação e avaliação de riscos
- Medidas para tratar os riscos
- Aprovação

Essas atividades descrevem todo processo de tratamento de dados pessoais previstos na LGPD.

6.1. Identificação dos agentes de tratamento e do encarregado

No capítulo 3 descrevemos alguns dos agentes de tratamento de dados pessoais são eles controlador, operador e o encarregado.

- O controlador é uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI). (BRASIL, 2018).
- O operador trabalha em conjunto ao controlador ele realiza o tratamento de dados pessoais em nome do controlador. (BRASIL, 2018).
- Já o encarregado é 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 (LGPD, art. 5º, VIII). (BRASIL, 2018).

6.2. Necessidade de elaborar o relatório

Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:

- para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º); (BRASIL, 2018).
- quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); (BRASIL, 2018).
- a qualquer momento sob determinação da ANPD (art. 38). (BRASIL, 2018).

Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD. (BRASIL, 2020).

A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade. (BRASIL, 2020).

Além dos casos específicos previstos pela LGPD no início desta seção 2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados; (BRASIL, 2018).
- rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 2º); (BRASIL, 2018).
- tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II); (BRASIL, 2018).
- processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20); (BRASIL, 2018).
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14); (BRASIL, 2018).
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42); (BRASIL, 2018).
- tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, 3º); (BRASIL, 2018).
- tratamento no interesse legítimo do controlador (LGPD, art. 10, 3º); (BRASIL, 2018).
- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.; (BRASIL, 2020).
- reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades. (BRASIL, 2020).

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

6.3. Descrição do tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento. (BRASIL, 2020).

A LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". (BRASIL, 2018).

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções. (BRASIL, 2020).

- **Natureza do tratamento**

A natureza representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso;
- medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

➢ **Escopo do tratamento**

O escopo representa a abrangência do tratamento de dados.

Nesse sentido, considerar destacar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são
- considerados dados pessoais sensíveis.
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento dedados pessoais é realizado em alta escala. (BRASIL, 2020).

➢ **Contexto do tratamento**

Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados. (BRASIL, 2020).

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;

- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais. (BRASIL, 2020).

➢ **Finalidade do tratamento**

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados. (BRASIL, 2020).

Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7 º e 11 da LGPD), no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiros;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiros;
- proteção do crédito;
- garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer

outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos. (BRASIL, 2018).

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD. (BRASIL, 2018).

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - Apoio e promoção de atividades do controlador;
>
> II - Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento. (BRASIL, 2018).

6.4. Necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III). (BRASIL, 2018).

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:

  - Esse tratamento de dados pessoais é indispensável;

  - Não há outra base legal possível de se utilizar para alcançar o mesmo propósito;

  - Esse processamento de fato auxilia no propósito almejado.
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
- Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
- Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Quais são as salvaguardas para as transferências internacionais de dados.

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais. (BRASIL, 2018).

6.5. Identificação e avaliação de riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018).

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. (BRASIL, 2020).

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. (BRASIL, 2020).

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

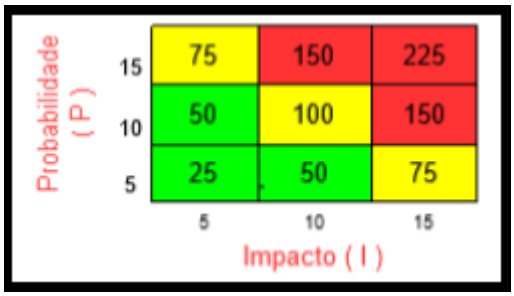
Quadro 1 - parâmetros escalares

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Fonte: BRASIL, 2020

A Figura 5 a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Figura 5 – Matriz de probabilidade x impacto



Fonte: BRASIL, 2020

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 5.

Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado;
- vermelho, indica risco alto.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016. (BRASIL, 2020).

Quadro 2 – Modelo para riscos referentes ao tratamento de dados pessoais

ID	**Risco referente ao tratamento de dados pessoais**	**P[1]**	**I[2]**	**Nível De Risco (PxI)[3]**
R01	Risco 1			
R02	Risco 2			
R0N	Risco N			

Fonte: BRASIL, 2020

Legenda: P – Probabilidade; I – Impacto.

Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais.

O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.

Quadro 3 – Modelo de riscos referente ao tratamento de dados pessoais

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Fonte: BRASIL, 2020

6.6. Medidas para tratar os riscos

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 (LGPD, art. 46.). (BRASIL, 2018).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.

A coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório. (BRASIL, 2020).

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis, até um risco de nível alto, devidos

aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais. (BRASIL, 2020).

Quadro 4 – Medidas para tratar os riscos

Risco	**Medida(s)**	**Efeito sobre o Risco**	**Risco Residual**			**Medida(s) Aprovada(s)**
			P	**I**	**Nível (P x I)**	
Risco 1	Medida 1; Medida 2; Medida N					
Risco 2	Medida 1; Medida 2; Medida N					
Risco N	Medida 1; Medida 2; Medida N					

Fonte: BRASIL, 2020

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior.

Quadro 5 – Exemplo de medidas para tratar os riscos

Risco	**Medida(s)**	**Efeito sobre o Risco**	**Risco Residual**			**Medida(s) Aprovada(s)**
			P	I	Nível (P x I)	
R01 Acesso não autorizado.	1. controle de acesso lógico 2. desenvolvimento seguro 3. segurança em redes	Reduzir	5	10	50	Sim
R04 Roubo.	1. controle de acesso lógico 2.controles criptográficos 3. proteção física e do ambiente	Reduzir	5	5	25	Sim
R06 Coleção excessiva.	1. Limitação da coleta.	Reduzir	5	10	50	Sim

Fonte: BRASIL, 2020

6.7. Aprovação

Esta seção visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa. (BRASIL, 2020).

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição. (BRASIL, 2020).

7. Recomendações para construção da RIPD para o processo de engenharia de requisitos

O tema em questão visa descrever os processos da RIPD com a proposta de implementação no processo de engenharia de requisitos levando em consideração que a AIP oportunidade para entender melhor os requisitos de privacidade e avaliar as atividades em relação a esses requisitos. (ISO/IEC 29134:2017).

Este capítulo apresenta recomendações para a construção da RIPD no processo de engenharia de requisitos. A seguir são apresentadas algumas recomendações de como o processo de engenharia de requisitos poderia apoiar a construção inicial do RIPD.

- **Levantamento de requisitos**

O levantamento de requisitos é a fase em que é descoberto os agentes "*stakeholders*" relacionados ao tratamento de dados pessoais. É nesta etapa que identificamos o controlador, operador e o encarregado do tratamento de dados pessoais.

Deve se identificar os processos de negócio que envolvam dados pessoais, considerando avaliar esses requisitos junto ao cliente, ver a necessidade de tratamento desses dados pessoais e se são realmente necessários para o sistema. Também deve se documentar os requisitos de segurança, consiste na definição das necessidades de proteção exigidas pelo software.

O primeiro ponto importante identificar um conjunto funcional de requisitos de segurança e privacidade, que deve ser usado como base para todo o software.

De um ponto de vista de segurança, ao documentar os requisitos busca-se garantir que as melhores práticas de segurança sejam cumpridas, mas não somente isso. É importante também observar a adesão a recomendações e ou exigências do mercado, bem como o cumprimento de exigências legais e normativas. Existem 5 conceitos básicos a serem abordados nos requisitos de segurança:

- Confidencialidade
- Integridade
- Não repúdio
- Prestação de contas
- Autenticidade

Definir e entender os requisitos de segurança é crucial para desenvolver um software de qualidade.

Os requisitos de segurança são a base para descrever a fase inicial da RIPD, onde identificamos as partes interessadas, o escopo, a natureza dos dados que deverá ser coletado e descrevemos no documento para avaliar impactos no sistema.

- **Análise de requisitos**

A análise de requisitos permite a criação de modelos de dados e de projeto, nos quais são definidas as restrições do software, como ele deve funcionar, como será a interface para o usuário. Pode -se analisar os modelos de dados e as restrições que afetam o sistema.

A modelagem de dados é uma atividade central de gerenciamento de dados. Afinal, ao fornecer uma representação visual de conjuntos de dados e seu contexto de negócios, ajuda a identificar as necessidades de informações para diferentes processos de negócios.

Nesta etapa podemos avaliar o levantamento de requisitos do processo de negócio para entender as necessidades da coleta de dados levantados pela fase anterior, documentar pontos críticos e avaliar a necessidade da coleta.

Nesta fase os requisitos de segurança precisam ser acordados e documentados antes que os sistemas de informação sejam desenvolvidos e/ou implementados.

É importante ressaltar que nessa fase os requisitos funcionais e não funcionais são analisados e pontos importantes de segurança são descobertos na análise dos requisitos.

Ao documentar no RIPD deve se identificar e avaliar riscos encontrado na análise de requisitos tendo em vista as medidas, salvaguardas e mecanismos de mitigação de

risco. A cada risco identificado, tende se definir a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

- **Especificação**

A especificação de requisitos documenta a fase anterior "Análise de requisitos". É todo requisito levantado e analisado, sobre um elemento, funcionalidade ou até mesmo um artefato ou, ainda, informações de qualquer tipo relacionadas ao ambiente que cerca o sistema.

Para o RIPD a especificação de requisitos permite aos desenvolvedores de sistemas de informação prever possíveis ameaças, suas consequências e contramedidas antes que um sistema esteja em funcionamento, minimizando a probabilidade de precisar reagir a essas ameaças a partir de possíveis ataques desastrosos a sistemas em funcionamento.

Para a especificação pode-se avaliar e decidir se alguns riscos são aceitáveis, até um risco de nível alto, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação como descrito no tópico 4.7, de medidas para tratamento de risco.

Deve-se destacar que o sistema tem de especificar no consentimento o risco de tratamento de dados de acordo com a norma ABNT NBR ISO/IEC 29184:2021 que especifica os controles que formatam o conteúdo e a estrutura dos avisos de privacidade *on-line*, bem como o processo de solicitação de consentimento para coletar e tratar dados pessoais (DP) de titulares de DP.

- **Verificação e validação**

A verificação envolve a análise do sistema para certificar se que os requisitos funcionais e não funcionais atendem os critérios estabelecidos. Já a validação, é a certificação de que o sistema atende as necessidades e expectativas do cliente.

Nesta etapa os requisitos de segurança têm de estar dentro dos critérios estabelecido seja ele a confidencialidade, integridade, não repúdio, prestação de contas e autenticidade como descrito no tópico 2 que descreve os processos de engenharia de requisitos.

A verificação e a validação têm o propósito de validar os requisitos de segurança e as medidas salvaguardas e de mitigação descritas no RIPD.

Ao realizar a verificação as partes interessadas têm de estar em acordo com os termos e critérios avaliados.

A formalização do RIPD se dá pela aprovação de todas as partes interessadas do tratamento de dados pessoais. O quadro abaixo demonstra uma forma de assinatura entre as partes para validar os processos de segurança.

Quadro 6 – Assinatura das partes interessadas

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	**ENCARREGADO**
_____ Nome do responsável Local, dia/mês/ano	_____ Nome do encarregado Local, dia/mês/ano

AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
_____ Nome do representante Local, dia/mês/ano	_____ Nome do representante Local, dia/mês/ano

Fonte: BRASIL, 2020

Após a aprovação e o documento formalizado, todos estarão cientes dos termos de segurança da informação e as metidas que foram tomadas para o tratamento de dados pessoais.

- **Gerência de requisitos**

Os requisitos devem ser documentados e controlados, de forma a minimizar o impacto e as dificuldades que possam vir a acontecer com as mudanças.

Para o RIPD a gerência de requisitos descreve medidas para controle de mudanças e providencia aprovação do cliente. No contexto de requisitos de segurança as mudanças relacionadas devem ser descritas de forma clara tendo em vista minimizar riscos e impactos na alteração.

Cabe destacar que a rastreabilidade é um ponto importante para a gerência de requisitos. A rastreabilidade de requisitos consiste na identificação de relações entre as

fontes dos requisitos, entre os requisitos propriamente ditos, e entre requisitos e os outros produtos da Engenharia de Software. (CASTRO, 2017).

A rastreabilidade permite a realização de uma análise de impacto mais eficiente na evolução do software. Essa análise ajuda na identificação de riscos associados a custos e cronograma e outros fatores que possam impactar em requisitos (restrições legais, por exemplo).

8. Conclusões e trabalhos futuros

Este trabalho apresenta recomendações para a construção da RIPD no processo de engenharia de requisitos, em que se utilizou técnicas para a construção do documento, que combinadas podem afirmar o compromisso com a privacidade e proteção dos dados pessoais.

Entre as contribuições deste trabalho estão o estudo da Lei Geral de Proteção de Dados Pessoais e como é a construção e elaboração de uma RIPD e apresenta recomendações para implementar a RIPD no processo de engenharia de requisitos.

Conclui-se a importância do relatório de impacto a proteção de dados para todas as áreas das empresas, principalmente se tratando de dados pessoais. Ao elaborar o RIPD, a organização realiza a avaliação da conformidade de suas operações de tratamento de dados em relação ao previsto pela LGPD – Lei Geral de Proteção de Dados, além de corroborar com a aderência da instituição ao princípio da responsabilização e prestação de contas, conforme apresentado no art. 6º, X, da referida legislação, ao demonstrar a adoção de medidas eficazes no cumprimento das normas de proteção de dados.

A RIPD traz uma grande contribuição para o processo de engenharia de requisitos tendo em vista a prevenção e mitigação de riscos em todos os processos de tratamento de dados, reforçando a conformidade com os requisitos de segurança.

Sugestões para trabalhos futuros incluem a aplicação do documento da RIPD em situações reais de empresas para ver sua efetividade. Também se destaca o desenvolver uma ferramenta que auxilie na construção da RIPD.

9. Referência

ABNT NBR ISO/IEC 29184:2021, Tecnologia da informação - Avisos de privacidade on-line e consentimento.

ALVES, Guilherme Barbosa. Uma proposta de processo de gerenciamento de riscos baseado na LGPD. 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3731. Acesso em: 14 out. 2022.

ALMEIDA, Vinicius. O que é Processo de Negócio: entenda a Classificação de Processos em uma organização, 2018. Disponível em: https://www.euax.com.br/2018/08/processo-de-negocio/. Acesso em: 16 maio. 2022.

BRASIL. Presidência da República. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 fev. 2022.

BRASIL. Ministério da Cidadania. Encarregado da LGPD. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx. Acesso em: 28 nov. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO, 2021A. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em: 26 out. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Sanções Administrativas: o que muda após 1º de agosto de 2021B. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 20 nov. 2022.

BRASIL. Ministério da Cidadania. Classificação dos Dados, 2021C. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados>. Acesso em: 20 nov. 2022.

BRASIL. Ministério da Cidadania. Direitos do(a) Titular, 2021D. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/direitos-do-titular>. Acesso em: 20 nov 2022.

BRASIL. Ministério da Cidadania. Encarregado da LGPD, 2021E. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/encarregado-da-lgpd>. Acesso em: Acesso em: 18 nov. 2022.

BRAZ, Fabricio. Requisitos de Segurança de Software. 2012. Disponível em: http://softwareseguro.blogspot.com/2012/10/requisitos-de-seguranca-de-software.html. Acesso em: 20 nov. 2022.

CASTRO, Eduardo. Gerência de Requisitos de software e a Matriz de Rastreabilidade. 2017. Disponível em http://rederequisitos.com.br/gerencia-de-requisitos-de-software-e-a-matriz-de-rastreabilidade/. Acesso em: 25 nov. 2022.

DIAS, Ricardo. Prototipagem de Software. 25/08/2019. Disponível em: https://medium.com/contexto-delimitado/prototipagem-de-software-7ac07027e6d8. Acesso em: 20 set. 2022.

DEVMEDIA. Requisitos, Modelagem e UML. Disponível em: https://www.devmedia.com.br/guia/requisitos-modelagem-e-uml/35697. Acesso em: 18 out. 2022.

FERNANDA. Elicitação de requisitos. 2018. Disponível em: https://medium.com/@fnandaleite/elicita%C3%A7%C3%A3o-de-requisitos-ff98a998189a. Acesso em: 27 nov. 2022.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. Métodos de pesquisa. Porto Alegre: Editora da UFRGS, 2009.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

GETPRIVACY. O que é e como elaborar o Relatório de Impacto à Proteção de Dados Pessoais. 2022. Disponível em: https://getprivacy.com.br/relatorio-de-impacto-lgpd/. Acesso em: 02 out. 2022.

ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*.

ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.*

JR CONSULTORIA. Pesquisa Quantitativa: O que é e como utilizar em seu negócio? 2021. Disponível em: https://jrconsultoria.com.br/pesquisa-quantitativa-o-que-e-e-como-utilizá-la-da-melhor-forma. Acesso em: 28 maio 2022.

LEHMAN, M. M. 1996. Laws of Software Evolution Revisited. In: Proceedings of the 5th European Workshop on Software Process Technology (outubro 09 - 11, 1996). C. Montangero, Ed. Lecture Notes in Computer Science, vol. 1149. Springer-Verlag, London, 108-124.

NARDI, Julio Cesar; FALBO, Ricardo de Almeida. Uma Ontologia de Requisitos de Software. 2006. Mestrado em Informática, Universidade Federal do Espírito Santo, Vitória - ES - Brasil. Disponível em: https://www.researchgate.net/publication/221561530_Uma_Ontologia_de_Requisitos_de_Software. Acesso em: 20 nov. 2022.

NASCIMENTO, Arthur Braga. A Era de Dados e o impacto da LGPD nos negócios, 2021. Disponível em: <https://valorinveste.globo.com/blogs/seu-negocio/post/2021/10/a-era-de-dados-e-o-impacto-da-lgpd-nos-negocios.ghtml>. Acesso em: 17 nov. 2022.

NÉGOCIO SEGURO. SEGURO CIBERNÉTICO: O QUE É E COMO SE PROTEGER DESSES RISCOS?. Disponível em:

<https://www.negocioseguroaig.com.br/industria/de-olho/seguro-cibernetico/>. Acesso em: 17 nov. 2022.

NOLETO, Cairo. T Tecnologia Requisitos não funcionais: o guia completo! 2020. Disponível em: https://blog.betrybe.com/tecnologia/requisitos-nao-funcionais/. Acesso em: 28 set. 2022.

MONITORA. Serviço de engenharia de requisitos: entenda como funciona. 2020. Disponível em: https://www.monitoratec.com.br/blog/servico-de-engenharia-de-requisitos/. Acesso em: 22 set. 2022.

PRESSMAN, Roger S. Engenharia de software [recurso eletrônico]: uma abordagem profissional; tradução Ariovaldo Griesi; revisão técnica Reginaldo Arakaki, Julio Arakaki, Renato Manzan de Andrade. – 7. ed. – Dados eletrônicos. – Porto Alegre: AMGH, 2011.

PRESSMAN, Roger S. Engenharia de software: uma abordagem profissional / Roger S. Pressman, Bruce R. Maxim; [tradução: João Eduardo Nóbrega Tortello ; revisão técnica: Reginaldo Arakaki, Julio Arakaki, Renato Manzan de Andrade]. – 8. ed. – Porto Alegre: AMGH, 2016.

PEREIRA, Eriky. SAIBA QUAIS SÃO OS 4 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO. 2019. Disponível em: https://blog-pt.lac.tdsynnex.com/saiba-quais-sao-os-4-principios-da-seguranca-da-informacao. Acesso em: 22 nov. 2022.

SOMMERVILLE, Ian; SAWYER, Peter. Requirements Engineering: a good practice guide - 1997.

SOMMERVILLE, I., Engenharia de Software, 8ª Edição. São Paulo: Pearson – Addison Wesley, 2007.

SOMMERVILLE, Ian. Engenharia de Software; tradução Ivan Bosnic e Kalinka G. de O. Gonçalves; revisão técnica Kechi Hirama. — 9. ed. — São Paulo: Pearson Prentice Hall, 2011.

SERPRO. QUEM VAI REGULAR A LGPD?, 2020. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 18 nov. 2022.

SERVICE. Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação. 2021. Disponível em: https://service.com.br/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao/#:~:text=Por%20exemplo%2C%20algu%C3%A9m%20pode%20deixar,seu%20login%20ao%20inseri%2Dlo. Acesso em: 20 nov. 2022.

SOFTWALL. Sanções administrativas da LGPD entram em vigor; entenda o que muda, 2021. Disponível em: <https://www.softwall.com.br/blog/sancoes-administrativas-da-lgpd/>. Acesso em: 18 nov. 2022.

TURINE, Marcelo Augusto Santos; MASIERO, Paulo Cesar. ESPECIFICAÇÃO DE REQUISITOS: UMA INTRODUÇÃO. 1996. Disponível em: http://www2.unemat.br/rhycardo/download/engenharia_de_requisitos.pdf. Acesso em: 26 set. 2022.

SILVA, João Guilherme P. da. Análise e Especificações de Requisitos. 2022. Tech - Análise Sistemas. Disponível em: http://www.linhadecodigo.com.br/artigo/3224/analise-e-especificacoes-de-requisitos.aspx. Acesso em: 26 set. 2022.

SEBRAE. O que é LGPD? 2020. Disponível em: https://www.sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd#:~:text=Ela%20foi%20inspirada%20na%20GDPR,passo%20importante%20para%20o%20Brasil. Acesso em: 18 nov. 2022.

UFPel. Ensaio sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) da Universidade Federal de Pelotas (UFPel). Disponível em:

https://wikigovernanca.ufpel.edu.br/_media/ens.ripd.ufpel.pdf. Acesso 27 em: mar. 2022.

UFPE. Diretriz: Modelo de Casos de Uso. 2006. Disponível em: https://www.cin.ufpe.br/~gta/rup-vc/core.base_rup/guidances/guidelines/use-case_model_CC121CF4.html. Acesso em: 25 nov. 2022.

VISURE. Especificação de requisito de software (SRS): dicas e modelo. 2022. Disponível em: https://visuresolutions.com/pt/software-requirement-specification-srs-tips-template/. Acesso em: 01 out. 2022.

VAZQUEZ, Carlos Eduardo et al. Engenharia de Requisitos: software orientado a negócio. Rio de Janeiro: Eletrônica: Abreu's System, 2016. 419 p.

VERÍSSIMO, Ricardo. Levantamento de Requisitos e Mapeamento de Processos. Disponível em: http://www.linhadecodigo.com.br/. Acesso em: 20 set. 2022.

VERAS, Christopher. Você sabe o que significa não repúdio? Descubra neste post! 2018. Disponível em: https://solutiresponde.com.br/voce-sabe-o-que-significa-nao-repudio-descubra-neste-post/. Acesso em: 25 nov. 2022.

WAZLAWICK, R. S. Metodologia de pesquisa para ciência da computação. Rio de Janeiro: Elsevier, 2014.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR
Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante LUCAS MONTEIRO SILVA do Curso de ENGENHARIA DA COMPUTAÇÃO, matrícula 20171003301006 na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado RECOMENDAÇÕES PARA A CONSTRUÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD) NO PROCESSO DE ENGENHARIA DE REQUISITOS, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 17 de DEZEMBRO de 2022.

Assinatura do autor: Lucas Monteiro Silva

Nome completo do autor: Lucas Monteiro Silva

Assinatura do professor–orientador: _____

Nome completo do professor-orientador: Adriana Silveira de Souza