

UNIVERSIDADE EVANGÉLICA DE GOIÁS - UNIEVANGÉLICA
ENGENHARIA DE SOFTWARE

CLARA ELIS PEREIRA
CAMILA DE SOUZA SILVA

**LEI GERAL DE PROTEÇÃO DE DADOS:
UM PROCESSO MÍNIMO PARA ADEQUAÇÃO E SEUS PRINCIPAIS CONCEITOS**

ANÁPOLIS – GO

2021

**CLARA ELIS PEREIRA
CAMILA DE SOUZA SILVA**

**LEI GERAL DE PROTEÇÃO DE DADOS:
UM PROCESSO MÍNIMO PARA ADEQUAÇÃO E SEUS PRINCIPAIS CONCEITOS**

Trabalho apresentado ao Curso de Engenharia de Software da Universidade Evangélica de Goiás – UniEVANGÉLICA, da cidade de Anápolis-GO como requisito parcial para obtenção do Grau de Bacharel em Engenharia de Software.

Orientador (a): Prof. Ms. Alexandre Moraes Tannus

ANÁPOLIS - GO

2021

FICHA CATALOGRÁFICA

Pereira, Clara Elis. Silva, Camila de Souza.

Lei Geral de Proteção de Dados: Um Processo Mínimo Para Adequação e Seus Principais Conceitos / Clara Elis Pereira, Camila de Souza Silva. - Anápolis, 2021.

Orientador: Alexandre Moraes Tannus.

Monografia - Universidade Evangélica de Goiás -- UniEVANGÉLICA, Curso de Engenharia de Software, Anápolis, 2021.

1. Dados. 2. Privacidade. 3. Transparência. 4. Adequação. I. Pereira, Clara Elis. II. Silva, Camila de Souza. III. Universidade Evangélica de Goiás – UniEVANGÉLICA. IV. Título.

REFERÊNCIA BIBLIOGRÁFICA

PEREIRA, Clara Elis. SILVA, Camila de Souza. **Lei Geral de Proteção de Dados: Um Processo Mínimo para Adequação e Seus Principais Conceitos**. Anápolis, 2021. 78 p. Monografia - Curso de Engenharia de Software. Universidade Evangélica de Goiás - UniEVANGÉLICA.

CESSÃO DE DIREITOS

NOMES DOS AUTORES: CLARA ELIS PEREIRA

CAMILA DE SOUZA SILVA

TÍTULO DO TRABALHO: LEI GERAL DE PROTEÇÃO DE DADOS: UM PROCESSO MÍNIMO PARA ADEQUAÇÃO E SEUS PRINCIPAIS CONCEITOS

GRAU/ANO: Graduação /2021.

É concedida à Universidade Evangélica de Goiás - UniEVANGÉLICA, permissão para reproduzir cópias deste trabalho, emprestar ou vender tais cópias para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte deste trabalho pode ser reproduzida sem a autorização por escrito do autor.

Clara Elis Pereira
Camila de Souza Silva
Anápolis – GO.

**CLARA ELIS PEREIRA
CAMILA DE SOUZA SILVA**

**LEI GERAL DE PROTEÇÃO DE DADOS:
UM PROCESSO MÍNIMO PARA ADEQUAÇÃO E SEUS PRINCIPAIS CONCEITOS**

Monografia apresentada para Trabalho de Conclusão de Curso de Engenharia de Software da Universidade Evangélica de Goiás - UniEVANGÉLICA, da cidade de Anápolis-GO como requisito parcial para obtenção do grau de Engenheiro(a) de Software.

Aprovado por:

**Prof. Ms. Alexandre Moraes Tannus
(ORIENTADOR)**

**Prof. Ms. Millys Fabrielle Carvalhaes
(AVALIADOR)**

Anápolis, 03 de Dezembro de 2021

RESUMO

Os dados possuem alto valor competitivo e são utilizados em sua maioria para atingir propósitos econômicos. Entretanto, nem sempre o caminho que esses dados percorrem são legítimos e esclarecidos. A Lei Geral de Proteção de Dados (LGPD) foi sancionada com o intuito de promover a liberdade e a privacidade de qualquer tratamento envolvendo dados com objetivos financeiros, e isso significa que, tanto órgãos públicos quanto empresas privadas terão de se adequar à lei, sob risco de penalidade em caso de descumprimento. No entanto, diversas companhias estão enfrentando dificuldades para adotar o processo de conformidade, devido à alta complexidade e imprecisão do tema. Logo, faz-se necessário criar um plano de adequação que auxilie na compreensão e implementação da lei, elucidando assim os principais pontos de dúvidas e definindo um processo mínimo de adequação. O processo será implementado no SigTuring, sistema de gestão da Fábrica de Tecnologias Turing, que tem por objetivo o registro do horário de entrada e saída de seus funcionários. Através da pesquisa exploratória realizada foi possível executar a análise de exemplos que estimularam a compreensão, e para identificar o caminho das informações foi realizado o mapeamento do fluxo de dados e a avaliação dos riscos, os quais possibilitam a visualização do estado atual da rota que os dados percorrem e auxilia na preservação do patrimônio organizacional. Como resultado, a pesquisa possibilitou grande avanço no conhecimento não só da lei como também de sua importância e abrangência, além de tornar claro as atividades necessárias para a elaboração coerente do plano de conformidade.

Palavras-Chave: dados; privacidade; transparência; adequação.

LISTA DE FIGURAS

Figura 1 – Conhecimento sobre a LGPD entre pessoas físicas	11
Figura 2 – Conformidade com a LGPD entre pequenas e médias empresas	12
Figura 3 – Dados, Informação e Conhecimento	31
Figura 4 – Principais causas de vazamento de dados nas empresas	33
Figura 5 – LGPD – Responsáveis, Quem e Como	35
Figura 6 – Matriz de Probabilidade x Impacto	38
Figura 7 – Critérios de nível de risco	39
Figura 8 – Pergunta 1 sobre a compreensão dos conceitos da LGPD	51
Figura 9 – Pergunta 2 sobre a compreensão dos conceitos da LGPD	52
Figura 10 – Comparativo entre os mapeamentos inicial e final	53
Figura 11 – Comparativo entre avaliação de riscos.....	55

LISTA DE QUADROS

Quadro 1 – Comparativo entre funções do controlador e do operador.....	19-20
Quadro 2 – Mapeamento Inicial Geral – Fábrica de Tecnologias Turing	36-37
Quadro 3 – Planejamento de atividades	45
Quadro 4 – Mapeamento Final Geral – Fábrica de Tecnologias Turing	46-47

LISTA DE TABELAS

Tabela 1 – Identificação e avaliação dos riscos.....	39
Tabela 2 – Identificação de medidas para tratar os riscos	40-42

LISTA DE ABREVIATURAS E SIGLAS

Siglas	Descrição
ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
DPO	Oficial de Proteção de Dados
GDPR	Regulamento Geral de Proteção de Dados
IDC	Corporação Internacional de Dados
LGPD	Lei Geral de Proteção de Dados

SUMÁRIO

1	INTRODUÇÃO	9
2	JUSTIFICATIVA	11
3	FUNDAMENTAÇÃO TEÓRICA.....	14
3.1.	Lei Geral de Proteção de Dados	14
3.2.	O Que São Dados?	15
3.2.1.	Conceito de Dados Pessoais	15
3.2.2.	Conceito de Dados Sensíveis	16
3.2.3.	Conceito de Dados Anônimos	16
3.3.	Banco de Dados.....	17
3.4.	Titular.....	17
3.5.	Agentes de Tratamento	18
3.5.1.	Controlador.....	18
3.5.2.	Operador	19
3.6.	Encarregado.....	20
3.7.	Autoridade Nacional de Proteção de Dados (ANPD)	20
3.8.	Bases Legais	21
3.8.1.	Bases Legais Para o Tratamento de Dados Pessoais	21
3.8.2.	Bases Legais para o Tratamento de Dados Pessoais Sensíveis	22
3.9.	Exceções de Inaplicabilidade	23
3.10.	Sanções Administrativas	23
4	METODOLOGIA DA PESQUISA	25
5	DESENVOLVIMENTO	27
5.1	Análise de Exemplos.....	27
5.2	Plano de Adequação	30
5.2.1	Conscientização	31
5.2.1.1	Porque os Dados são Importantes?.....	31
5.2.1.2	Porque Regulamentar o Tratamento de Dados?	33
5.2.1.3	Apresentação da Lei.....	35
5.2.2	Mapeamento de Dados.....	37
5.2.2.1	Avaliação de Riscos	39
5.2.3	Diagnóstico	44

5.2.4	Planejamento	46
5.2.5	Implementação.....	47
5.2.6	Monitoramento	51
6	RESULTADOS ALCANÇADOS.....	52
7	CONCLUSÃO E CONSIDERAÇÕES FINAIS	57
	APÊNDICE A – DOCUMENTO DE IDENTIFICAÇÃO DO CONTROLADOR	62
	APÊNDICE B – POLÍTICA DE DESCARTE – FÁBRICA DE TECNOLOGIAS TURING	64
	APÊNDICE C – POLÍTICA DE PRIVACIDADE – FÁBRICA DE TECNOLOGIAS TURING	66
	APÊNDICE D – SUGESTÃO DE BOAS PRÁTICAS DE SEGURANÇA E PROPOSTA DE FERRAMENTA	70
	APÊNDICE E – TERMO DE AUTORIZAÇÃO PARA MENORES DE IDADE	75

1 INTRODUÇÃO

Um dos maiores problemas enfrentados pela sociedade digital é o uso indevido de informações e as consequências resultantes disso. Com a globalização e o rápido desenvolvimento da tecnologia, a comunicação foi acelerada através de dispositivos interativos, formando uma onda massiva de dados e uma forte disputa entre as empresas, o que acabou desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes (RAPÔSO, 2019). Os dados representam ativos valiosos para as organizações, visto que podem ser utilizados para detecção de padrões e resolução de problemas de negócio, além de que, são empregados em sua maioria para propósitos lucrativos e/ou financeiros. “Segundo a provedora de inteligência de mercado IDC, 2,5 quintilhões de bytes de informações são criados todos os dias e 49% das empresas conseguem monetizá-los, isto é, vender e rentabilizar as informações obtidas por meio de dados” (NSC, 2019). Desse modo, foi promulgada a Lei Geral de Proteção de Dados (LGPD), a qual impõe regras para o tratamento dos dados e impacta diretamente companhias que os administram.

Conforme o Art. 1º da Lei Nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados determina diretrizes para proteger os direitos fundamentais de liberdade e privacidade de dados, assim como garantir a transparência em todo seu tratamento (BRASIL, 2018). Foi sancionada em 2018 e passou a vigorar em 2020, sendo estabelecida como forma de balancear o controle sobre o que acontece com os dados e em quais circunstâncias deverão ser coletados. Junto com a proteção dos dados, a lei trará grandes mudanças no cenário corporativo.

É considerada um marco jurídico único no Brasil e abrange tanto as organizações públicas quanto as privadas, que terão que se adequar a essa nova legislação, a qual preconiza a proteção dos direitos fundamentais de liberdade e privacidade dos cidadãos brasileiros (DONDA, 2020). Com a adoção da lei, o Brasil agora se equipara a outros países que possuem modelos robustos para a proteção de dados. É fundamental que as organizações adaptem em toda a sua estrutura e cadeia de funcionários os princípios éticos da lei, ajustando a segurança de seus dados e de suas tecnologias, além de definirem uma relação transparente em seu trabalho e capacitar seus funcionários (RAPÔSO, 2019).

Todavia grande parte das empresas estão encontrando dificuldades para realizar a implementação da LGPD. Conforme BluePex (2020), de 389 pequenas e médias empresas,

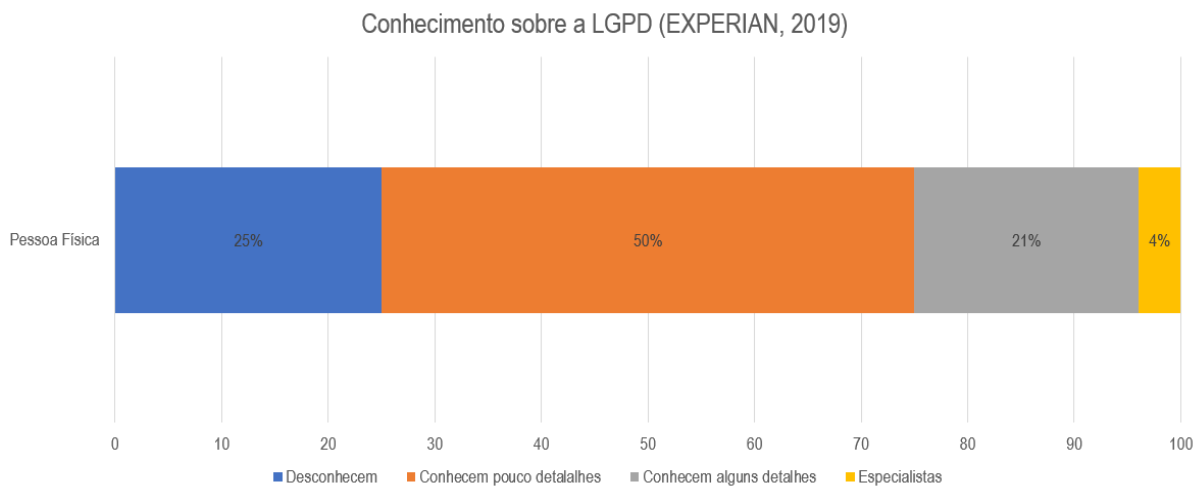
apenas 2% delas estão totalmente preparadas para as regras impostas. Dessa forma, é notável que a legislação representa um grande desafio para a maioria das organizações, visto que 30% delas estão totalmente despreparadas. Um dos principais obstáculos encontrados pelas companhias é a falta de exatidão que a lei traz, tendo em vista sua abrangência e quantidade de imposições a serem seguidas. “É uma boa lei, extremamente necessária, mas poderia ter sido mais precisa. Pode trazer insegurança jurídica para as empresas” (RUSSO, 2020). Embora a lei determine diversas premissas para o controle dos dados, ela não visa esclarecer como as organizações farão de fato para que esses requisitos sejam atendidos.

Como objetivo geral, é necessário estabelecer um plano de adequação da LGPD, voltado para pequenas e médias empresas, juntamente com o mapeamento dos dados e a avaliação de riscos. De modo específico, primeiro obtém-se compreensão quanto aos princípios e diretrizes da lei, para em seguida definir um processo mínimo de adequação. Depois de ter o processo definido, é necessário estipular quais serão os procedimentos necessários para sua implementação. Posteriormente, aplica-se o processo em um cenário real.

2 JUSTIFICATIVA

A implementação da Lei Geral de Proteção de Dados exige mudanças de processos e estabelecimento de padrões em todas as atividades de tratamento de dados. Contudo, ainda existem alguns impasses que dificultam o seu processo de adequação. Estatísticas apontam cada vez mais a carência de conhecimento e de conformidade em relação à nova Lei Geral de Proteção de Dados, por parte não só de pessoas físicas, como também de pessoas jurídicas. Um levantamento realizado com 1.564 pessoas físicas sobre o conhecimento da LGPD reforça a ausência de saber acerca de suas premissas, conforme Experian (2019):

Figura 1: Conhecimento sobre a LGPD entre pessoas físicas.

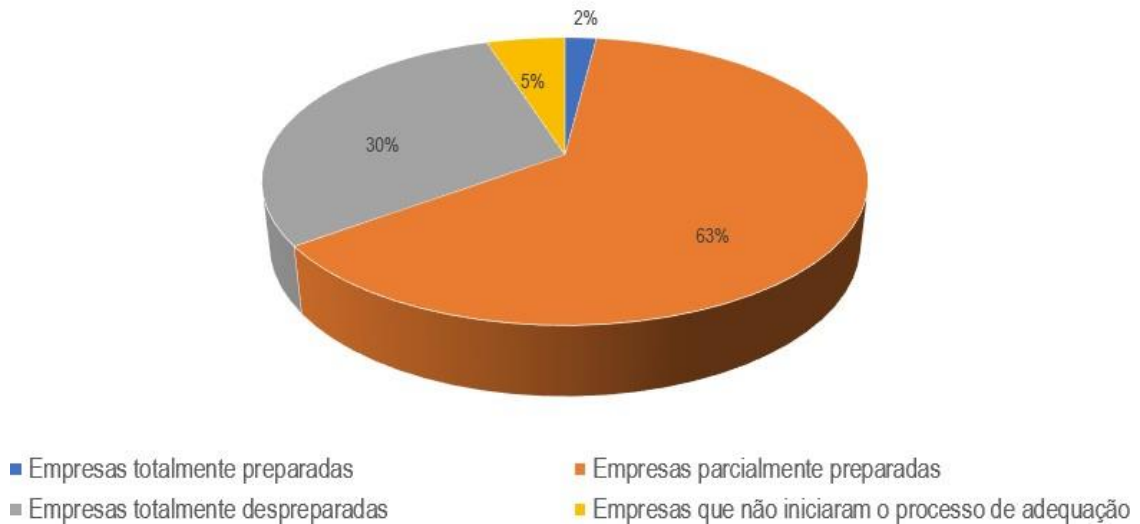


Fonte: Experian, 2019

É notável que o alcance da LGPD entre pessoas físicas representa um obstáculo no processo de adequação, visto que para estar de acordo com a lei é necessário antes conhecê-la. Ao analisar a figura 1, observa-se que 96% dela está em fase de pouco, ou nenhum conhecimento sobre a legislação, o que fortalece ainda mais a necessidade de esclarecimento sobre seus conceitos. Uma segunda pesquisa realizada entre pessoas jurídicas, isto é, entre 389 pequenas e médias empresas, reflete o despreparo organizacional para a chegada da LGPD, conforme BluePex (2020):

Figura 2: Conformidade com a LGPD entre pequenas e médias empresas.

Conformidade com a LGPD entre pequenas e médias empresas (BLUEPEX 2020)



Fonte: Bluepex, 2020.

A adequação da Lei Geral de Proteção de Dados representa um dilema para as organizações, visto que das 389 companhias entrevistadas, apenas 8 delas (2%) se consideram preparadas. Isso demonstra a dificuldade de preparo e deixa em evidência a importância de se ter um procedimento adaptado às circunstâncias da lei. Mediante a extensão da inadimplência provocada pela amplitude e imprecisão do tema, faz-se necessário a criação de um processo mínimo de conformidade, que contará com dois pontos principais: o mapeamento do fluxo dos dados e a avaliação dos riscos.

Através do mapeamento do fluxo de dados é possível fornecer uma visão bastante detalhada das informações que a organização possui, permitindo acompanhar em quais processos estes dados estão sendo utilizados, juntamente com a sua finalidade (REDEMPRESA, 2020). O mapeamento feito de forma correta indica o caminho que os dados percorrem do início ao fim, sendo bastante vantajoso, pois não só ajuda a identificar e eliminar inconsistências e redundâncias, mas também padroniza todas as atividades de tratamento de dados. Além disso, proporciona maior segurança jurídica perante à LGPD.

A mensuração de riscos é bastante significativa dentro do contexto de adequação à lei, pois pode-se afirmar que:

“Ainda que o empresário tenha compreendido as obrigações para garantir a privacidade de seus clientes, muitos ainda não sabem por onde começar essa implantação, pois sequer têm ideia dos riscos existentes no seu próprio negócio” (GRALHA, 2020).

Conhecer os riscos existentes e gerenciá-los auxilia a forma de tratar fatores que podem influenciar o ambiente de trabalho, além de preservar o patrimônio institucional e as vidas associadas, como por exemplo, no caso de um vazamento de dados.

3 FUNDAMENTAÇÃO TEÓRICA

3.1. Lei Geral de Proteção de Dados

A LGPD dispõe sobre o tratamento de dados pessoais, por pessoa natural e jurídica, tanto em meios físicos quanto digitais, com o propósito de proteger os direitos de privacidade e liberdade dos titulares (BRASIL, 2018). Foi sancionada como forma de equilibrar a desigualdade de poder sobre a informação entre o proprietário dos dados e quem os utiliza e compartilha. O Brasil já dispõe de diversas regulamentações e diretrizes que atuam na preservação e privacidade dos dados, no entanto, as várias leis setoriais acabam por criar um sistema legal complexo. A LGPD visa alterar esse cenário, por meio de uma legislação exclusiva e delimitada sobre o tema. Para Pinheiro (2020, p.11) “é uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas”.

A lei foi criada com base no GDPR, regulamento de proteção de dados para países constituintes da União Europeia. Aplica-se a todas as operações de tratamento de dados realizadas em território brasileiro, visando monitorar o uso dos dados que tenham sido coletados em solo nacional. Conforme Maciel (2019, p. 17):

A LGPD adotou o modelo do regulamento europeu. Embora mais sucinto, seus pilares são praticamente os mesmos (...). A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, valor cada vez mais na pauta dos cidadãos a partir da divulgação cada vez maior de casos de uso indevido de tais informações.

A disseminação dos casos de utilização inadequada de informações ressalta a importância de protegê-las, e um dos propósitos da LGPD é proporcionar maior estabilidade entre o uso dos dados e a privacidade dos mesmos. Dessa forma, a legislação determina 10 princípios fundamentais a serem observados durante o tratamento de dados, voltados para maior compreensão. Donda (2020, p. 21) os descreve como sendo:

- a) **Finalidade** – propósito legítimo da coleta e do tratamento de dados informados ao titular.
- b) **Adequação** – o tratamento deve ser compatível com a finalidade.
- c) **Necessidade** – limitar o tratamento ao mínimo necessário.

- d) **Livre acesso** – garantir ao titular consulta (gratuita), duração e integralidade dos seus dados.
- e) **Qualidade dos dados** – exatidão, clareza e relevância dos dados de acordo com a necessidade e para cumprir a finalidade.
- f) **Transparência** – garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
- g) **Segurança** – adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- h) **Prevenção** – adotar medidas para prevenir a ocorrência de danos.
- i) **Não discriminação** – não permitir a realização do tratamento para fins discriminatórios, ilícitos ou abusivos.
- j) **Responsabilização e prestação de contas** – demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os princípios da LGPD são fundamentais para melhor percepção sobre o tema, visto que eles são a base da lei e validam o tratamento dos dados, proporcionando maior delimitação sobre o uso dos mesmos. Além dos que foram citados, a legislação também instituiu o princípio da boa-fé, o qual consiste na conduta apropriada e comportamento ético nas atividades aplicadas aos dados, evitando assim fraudes e abusos.

3.2. O Que São Dados?

3.2.1. Conceito de Dados Pessoais

Dado pessoal pode ser descrito como toda informação que possa identificar uma pessoa ou torná-la identificável, de forma direta ou indiretamente. Nome, CPF (Cadastro de Pessoa Física), endereço e cor dos olhos são exemplos de dados pessoais.

O Regulamento 2016/679 da União Europeia (General Data Protection Regulation - GDPR), que serviu como suporte para a construção da LGPD, em seu art. 4º, n.1, define os dados pessoais como:

Dados pessoais, informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

Já para Doneda (2020, p. 139) os dados podem ser definidos da seguinte forma:

O “dado” apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição.

Um dado sozinho pode não ser capaz de identificar uma pessoa ou produzir sentido, não sendo o bastante para conduzir compreensão. Quando um conjunto de dados é tratado e organizado, de forma a proporcionar coerência dentro de um determinado contexto, ele se torna uma informação. Isto é, a informação representa a ordenação de um agrupamento de dados, que tem significado real e pode ser usada para fundamentar o conhecimento.

3.2.2. Conceito de Dados Sensíveis

Os dados sensíveis são uma espécie de dados pessoais que constituem uma classe diferente devido ao seu conteúdo oferecer uma vulnerabilidade especial: a discriminação (BIONI, 2019). Por meio dos dados sensíveis é possível identificar as individualidades mais significativas das pessoas, portanto, é necessário ter a atenção ampliada em todo o seu tratamento. Para Pinheiro (2020, p. 19-20):

São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como 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 a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Os dados sensíveis possuem um potencial maior para gerar riscos consideráveis aos direitos e liberdades fundamentais do titular, e seu tratamento deve ser submetido a uma gestão especial para análise minuciosa. Logo, se inseridos em um contexto inadequado de utilização podem causar atos discriminatórios e nocivos, além de expor outras questões sensíveis do titular.

3.2.3. Conceito de Dados Anônimos

Dados anônimos são dados relativos a alguém que não possa ser identificado, considerando a utilização das técnicas razoáveis e disponíveis na circunstância de seu

tratamento (BRASIL, 2018). Quando um dado se torna anônimo, ele perde a probabilidade de ser associado a um determinado indivíduo, direta ou indiretamente. Doneda (2020, p. 142) demonstra a utilidade de usá-los:

Um dado pode também se referir a uma pessoa indeterminada. Este é o caso do dado anônimo, útil para diversas finalidades nas quais tem valor a informação referente a uma determinada coletividade ou corte específico de indivíduos, sem que as pessoas às quais se refiram possam ser nominadas.

A anonimização oculta dados que podem ser sensíveis antes mesmo de serem autorizados para uso, tornando os dados anônimos extremamente válidos para análises coletivas ou direcionadas. Um exemplo são pesquisas gerais que revelam algum tipo de preferência, voltadas para deliberação onde o mais importante é saber o que foi escrito e não quem escreveu.

3.3. Banco de Dados

Um banco de dados pode ser compreendido por uma coleção estruturada de dados, formada por um conjunto de informações, nas quais podem estar distribuídas ou somente em um único lugar, independente do meio no qual está armazenado, ou seja, pode ser de origem digital ou manual (POHLMANN, 2019). As informações agrupadas de forma a produzir algum sentido constituem um banco de dados. É comum que as organizações tenham diversas informações que precisam ser ordenadas e agrupadas e lidem com grande volume de dados diariamente. Portanto, é importante ter um banco de dados gerenciável que armazene todos os dados de forma eficiente, assim, quando tratados e analisados, servirão como base para tomada de decisões.

3.4. Titular

O titular é a pessoa natural identificada ou identificável, que possui seus dados como objeto de tratamento (BRASIL, 2018), e pode ser compreendido como o proprietário dos dados. É importante destacar que dados de pessoas jurídicas não se enquadram no escopo da LGPD. Para garantir a transparência em todo o processo de uso, desde a coleta dos dados até seu descarte, a lei concede novos direitos aos titulares, não explícitos anteriormente.

São eles:

- a) Confirmação da existência de tratamento;
- b) Acesso aos dados;
- c) Correção de dados incompletos, inexatos ou desatualizados;
- d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- e) 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;
- f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- g) Informação das entidades públicas e privadas com os quais o controlador realizou uso compartilhado de dados;
- h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- i) Revogação do consentimento, nos termos do §5º do art. 8º desta lei.
 § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
 § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei (BRASIL, 2018).

As novas prerrogativas atribuídas aos titulares salientam a autodeterminação informativa, um dos fundamentos presentes na lei com o intuito de ressaltar o poder que cada indivíduo tem sobre os próprios dados e em quais cenários podem ser coletados. É fundamental entender cada um dos direitos de forma clara para aplicá-los, visto que eles são um dos pontos principais durante o processo de adequação.

3.5. Agentes de Tratamento

Os agentes de tratamento são as entidades responsáveis pelo processamento das informações do titular. Pohlmann (2019, p. 56) os relata:

Eles são os responsáveis jurídicos por eventos de segurança relacionados com os dados dos titulares. Assim, no caso de um vazamento de dados, por exemplo, serão eles quem devem prestar contas as autoridades e aos titulares (...) também cabe aos agentes de tratamento a realização de medidas de segurança que permitam (ou tentem) garantir a segurança dos dados tratados.

A LGPD atribui os agentes de tratamento ao controlador e operador, e exige que todas as operações de tratamento de dados sejam registradas conforme o Art. 37. Se houver perda, dano, ou algum tipo de acesso não autorizado os agentes podem ser submetidos a penalidades por infração à lei e imprudência com os dados que estavam sob sua responsabilidade.

3.5.1. Controlador

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018). Em suma, o controlador é quem manda no que acontece com os dados, e pode ser tanto uma pessoa física quanto uma empresa. Seu papel é garantir a transparência para com o titular e adotar medidas de segurança e boas práticas para estar em conformidade com a legislação, visto que é sobre ele que incide toda a responsabilidade do tratamento dos dados.

3.5.2. Operador

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018). O operador é a pessoa designada pelo controlador para realizar tratamento dos dados de fato, e deve seguir todas as instruções que lhe foram estabelecidas. Além disso, podem existir situações em que o controlador e o operador são a mesma pessoa. O quadro 1 apresenta uma análise comparativa entre as funções instruídas ao controlador e ao operador:

Quadro 1: Comparativo entre funções do controlador e do operador

	OBRIGAÇÕES GERAIS	
	CONTROLADOR	OPERADOR
Limites para tratamento	Tratar dados com base legal definida	Tratar dados conforme propósito definidos pelo controlador
Registros	Registro das atividades	Registro das atividades
Direitos dos titulares	Atender aos direitos dos titulares	Colaborar com o controlador
Incidentes	Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares	Informar ao controlador casos de incidentes

Boas práticas de segurança	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	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
Programa de Governança em privacidade	Implementar Programa de Governança em Privacidade, observadas a estrutura, a escala e o volume de suas operações, bem com o a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados	Receber e estar ciente do Programa de Governança adotado pelo controlador

Fonte: Adaptado. (MACIEL, 2019, p. 64).

3.6. Encarregado

O encarregado de dados, também chamado de DPO, é a pessoa indicada pelo controlador para atuar como intermediário de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (BRASIL, 2018). O encarregado não sofre penalidades tal qual o controlador e o operador, e é fundamental que suas práticas e atividades estejam alinhadas com os padrões de conformidade da empresa. Suas funções consistem em prestar esclarecimento aos titulares, considerar suas reclamações, receber instruções da ANPD e executar as demais atribuições.

3.7. Autoridade Nacional de Proteção de Dados (ANPD)

A autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2018). A ANPD tem por objetivo efetuar fiscalizações que sejam pertinentes ao tratamento de dados, elaborar diretrizes de regulamentação e aplicar sanções em caso de violação ou não

cumprimento da lei. Sua eficiência fiscalizatória será crucial para a consolidação da LGPD em todo país, e é fundamental destacar que, tão importante quanto à criação de leis que regulamentam o tratamento de dados, é a maneira legal pelas quais elas se farão cumpridas.

3.8. Bases Legais

3.8.1. Bases Legais Para o Tratamento de Dados Pessoais

Para o tratamento de dados pessoais, a LGPD estabelece alguns requisitos, ou bases legais, mediante as quais se permite que os dados sejam processados, com a observância dos demais artigos da lei (POHLMANN, 2019). As bases legais nada mais são do que as hipóteses em que pode ocorrer o tratamento de dados. Isto significa que qualquer pessoa que trate dados com a finalidade econômica precisa ter uma base legal para fundamentar sua coleta, para que o tratamento de dados realizado seja autêntico e lícito. A LGPD define em quais hipóteses o mesmo poderá ser realizado:

- a) Mediante o fornecimento de consentimento pelo titular;
- b) Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- c) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- d) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- e) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- f) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral
- g) Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- h) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- i) Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- j) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018).

É necessário definir uma base legal para cada finalidade de tratamento de dados. Com a LGPD em vigor, as organizações que realizarem a análise de dados sem definir uma das hipóteses de tratamento que justifique corretamente sua coleta, estará tratando os dados de maneira ilegítima. Além disso, bases legais não têm dependência entre si e se relacionam de

maneira separada.

3.8.2. Bases Legais para o Tratamento de Dados Pessoais Sensíveis

Os dados sensíveis, por possuírem potencial discriminatório, necessitam de uma análise especial para poderem ser tratados. Isso também inclui as bases legais, que precisaram ser alteradas para lidar com esse tipo de dados. É necessário adotar medidas cautelosas e dobrar a atenção no que diz respeito aos princípios da lei e direitos dos titulares, visto que um incidente eventual de vazamento de dados sensíveis pode ser altamente prejudicial, sobretudo por ferir diretamente os direitos de liberdade e privacidade do titular. A LGPD estabelece em quais hipóteses poderá ocorrer o tratamento de dados sensíveis:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- a) Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- b) Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
 - c) Cumprimento de obrigação legal ou regulatória pelo controlador;
 - d) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - e) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - f) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
 - g) Proteção da vida ou da incolumidade física do titular ou de terceiros;
 - h) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - i) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018)

Embora semelhantes, as bases legais para o tratamento de dados sensíveis diferem das bases para tratamento de dados comuns. Inclusive o consentimento, que mesmo estando presente nas duas hipóteses, se tratando de dados sensíveis, é necessário que seja mais detalhado e robusto, concedido de forma destacada e apenas para finalidades específicas. Além disso, deixam de existir as bases legais de execução de contrato, legítimo interesse e proteção ao crédito, já que essas bases tornam inviável a utilização de dados sensíveis. Também foi adicionada uma nova base legal, a qual permite o tratamento de dados sensíveis quando se tem a intenção de prevenir algum tipo de fraude ou engano com as informações do titular.

3.9. Exceções de Inaplicabilidade

Como toda legislação, a LGPD também dispõe de situações em que não é necessário aplicá-la. O Art. 4º define em quais cenários não é preciso se adaptar às suas circunstâncias: quando o tratamento de dados é realizado por uma pessoa natural para fins particulares e não financeiros; fins exclusivamente jornalísticos, artísticos, ou acadêmicos; fins voltados para segurança pública, defesa nacional e segurança do Estado; atividades de investigação; dados que são provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país (BRASIL, 2018). Apenas finalidades específicas são exceções de aplicação da lei, principalmente quando o tratamento de dados não é feito com viés econômico. Órgãos públicos, pessoas jurídicas e pessoas físicas que tratem dados com propósitos financeiros são redigidos pelo escopo da legislação e precisam adotar o processo de conformidade.

3.10. Sanções Administrativas

A LGPD também prevê sanções administrativas em caso de descumprimento, essas que variam conforme a intensidade da infração. São definidas como:

- a) Advertência, com indicação de prazo para adoção de medidas corretivas;
- b) 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;
- c) Multa diária, observado o limite total a que se refere o inciso II;
- d) Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- e) Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- f) Eliminação dos dados pessoais a que se refere a infração;
- g) 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;
- h) 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;
- i) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

As sanções são aplicáveis a todos os agentes de tratamento, e o titular que identificar

violação dos seus direitos mesmo após já ter notificado a empresa poderá ir até o site da ANPD para formalizar sua queixa. Caso a organização receba advertência, é imprescindível que as medidas necessárias sejam tomadas o mais rápido possível, evitando assim deixar que uma penalidade ainda maior seja imposta.

O proceso mínimo estabelecido abordará a definição de todos os papéis necessários para conformidade com a lei e a categorização dos dados, os rotulando como comuns ou sensíveis. Os agentes de tratamento, assim como os titulares dos dados serão devidamente identificados na organização de acordo com suas funções, e o tratamento de dados se tornará legítimo, visto que para cada finalidade encontrada, uma base legal será decidida. Logo, o plano de adequação será executado de acordo com as necessidades e demandas da empresa.

4 METODOLOGIA DA PESQUISA

Visando uma melhor compreensão das premissas estabelecidas pela LGPD, foram realizadas pesquisas exploratórias, a fim de ampliar o conhecimento sobre a lei. Foi realizada a análise de exemplos que auxiliaram a compreensão, proporcionando um melhor discernimento sobre os conceitos estabelecidos. Além disso, a definição dos processos necessários para sua implementação se deu através da avaliação de riscos e do mapeamento do fluxo dos dados. O mapeamento apresenta como as organizações estão lidando com questões como privacidade e com a segurança dos dados de seus colaboradores e clientes (JUSBRASIL, 2020) juntamente com a identificação das principais demandas a serem abordados no processo de adequação. A avaliação dos riscos foi feita com o intuito de preveni-los, visto que ela é muito importante para dar visibilidade à situação dos dados, assim como priorizar os investimentos e proteger esses ativos da melhor maneira (DONDA, 2020). A mitigação dessas ameaças foi embasada no guia de avaliação de riscos instituído pelo Governo Digital (2021).

Para ficar em conformidade com a lei, foi realizado um estudo de caso com abordagem exploratória, analisando os pontos mais imprecisos da legislação com o objetivo de favorecer total clareza e um maior entendimento da temática proposta, bem como o direcionamento da pesquisa e a obtenção de padrões. Assim como o mapa dos dados, o procedimento de adequação seguiu o método proposto pela advogada Mariana de Toledo, através do Manual da LGPD Descomplicado, o qual consistiu na aplicação de seis principais fases, que podem ser empregadas em todo método de conformidade, independentemente do nicho empresarial. Tais fases são compostas por:

Conscientização: consiste em expor a lei e seus fundamentos, tencionando demonstrar sua relevância e aplicação prática para os colaboradores da companhia; mapeamento: é a construção do mapa de dados, e tem por objetivo encontrar o estado atual de circulação dos dados dentro da empresa; diagnóstico: é a fase em que é necessário identificar as principais zonas de desconformidade por meio do mapeamento realizado na etapa anterior e indicar as possíveis soluções para minimizar os riscos existentes; planejamento: significa idealizar como as soluções serão colocadas em prática e montar um cronograma para cumprimento; implementação: o objetivo desta fase é atender ao plano elaborado na fase anterior, criando e descrevendo todos os documentos necessários e adotando atividades de boas práticas; monitoramento: é a constante supervisão da conformidade com as diretrizes da lei e a busca por melhora progressiva (TOLEDO, 2021).

É necessário realizar a análise aprofundada das necessidades de cada companhia, suas

principais demandas e particularidades próprias do seu ramo organizacional. No entanto, as etapas do processo sempre serão as mesmas, em todo procedimento de adequação. Ademais, foi realizada a validação da efetividade do esquema estratégico através da aplicação do método em um cenário real, o qual seguiu os critérios propostos.

5 DESENVOLVIMENTO

5.1 Análise de Exemplos

Visando a obtenção de conhecimento quanto às principais diretrizes da LGPD, foram realizadas análises de exemplos das bases legais objetivando aumentar o nível de compreensão sobre seus conceitos. As bases legais representam os cenários em que são permitidos realizar a coleta e demais tipos de tratamento de dados, no entanto estão sujeitas a dúvidas e podem acabar gerando incerteza em suas hipóteses. A exploração do tema permitiu entendê-las através de exemplos:

a) Consentimento:

É extremamente importante dispor de meios que confirmem a autenticidade do consentimento expresso, além de que existem formas diferentes de obtê-lo. Exemplo: Quando navega-se em um website e surge uma caixa de seleção com o texto adequado solicitando a autorização do titular para envio de anúncios personalizados. A maneira demonstrada é através de um formulário web, por isso é essencial que nenhuma opção esteja pré-selecionada. A evidência do consentimento será eletrônica e “deve conter uma forma clara de comprovar que um determinado titular aceitou o processamento de seus dados, desde um determinado endereço IP, em uma data e hora específica” (POHLMANN, 2019, p. 77).

b) Cumprimento de Obrigação Legal:

Quando existem legislações que obriguem o tratamento de dados, este poderá ser realizado sem o consentimento prévio do titular.

Exemplo: A lei nº 13.787 de 27 de dezembro de 2018 em seu art. 6º informa que os prontuários em suporte de papel e os digitalizados só poderão ser eliminados decorrido o prazo mínimo de 20 anos a partir do último registro (BRASIL, 2018). Desse modo, os dados dos pacientes contidos nos prontuários podem ser armazenados independente da sua autorização.

c) Execução de Políticas Públicas:

Os agentes de administração pública poderão coletar dados para executar políticas

previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (BRASIL, 2018).

Exemplo: Quando há necessidade de coleta de dados para que a administração pública exerça a entrega de serviços públicos, como saneamento básico e programas de assistência social.

d) Estudo por Órgão de Pesquisa

Órgãos de pesquisa podem coletar dados quando necessários para conclusão de estudos desde que seja garantida sua anonimização sempre que possível e observados os demais fundamentos da lei. Os órgãos de pesquisa precisam ter em sua missão institucional ou em seu objetivo social a pesquisa básica ou aplicada de caráter científico, histórico, tecnológico ou estatístico (BRASIL, 2018).

Exemplo: Situações em que o IBGE coleta dados para fundamentar pesquisas demográficas.

e) Execução ou Preparação Contratual

Nessa base legal, o tratamento de dados se dará a pedido do próprio titular para garantir a execução de um contrato ou de seus procedimentos preliminares (TRIPLA, 2019) desde que o tratamento de dados seja imprescindível para a consumação do mesmo.

Exemplo: Quando há contratação de funcionários e é preciso fornecer dados para formalizar o contrato (desde que tenha sido solicitado pelo próprio titular).

f) Exercício Regular de Direito

“Não há necessidade de consentimento para utilizar os dados pessoais da parte ex-adversa num processo judicial, administrativo ou arbitral” (MACIEL, 2019, p. 34).

Essa base legal deve ser usada quando uma parte deseja produzir provas contra a outra dentro de algum dos processos permitidos.

Exemplo: Quando existe a necessidade de processar outra pessoa não é preciso consentimento da parte oposta.

g) Proteção da Vida

O valor da vida humana pode ser tido como um bem jurídico, e a LGPD considera possível o tratamento de dados pessoais em cenários de necessidade de preservação da vida (POHLMANN, 2019).

Exemplo: Em caso de acidente, é possível ter acesso aos documentos da(s) vítima(s).

h) Tutela da Saúde

Profissionais da saúde, serviços de saúde ou sanitários têm autorização legal para tratar dados pessoais que sejam necessários para exercer suas atividades (GET PRIVACY, 2021).

Exemplo: A análise de dados necessária para notificar um paciente sobre o resultado de um exame, ou em uma campanha de vacinação.

i) Legítimo interesse

Atende a interesses legítimos do controlador ou de terceiros, salvo se prevalecerem direitos fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018).

Exemplo: Pesquisas operacionais dentro de uma empresa, quando não há possibilidade de utilização de outra base legal.

j) Proteção do Crédito

Garantia aos órgãos de proteção ao crédito, para que possam incluir dados de consumidores em cadastros positivos, ou caso o titular possua pendências financeiras. (GET PRIVACY, 2021)

Exemplo: Tratamento de dados pessoais realizado pelo Serasa.

A exposição das bases legais em situações da realidade estimula sua compreensão. Existem bases que somente pessoas específicas poderão utilizá-las, como é o caso do estudo por órgãos de pesquisa e de execução de políticas públicas, que é direcionada ao tratamento de dados realizado pelo poder público. É importante analisar as particularidades de cada companhia para escolher a base legal mais adequada, visto que é por meio delas que o tratamento das informações se torna legítimo e justificado.

5.2 Plano de Adequação

O plano de adequação será aplicado no sistema da Fábrica de Tecnologias Turing (FTT), uma organização que possibilita a inclusão de acadêmicos no mercado de trabalho. É um ambiente que proporciona a simulação de uma fábrica de software na prática, juntamente com o desenvolvimento de novas tecnologias. Oferece oportunidade aos alunos de participação em todas as etapas de construção de um projeto, desde o desenvolvimento inicial até a implementação. A FTT atende a projetos da instituição, mas também pode receber projetos de empresas externas através de parcerias. Tem como foco o mercado de trabalho, bem como a atualização tecnológica constante através de pesquisas. O sistema utilizado será o SigTuring, um sistema de gestão acadêmica o qual os funcionários (alunos) utilizam para registrar o horário de entrada e saída, assim como o acompanhamento de projetos.

A análise de conceitos da LGPD permitiu elevar o nível de compreensão sobre seus princípios, bem como suas hipóteses de coleta, as quais foram explicitadas através de exemplos. A pesquisa possibilitou avanço suficiente para estruturar um processo de conformidade mínimo e viável, estipulado em seis principais fases que são percorridas a seguir.

5.2.1 Conscientização

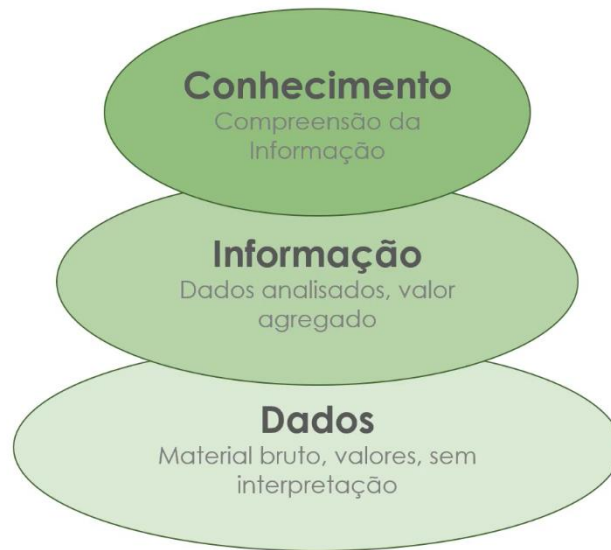
A conscientização é a primeira fase do processo de adequação e uma das mais importantes, pois “a segurança da informação é sempre associada a uma corrente e a escolha do elo mais fraco desta corrente é uma unanimidade: o usuário” (ARAÚJO, 2005, p. 69). Adotar atividades que informem a importância da lei e incentivem boas práticas de segurança dentro da empresa é essencial para a consolidação do plano de conformidade. Com a LGPD em vigor, acrescenta-se mais uma razão para conscientizar os usuários de determinada companhia que agora existe de fato uma regulamentação sobre o tratamento de dados e cada um deve entender seu papel dentro dela (POHLMANN, 2019).

É necessário entender o funcionamento interno do fluxo dos dados, a missão da companhia e a importância dos dados para seu negócio. A primeira etapa para uma conscientização efetiva é introduzir o contexto em que a lei está inserida e o porquê dela ser tão relevante no cenário atual.

5.2.1.1 Porque os Dados são Importantes?

A relevância dos dados vem crescendo significativamente dentro do contexto econômico. Para o cientista de dados Clive Humby, “dados são o novo petróleo”, e quando analisados e processados corretamente agregam valor expressivo. No entanto, ao contrário do petróleo, os dados são uma fonte de recurso inesgotável. “A maior riqueza se encontra não nos dados em si, mas sim na capacidade de usá-los de forma analítica. A inteligência por trás deles é quem determina seu maior valor” (RIPARI, 2019). Os dados em seu estado bruto não agregam muito significado, mas quando associados a outros dados, revelam as mais profundas individualidades. A forma como são avaliados e analisados refletem diretamente em sua extração de valor, conforme a figura 3:

Figura 3: Dados, informação e conhecimento.



Fonte: Palazzo, 2020.

Para Palazzo (2020), os dados são considerados valores binários dentro do ambiente digital e podem ser cadeias de caracteres ou imagens sem nenhuma interpretação. Eles compõem a realidade, mas não levam consigo significado. Por exemplo, o número 220 é um dado, entretanto não informa a grandeza e contexto a que pertence. É apenas um número avulso que sozinho não produz sentido nem representação da realidade. Quando associado a outros dados ou inserido dentro de um contexto, passa a ter significado. Ou seja, 220 volts já é uma informação, a qual associa um valor (dado) a uma grandeza elétrica e agrega valor quando interpretados dentro de um cenário. O conhecimento por sua vez pode ser entendido como a habilidade de compreender a informação e utilizá-la para um determinado fim. O conhecimento referente a 220 volts é que é uma tensão elétrica alta e arriscada para o ser humano, sendo necessário a utilização de ferramentas adequadas para lidar com esse tipo de voltagem.

A aplicação do conhecimento extraído por meio das informações é o fator determinante da utilidade que os dados possam vir a ter, por isso são valiosos quando tratados e analisados de forma correta. Atualmente, dados são os principais ativos de uma organização, pois é através deles que a empresa conhece seu consumidor. Supondo que uma loja de roupas colete dados sobre gênero, idade e estilos mais vendidos. Inicialmente esses dados podem não ter relevância para a empresa, mas depois de processados e analisados, geram rendimentos consideráveis, pois, através deles a organização pode filtrar informações pertinentes a seu público alvo, como o gênero, faixa etária e preferências de moda. Por meio dessas informações pode-se adotar esquemas estratégicos de propaganda e direcionar a publicidade para clientes em potencial. Isto

é, a organização coleta dados que quando relacionados se tornaram informações, e a partir delas, extraíram conhecimento e o transformaram em lucro. Para Toledo (2021, p. 12) “quanto mais as empresas te conhecem, mais elas têm poder de influência sobre seus hábitos”, e isso resulta em geração de lucro através de experiências cada vez mais personalizáveis e atraentes.

Além disso, a essencialidade dos dados para a sobrevivência corporativa se mostra muito presente no cotidiano. De que modo o Facebook e Instagram se tornaram umas das maiores empresas do mundo se os serviços oferecidos ao público são gratuitos? A resposta é clara, por meio dos dados. Segundo Fernandes (2019), aproximadamente 89% do faturamento do Facebook é proveniente de anúncios digitais e publicidades direcionadas, essas que são realizadas com embasamento analítico de dados dos usuários. Logo, o conhecimento obtido para construção de anúncios personalizáveis é transformado em um negócio altamente lucrativo, o que ressalta a importância que os dados têm na sociedade informacional.

5.2.1.2 Porque Regular o Tratamento de Dados?

A propagação de notícias sobre vazamento de dados vem se tornando cada vez mais frequente na atualidade. Os dados pessoais são solicitados constantemente, de forma tanto manual quanto física, e isso pode causar impactos significativos quando essa solicitação não for regulamentada. Um exemplo é a requisição de CPFs em farmácias, que parece ser uma prática inofensiva voltada para aplicação de descontos, mas pode ter como objetivo coletar e reunir dados sobre histórico de compras para propósitos lucrativos. “Com base nesses dados, um plano de saúde pode recusar um contrato ou reajustar a mensalidade” (AMBEP, 2021). A venda de dados para outras empresas se tornou uma grande fonte de monetização.

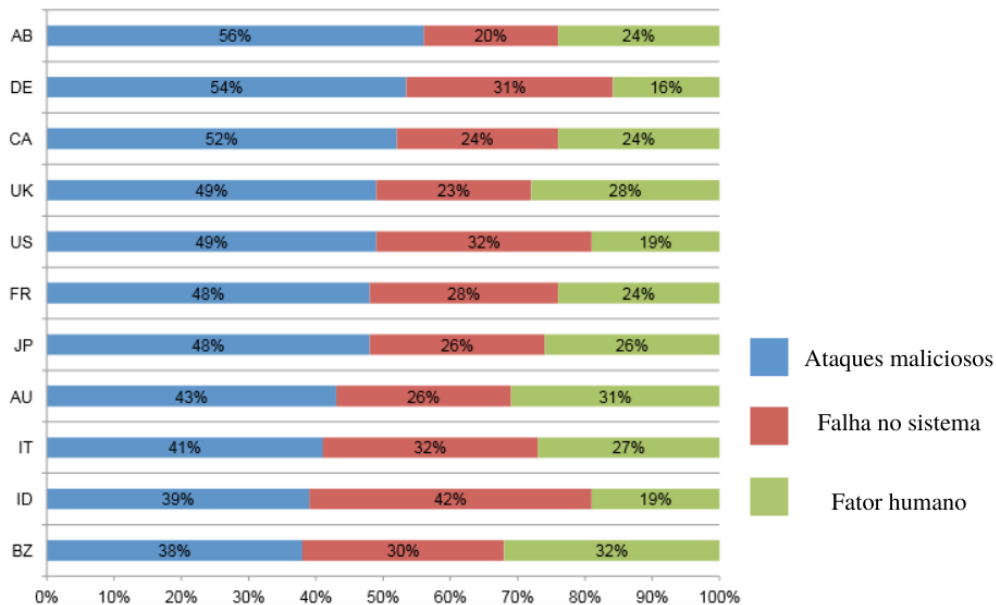
Dados pessoais podem ser considerados traços da personalidade, e quando associados a outros dados são capazes de revelar não só a identidade de uma pessoa como também seus gostos e preferências, o que pode resultar em manipulação de escolhas. Uma demonstração foi o escândalo em 2018 envolvendo o Facebook e a empresa de marketing Cambridge Analytica, a qual coletou dados de forma totalmente ilegítima com o objetivo de utilizá-los em campanhas políticas. “O mecanismo teria permitido entender os traços comportamentais dos eleitores para oferecer-lhes propaganda política com mais chances de êxito” (ALVES, 2018). Através de um simples teste de personalidade, cerca de 50 milhões de pessoas tiveram as informações vazadas com o intuito de influenciar sua decisão política. Após o acontecimento, o fundador do Facebook Mark Zuckerberg começou a empregar diversas medidas para preservar o usuário, como o direito de desvincular a conta da rede social de outras aplicações e sites, visto que foi

um desses aplicativos de perguntas e respostas que estava roubando dados não só do usuário em questão mas ainda de seu ciclo de amizade (CARVALHO e TAGLIAFERRO, 2020).

É evidente que a análise de dados algorítmica afeta as ações do usuário no sistema. “Com os dados coletados do cliente, tenta-se mapear o comportamento do consumidor, por exemplo: onde clicou, como se comportou na rede e o que o levou a uma decisão de compra” (OLIVEIRA, 2020), podendo ofertar a longo prazo produtos e serviços pertinentes a sua opção. O caso da Cambridge Analytica foi a alavanca que deu início a discussões sobre o poder de influência que um algoritmo pode ter nas decisões pessoais. Isso reforça a importância do cuidado durante o manuseio e fornecimento de dados, visto que sua utilização desenfreada pode afetar até mesmo a democracia.

Um estudo em parceria pela IBM e o Instituto Ponemon em 2016 mostra as principais causas de vazamento de dados. A pesquisa contou com a participação de 350 empresas de 12 países: Alemanha, Austrália, Brasil, Canadá, Estados Unidos, França, Japão, Índia, Itália, Reino Unido, Arábia Saudita e Emirados Árabes Unidos (as duas últimas nações são organizadas dentro da “Região Árabe” no estudo). A análise levou em consideração três grandes fatores como causadores do vazamento de dados na empresa: ataques virtuais, falhas de sistema e erro de funcionários, conforme a figura 4:

Figura 4: Principais causas de vazamentos de dados nas empresas.



Fonte: Adaptado. Held, 2016.

Observa-se que a estatística brasileira pode ser alarmante para as empresas nacionais, visto que, de todas as nações participantes da pesquisa, o Brasil é o detentor do maior índice de erros ocasionados por contribuintes da própria organização (32%). Isso evidencia ainda mais a

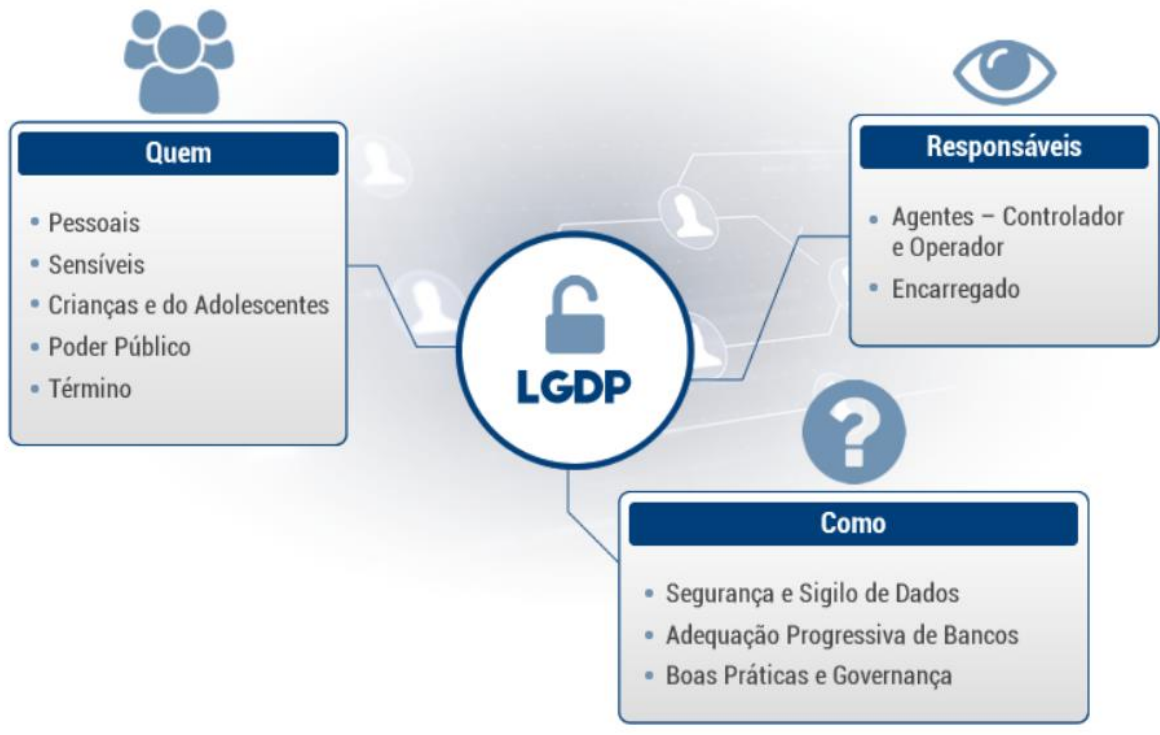
relevância de conscientizar os usuários sobre o poder que os dados têm e as consequências de um vazamento. “Um usuário despreparado é uma ameaça constante à segurança da organização, aos seus ativos, e, por conseguinte, aos titulares de dados tratados pela organização” (PHOLMANN, 2019, p. 94). É essencial adotar medidas preventivas, tanto de reforço da segurança do sistema quanto de incentivo e boas práticas de colaboradores, pois, apesar de a falha humana no Brasil ser maior do que em outros países, os ataques maliciosos ainda são as principais causas de quebra de sigilo de informações privadas.

5.2.1.3 Apresentação da Lei

A Lei Geral de Proteção de Dados foi criada com a finalidade de garantir o respeito à privacidade e a autodeterminação informativa, juntamente com o desenvolvimento da pessoa natural (BRASIL, 2018). Sua extensão varia de um simples currículo impresso com diversos dados pessoais até o banco de dados mais robusto e completo de uma corporação.

Para introduzir a LGPD na companhia em questão, foi realizado um seminário com o intuito de esclarecer as principais premissas da lei e a importância de implementá-la. Foram analisados os princípios e as bases legais já citados anteriormente, bem como as sanções previstas em caso de descumprimento. Além disso, foi realizada uma discussão de exemplos voltados para estimular a compreensão, definindo quem serão seus responsáveis e quais tipos de dados a lei tratará, conforme a figura 5:

Figura 5: LGPD – Responsáveis, Quem e Como.



Fonte: Cenofisco, 2021.

Em síntese, a LGPD regulamenta todas as formas de tratamento de dados, sejam eles pessoais, sensíveis, de crianças e adolescentes ou tratados pelo Poder Público. Também abordará o descarte de forma correta, visando proporcionar a segurança e sigilo do descarte dessas informações. Exigirá a adequação gradativa de bancos juntamente com a elaboração de documentos que comprovem a legitimidade do uso dos dados e a execução de boas práticas de segurança e governança. As pessoas responsáveis pelo cumprimento da lei serão o controlador e o operador, e quem ficará responsável pelo intermédio de comunicação com o órgão fiscalizador será o encarregado.

5.2.2 Mapeamento de Dados

O mapeamento de dados é o ponto de partida para entender melhor o funcionamento do fluxo dos dados dentro de uma organização. O objetivo dessa fase é identificar de fato as principais contingências da companhia, acompanhando todo o caminho que os dados percorrem. Para Donda (2020, p. 45): “Esse é o mais importante e complexo processo de adequação da LGPD, pois os dados são o ativo-alvo para o tratamento correto e devemos saber inicialmente onde estão localizados”. Nesta fase encontra-se a origem dos dados, sua categoria e se eles realmente são necessários para atingir tal finalidade. É importante destacar que o mapeamento inicial é feito com o intuito de encontrar divergências, e deve constar como os dados se encontram no presente estado da organização, mesmo que inadequados. Deve-se fazer perguntas questionando qual a base legal que legitima o tratamento daquele dado e quem terá acesso a eles, conforme o quadro 2:

Quadro 2: Mapeamento Inicial Geral – Fábrica de Tecnologias Turing

MAPEAMENTO INICIAL GERAL – FÁBRICA DE TECNOLOGIAS TURING		
Tema	Orientação	Resposta
Finalidade	A finalidade deverá ser clara e objetiva e definir o motivo pelo qual os dados estão sendo coletados.	Cadastro no sistema de ponto
Origem	Apontar as principais origens dos dados, ou seja, as entradas e meios de coleta de dados (site, locais físicos, aplicativos.)	Coleta digital através do sistema da universidade
Dados	Quais dados foram coletados de fato para aquela finalidade.	Nome, data de nascimento, CPF, RG, telefone, e-mail, endereço, sexo, estado civil
Categoria	Indica se os dados coletados se encaixam em dados comuns ou dados sensíveis.	Nenhuma

Base Legal	Indicar a base legal da LGPD que torna o tratamento de dados legítimo.	Nenhuma
Compartilhado com outras empresas	Indicar as companhias parceiras em que há o compartilhamento de dados.	Não
Dados de crianças e adolescentes	Identificar se nos dados analisados há a coleta de dados de pessoas menores de idade (18 anos incompletos).	Sim
Transferência internacional de dados	Verificar a transferência de dados pessoais para empresas localizadas fora do país.	Não
Localidade do tratamento	Localidade geográfica de onde ocorre o tratamento de dados.	Anápolis, Goiás, Brasil
Onde estão armazenados	Onde os dados serão mantidos.	Banco de dados corporativo
Quem tem acesso	Todos os que conseguem visualizar, editar ou excluir dados.	Scrum Master, líder técnico e professores orientadores
Titular dos dados	Aquele que possui seus dados como objeto de tratamento.	Funcionários
Ambiente de tratamento	Âmbito em que os dados são tratados. Físico, digital ou ambos.	Digital
Tempo de vida	Prazo em que os dados são mantidos na organização até atingir sua finalidade.	Não descartados
Direito dos titulares	Verificar se os direitos dos titulares estão explícitos referente ao tratamento de dados realizado	Não

5.2.2.1 Avaliação de Riscos

A avaliação de riscos é realizada juntamente com o mapeamento de dados, visando detectar as principais ameaças e vulnerabilidades que as informações podem ter dentro do sistema. Além disso, o princípio da prevenção da LGPD ressalta a importância de identificar e prevenir a ocorrência dessas ameaças como resultado do tratamento de dados. Para Donda (2020, p. 87): “A avaliação e a análise de riscos são muito importantes para dar visibilidade à situação dos ativos, assim como priorizar os investimentos e proteger os ativos da melhor maneira”. Assim como o mapeamento de dados, a avaliação de riscos auxilia no controle de divergências e contribui para a preservação dos patrimônios organizacionais. Será dividido em fases, sendo elas:

a) Definição de um processo:

O processo utilizado será o fluxo abordado no mapeamento de dados, o qual consta os dados dos funcionários da Fábrica de Tecnologias Turing.

b) Identificação e avaliação de riscos:

Para identificar os riscos foi utilizada a matriz de Probabilidade x Impacto disponibilizada pelo Governo Digital, que serve como mecanismo de apoio para estabelecer os parâmetros de classificação dos níveis de risco.

Figura 6: Matriz de Probabilidade x Impacto.

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Fonte: Governo Digital, 2021.

Os critérios escalares estabelecidos são definidos em baixo, moderado e alto, com valores correspondentes 5, 10 e 15, conforme a figura 7:

Figura 7: Critérios de nível de risco.

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

Fonte: Governo Digital, 2021.

À medida em que os riscos são identificados, define-se a probabilidade de ocorrência dele e o impacto causado se esse risco ocorrer. Depois, multiplicam-se os dois valores, que irão resultar no nível de risco para cada evento. A identificação de riscos foi realizada na empresa juntamente com o controlador dos dados, o qual possui maior propriedade sobre os riscos que ameaçam a integridade das informações.

Tabela 1: Identificação e avaliação dos riscos

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	5	10	50
R02	Modificação não autorizada.	5	5	25
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	10	50
R06	Coleção excessiva.	5	5	25
R07	Informação insuficiente sobre a finalidade do tratamento.	15	5	75
R08	Tratamento sem consentimento do titular dos dados pessoais.	15	15	225
R09	Falha em considerar os direitos do titular dos dados pessoais.	15	10	150
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	5	5	25
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	10	50
R14	Reidentificação de dados pseudonimizados.	5	5	25

Fonte: Adaptado. Governo Digital, 2021.

c) Identificação de medidas para o tratamento dos riscos. É necessário definir uma resposta ao risco, sendo elas:

- Evitar: Não iniciar ou continuar com a atividade que causa o risco;
- Aceitar: Baixo impacto e/ou baixa probabilidade;
- Compartilhar: Dividir os riscos com outros setores;
- Reduzir: Realizar ações para mitigar os riscos.

Tabela 2: Identificação 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.	Aceitar	5	10	50	Sim
	2. Desenvolvimento Seguro.					
	3. Monitoramento de logs.					
R02 Modificação não autorizada.	1. Monitoramento de logs.	Aceitar	5	5	25	Sim
R03 Perda.	1. Monitoramento dos dados.	Reduzir	5	15	75	Sim
	2. Ferramentas de segurança.					
R04 Roubo.	1. Controle de acesso.	Reduzir	5	15	75	Sim
	2. Controles criptográficos.					
R05 Remoção não autorizada.	1. Controle de acesso.	Aceitar	5	10	50	Sim
	2. Monitoramento de logs.					
R06 Coleção Excessiva.	-	Evitar	5	5	25	Sim

R07	Informação insuficiente sobre a finalidade do tratamento.	-	Evitar	15	5	75	Sim
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	1. Documentação contendo os termos sobre o tratamento dos dados utilizados.	Reduzir	15	15	225	Sim
		2. Solicitar consentimento antes do tratamento ser realizado.					
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	1. Identificar os direitos do titular.	Reduzir	10	10	100	Sim
		2. Monitoramento do processo de tratamento.					
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	-	Evitar	5	5	25	Sim
R11	Retenção prolongada de dados pessoais sem necessidade.	1. Definição de prazos referente aos dados que ficarão armazenados.	Reduzir	5	5	25	Sim
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	-	Aceitar	5	15	75	Sim

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.).	1.Validação dos dados de entrada.	Aceitar	5	10	50	Sim
	2.Monitoramento dos dados.					
R14 Reidentificação de dados pseudonimizados.	-	Aceitar	5	5	25	Sim

Fonte: Adaptado. Governo Digital, 2021.

5.2.3 Diagnóstico

O diagnóstico é a etapa responsável por encontrar lacunas e áreas de divergência com a lei. Para Toledo (2021, p. 75): “O objetivo desta fase é identificar os principais pontos de desconformidade com a legislação, através do mapeamento de dados feito na fase anterior”. Nesse momento é identificado se o que a empresa tem feito e como tem feito, está de acordo com os parâmetros estabelecidos pela LGPD. É realizada a análise da avaliação de riscos e do mapeamento de dados, visando apontar recursos pertinentes. As principais áreas de divergência são:

- a) Ao analisar o mapeamento, percebe-se que os dados atualmente não são categorizados na organização, dificultando saber a existência do tratamento de dados sensíveis. É necessário averiguar, se, para a finalidade de cadastrar um novo funcionário no sistema, existe realmente a necessidade de coleta de dados sensíveis de acordo com os termos da lei. É preciso analisar todos os dados recolhidos para aquela finalidade e verificar se algum deles é considerado sensível. Caso não seja, a organização deve categorizar o tratamento somente com dados pessoais;
- b) Não existe uma base legal definida que torne o tratamento de dados legítimo. É imprescindível encaixar o tratamento de dados em uma das bases legais disponíveis, definindo uma delas para cada finalidade que houver;
- c) A organização também realiza o tratamento de dados de pessoas menores de idade, visto que pode vir a acontecer a entrada de um aluno com os 18 anos incompletos. Quando esse for o caso, a LGPD exige que seja solicitado o consentimento dos pais ou responsável legal, e que a companhia mantenha pública a informação sobre os tipos de dados coletados, assim como sua utilização;
- d) É preciso definir um tempo limite para armazenamento dos dados, já que a organização não conta com uma política de descarte;
- e) Não existe um documento informando os direitos dos titulares;
- f) Não existem papéis bem definidos sobre os responsáveis por cumprir a lei;

- g) Não há incentivo à execução de boas práticas para proteção dos dados;
- h) A organização possui um risco de alto nível sobre o tratamento de dados sem o consentimento do titular, sendo fundamental informá-lo sobre o que acontece com seus dados a partir do momento em que são coletados;
- i) Os direitos dos titulares não estão sendo considerados, já que é necessário identificá-los e informá-los anteriormente.

Além dos principais pontos de divergência encontrados, também é necessário identificar medidas de mitigação de riscos, como o controle de acesso e a adoção de ferramentas de apoio que reforcem a proteção dos dados. Ademais, a organização não conta com uma política de privacidade que informe quais são os direitos dos titulares e outras questões que precisam ser esclarecidas e transparentes. Além do incentivo a boas práticas de segurança e privacidade, sugere-se a adoção de mecanismos que auxiliem na proteção das informações em relação aos riscos, como perda e destruição.

5.2.4 Planejamento

Depois de identificadas todas as divergências através do diagnóstico, é necessário planejar quais e como serão implementadas as atividades e documentos necessários para conformidade com a lei. Para Toledo (2021, p.76) “O objetivo dessa fase é planejar a forma de execução das soluções propostas na fase anterior, criando um plano de ação e um cronograma de execução”. É preciso colocar como prioridade as áreas que apresentam maior risco ou desconformidade com a lei, levando em consideração os recursos e ferramentas disponíveis. É necessário montar um cronograma estratégico que aborde todas as atividades elencadas, executando-as de acordo com suas dependências, conforme o quadro 3:

Quadro 3: Planejamento de atividades.

ATIVIDADE	Setembro 2021				Outubro 2021			
	1ª semana	2ª semana	3ª semana	4ª semana	1ª semana	2ª semana	3ª semana	4ª semana
Categorização de Dados	x							
Definição de Base Legal		x						
Definição de política de descarte			x					
Elaboração da Política de Privacidade explicitando o tratamento de dados e os direitos do titular				x	x			
Elaboração do termo de autorização para menores de 18 anos					x			
Elaboração do documento de definição de papéis						x		
Elaboração do código de sugestão de boas práticas							x	
Proposta de ferramenta								x

Fonte: Autor, 2021.

5.2.5 Implementação

Após o mapeamento e diagnóstico dos problemas encontrados, é necessário elaborar e efetivar as atividades elencadas. A implementação é a execução das soluções descobertas para as divergências identificadas na fase de diagnóstico. Para Toledo (2021, p 76): “O objetivo dessa fase é colocar em prática todo o plano de ação estabelecido na fase anterior, incluindo a elaboração de todos os documentos que se fizerem necessários”. A princípio, adequa-se o mapeamento feito inicialmente por meio da definição da base legal e dos demais procedimentos de conformidade, resultando em uma versão final adequada. Após realizar as correções, inicia-se a produção dos documentos, visando desenvolvê-los de forma correta e transparente.

Quadro 4: Mapeamento Final Geral – Fábrica de Tecnologias Turing.

MAPEAMENTO FINAL GERAL – FÁBRICA DE TECNOLOGIAS TURING		
Tema	Orientação	Resposta
Finalidade	A finalidade deverá ser objetiva e definir o motivo pelo qual os dados estão sendo coletados.	Cadastro no sistema do ponto
Origem	Apontar as principais origens dos dados, ou seja, as entradas e meios de coleta de dados (site, locais físicos, aplicativos.)	Coleta digital através do sistema da universidade
Dados	Quais dados foram coletados de fato para aquela finalidade.	Nome, data de nascimento, CPF, RG, telefone, e-mail, endereço, sexo, estado civil
Categoria	Indica se os dados coletados se encaixam em dados comuns ou dados sensíveis.	Comum
Base Legal	Indicar qual a base legal da LGPD que torna o tratamento de dados legítimo.	Execução ou preparação contratual

Compartilhado com outras empresas	Indicar as companhias parceiras em que há o compartilhamento de dados.	Não
Dados de crianças e adolescentes	Identificar se no fluxo analisado há a coleta de dados pessoais de menores de idade (18 anos incompletos).	Sim
Transferência internacional de dados	Verificar a transferência de dados pessoais para empresas localizadas no exterior.	Não
Localidade do tratamento	Localidade geográfica de onde ocorre o tratamento de dados.	Anápolis, Goiás, Brasil
Onde estão armazenados	Onde os dados serão mantidos.	Banco de dados corporativo
Quem tem acesso	Todos os que conseguem visualizar, editar ou excluir dados.	Scrum Master, líder técnico e professores orientadores
Titular dos dados	Aquele que possui seus dados como objeto de tratamento.	Funcionários
Ambiente de tratamento	Âmbito em que os dados são tratados. Físico, digital ou ambos.	Digital
Tempo de vida	Prazo em que os dados são mantidos na organização até atingir sua finalidade.	6 meses após o desligamento do titular
Direito dos Titulares	Verificar se os direitos dos titulares estão explícitos referente ao tratamento de dados realizado	Sim

Fonte: Autor, 2021.

Depois de categorizar todos os dados e encontrar uma base legal que torna seu tratamento válido, a próxima atividade realizada foi a produção dos principais documentos para estar de acordo com a LGPD. É essencial ressaltar que os documentos elaborados possuem caráter recomendatório, o que significa que as atividades propostas são sugestões de como ficar em conformidade com a lei e cabe à organização adotar de fato esses processos. Todos os

documentos que se fizeram necessários de elaboração na fase de planejamento estarão disponíveis como apêndices para consulta. A primeira tarefa realizada foi definir um tempo para eliminação dos dados, já que a companhia não estabelecia um prazo limite. Com o auxílio de orientadores da empresa foi elaborada uma política de descarte, visando descrever as hipóteses em que os dados serão excluídos. A política de descarte está disponível no apêndice B e foi dividida entre as disposições gerais para a exclusão dos dados, as hipóteses para o descarte adequado e seguro e os direitos do titular. As circunstâncias definidas para o descarte são mediante a solicitação do titular e por meio de seu desligamento total com a organização, depois que a finalidade para qual os dados foram coletados for devidamente atingida.

Visando proporcionar transparência com os titulares dos dados, foi elaborada uma política de privacidade voltada para esclarecimento sobre quais são os direitos como proprietário dos dados e o modo como podem exercê-los. O documento descreve a empresa em questão e contém informações sobre:

- a) A quem a política é aplicada;
- b) Quais dados são coletados, como e por que são coletados;
- c) Tratamento de dados sensíveis;
- d) Compartilhamento de dados com terceiros, bem como a transferência internacional de dados;
- e) Tempo de armazenamento;
- f) Medidas para manter os dados seguros;
- g) Tratamento de dados de menores de idade;
- h) Base legal do tratamento de dados;
- i) Direitos dos titulares e como exercê-los;
- j) Alteração da política de privacidade;
- k) Responsabilidade;
- l) Isenção de responsabilidade.

A política de privacidade tem o intuito de informar ao titular o processo do tratamento de seus dados na organização, e foi formulada com embasamento no manual da LGPD proposto pela advogada Mariana de Toledo (2021). A política está disponível para consulta no apêndice C e tem como foco a transparência com o titular, com informações claras e precisas sobre a organização em si e sobre o que acontece com os dados lá dentro, além de possuir informações de contato caso seja necessário para atualização ou correção de algum dado obsoleto. Todos os

itens elencados no documento têm o propósito de comunicar a forma de gestão das informações e objetiva criar um canal de confiança mútua.

O próximo documento elaborado foi o termo de autorização para aqueles alunos que desejarem ingressar na companhia e não tiverem 18 anos completos. Por se tratar de um curso superior, a entrada de menores de idade acontece de forma esporádica, no entanto as exceções não podem ser tratadas como maioria. Por este motivo foi produzido o termo de autorização, presente no apêndice E, que visa informar a manifestação livre e inequívoca pela qual o responsável legal do titular dos dados concorda que a organização trate seus dados para uma finalidade específica. O documento também expressa como e quais dados são coletados, além de outras perguntas pertinentes.

A documentação sobre os papéis da LGPD ficou registrada somente com o esclarecimento das atividades realizadas pelo controlador, visto que existem situações em que o controlador e o operador são a mesma pessoa. Quanto ao encarregado, de acordo com a minuta de resolução publicada pela ANPD sobre a aplicação da lei para os agentes de tratamento, em seu Art. 13 da seção V, “os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD” (Governo do Brasil, 2021, p.5), logo, produziu-se exclusivamente o documento de identificação do controlador e de suas diferentes funções, disponibilizado no apêndice A.

Visando reforçar a proteção das informações, foram elencadas algumas atividades de boas práticas com o intuito de evitar perda ou roubo de dados causados por imprudência dos próprios funcionários. Além do incentivo à execução de técnicas adequadas para proteger os dados de pessoas mal-intencionadas, sugere-se a adoção de no mínimo uma ferramenta apta a proporcionar algum tipo de segurança. Junto com as atividades de boas práticas existe uma proposta de ferramenta para agendamento de backup disponível no apêndice D, que tem por objetivo diminuir os riscos relacionados com a perda de informação.

5.2.6 Monitoramento

O monitoramento tem o intuito de proporcionar uma melhoria contínua na esfera corporativa por meio do acompanhamento constante de cumprimento da LGPD. Para Toledo (2021, p. 77):

Essa fase tem o objetivo de manter um monitoramento constante do cumprimento das diretrizes estabelecidas no programa de governança em proteção de dados, fazer as atualizações que se fizerem necessárias e garantir que a organização se mantenha em conformidade.

Para um efetivo controle de observância da lei, sempre que a organização receber novos dados para tratamento, estes devem ser categorizados e submetidos a uma base legal. Caso a companhia opte por tratar esses dados para uma finalidade diferente do cadastro no sistema, essa alteração deve ser informada ao titular antes da coleta. Além disso, qualquer mudança referente ao tratamento de dados deve ser explícita e esclarecida. Na política de privacidade existe um item que reserva o direito de modificação por consequência de futuras adequações do sistema ou por mudanças no cenário legislativo. O controle de observância da lei também engloba a atualização constante de sistemas, principalmente de banco de dados e de ferramentas de segurança.

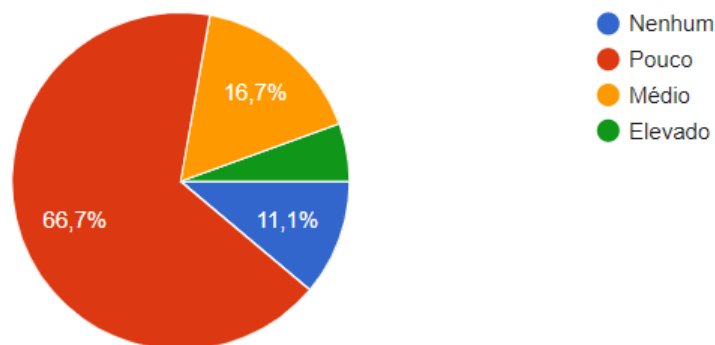
6 RESULTADOS ALCANÇADOS

A pesquisa realizada proporcionou grande avanço não só no cenário corporativo como também no conhecimento sobre a LGPD por parte dos colaboradores. É extremamente importante ressaltar que o intuito da pesquisa é contextualizar e esclarecer a Lei Geral de Proteção de Dados em razão do crescente número de pessoas físicas e jurídicas inadimplentes com a legislação, assim como definir um processo mínimo voltado para adoção do estado de conformidade. Dentro da fase de conscientização, foi realizada uma palestra para os colaboradores da companhia, com o objetivo de mostrar o valor que os dados têm para a sociedade informacional, a importância de regulamentar o tratamento desses dados e a apresentação da LGPD. A organização contava com um total de 21 funcionários, os quais 18 deles estavam presentes na apresentação. Foram discutidas as principais causas de vazamento de dados no mundo e a importância de sensibilizar os funcionários de que a proteção de suas informações pessoais pode evitar danos diversos. Ao final da palestra, foi produzido um questionário indagando se já havia conhecimento prévio da legislação e se os conceitos apresentados permitiram elevar o nível de compreensão sobre a LGPD, com o objetivo de implantar realmente uma cultura de proteção de dados na empresa.

Figura 8: Pergunta 1 sobre a compreensão dos conceitos da LGPD

Como você avalia sua compreensão sobre a LGPD antes dos conceitos apresentados?

18 respostas

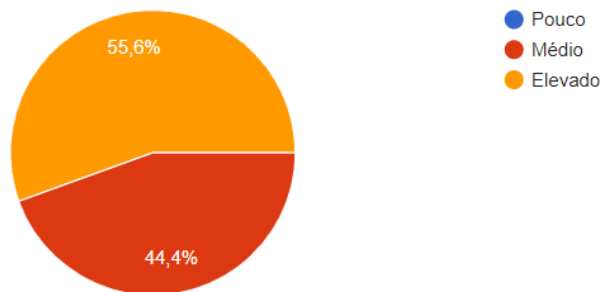


Fonte: Autor, 2021.

Ao observar a figura 8, percebe-se que 11,1% dos colaboradores demonstraram não ter nenhum conhecimento prévio sobre a LGPD, e isso ressalta a escassez de conhecimento sobre a legislação mesmo depois dela já ter entrado em vigor. Observa-se que mais da metade dos funcionários relataram ter pouca compreensão sobre a lei, totalizando quase 67% de pessoas

com entendimento raso, o que evidencia ainda mais a necessidade de esclarecimento. Apenas 5,3% de pessoas relataram ter uma noção elevada sobre a lei, sendo que 16,7% ainda se consideravam medianos. Os conceitos apresentados possibilitaram o acesso a várias informações úteis dentro do contexto da LGPD, tal qual seus princípios e sanções administrativas. A análise de exemplos das bases legais permitiu elucidar as hipóteses de coleta e associá-las a situações corriqueiras e de fácil entendimento, tendo sempre como foco o aumento de noção sobre a lei, conforme a figura 9:

Figura 9: Pergunta 2 sobre a compreensão dos conceitos da LGPD.
Como você avalia sua compreensão sobre a LGPD depois dos conceitos apresentados?
18 respostas



Fonte: Autor, 2021.

Entende-se que a explicação das principais diretrizes da legislação, a exibição de casos reais de vazamento de dados e a análise de exemplos das bases legais resultaram em um aumento significativo do nível de compreensão sobre a LGPD. Nota-se que nenhum colaborador se considera pouco conhecedor da legislação depois dos conceitos expostos, o que destaca ainda mais a validade que a fase de conscientização possui. Dos 18 funcionários participantes, 44,4% se consideram com um conhecimento mediano sobre a lei depois de serem apresentados a suas diretrizes, e 55,6% votaram que agora possuem conhecimento elevado através dos conceitos retratados. É importante ressaltar que o questionário não valida a efetividade da LGPD entre os funcionários, no entanto deixa em evidência o aumento do grau de percepção de suas diretrizes centrais. A expansão do conhecimento sobre a LGPD fomenta a implantação de uma cultura de proteção de dados voltada para a preservação da privacidade na empresa, e foi de extrema importância para o levantamento de pesquisa realizado.

Na fase de mapeamento, produziu-se o mapa dos dados do estado atual em que aquela organização se encontrava. Após a identificação das principais áreas de desconformidade e os

devidos procedimentos de adequação e categorização, as informações foram mapeadas novamente visando produzir um mapeamento geral adequado, conforme a figura 10:

Figura 10: Comparativo entre os mapeamentos inicial e final.

MAPEAMENTO INICIAL GERAL - FTT		MAPEAMENTO FINAL GERAL - FTT	
Tema	Resposta	Tema	Resposta
Finalidade	Cadastro no sistema do ponto	Finalidade	Cadastro no sistema do ponto
Origem	Coleta digital através do site da universidade	Origem	Coleta digital através do site da universidade
Dados	Nome, data de nascimento, CPF, RG, telefone, e-mail, endereço, sexo, estado civil	Dados	Nome, data de nascimento, CPF, RG, telefone, e-mail, endereço, sexo, estado civil
Categoria	Nenhuma	Categoria	Comum
Base Legal	Nenhuma	Base Legal	Execução ou preparação contratual
Compartilhado com outras empresas	Não	Compartilhado com outras empresas	Não
Dados de crianças e adolescentes	Sim	Dados de crianças e adolescentes	Sim
Transferência internacional de dados	Não	Transferência internacional de dados	Não
Localidade do tratamento	Anápolis, Goiás, Brasil	Localidade do tratamento	Anápolis, Goiás, Brasil
Onde estão armazenados	Banco de dados corporativo	Onde estão armazenados	Banco de dados corporativo
Quem tem acesso	Scrum Master, líder técnico e professores orientadores	Quem tem acesso	Scrum Master, líder técnico e professores orientadores
Titular dos dados	Funcionários	Titular dos dados	Funcionários
Ambiente de tratamento	Digital	Ambiente de tratamento	Digital
Tempo de vida	Não descartados	Tempo de vida	6 meses após o desligamento do titular
Direito dos Titulares	Não	Direito dos Titulares	Sim

Fonte: Autor, 2021.

As partes em destaque no mapeamento final geral representam as mudanças realizadas para aproximar a organização de um estado de maior conformidade. Depois de obter todos os dados tratados pela companhia, eles foram classificados como dados pessoais comuns, não havendo a existência de dados sensíveis naquele fluxo. Posteriormente, definiu-se a base legal para tornar aquele tratamento de dados legítimo e informado ao titular. Observou-se que existe a possibilidade mínima de tratamento de dados de menores de 18 anos, tornando necessária a obtenção da concordância do responsável legal, que será adquirida por meio do termo de autorização para menores de idade, elaborado durante o processo de adequação. Além do termo de autorização, produziu-se a política de descarte dos dados, estipulando um tempo para que os mesmos fossem eliminados de acordo com os critérios da lei. Ademais, os direitos dos titulares foram apresentados juntamente com um e-mail de contato para corrigi-los caso necessário.

Todas as informações pertinentes ao tratamento dos dados foram esclarecidas através da elaboração da política de privacidade, a qual descreve o objetivo da organização, a finalidade de coleta dos dados, as medidas de segurança adotadas e outros itens relevantes para o cumprimento da transparência com o proprietário dos dados. Na fase de implementação, com o objetivo de definir os papéis necessários para concordância com a LGPD, estruturou-se um documento de identificação do controlador, agente de tratamento responsável pelas decisões referentes às informações coletadas. Por se tratar de uma companhia de pequeno porte, a empresa não conta com duas pessoas diferentes para as funções de controlador e operador, sendo o mesmo funcionário para decidir sobre o tratamento de dados e realizá-los de fato. O documento contém a identificação do controlador bem como suas funções e canal para contato. O encarregado dos dados, que é a pessoa indicada pelo controlador para atuar como via de comunicação entre o titular, o controlador e a ANPD, não foi elencado dentro do processo de adequação, visto que em agosto de 2021 a ANPD publicou no site do governo uma minuta para os agentes de tratamento de empresas de pequeno porte, a qual dispensa a obrigação de indicar alguém para atuar como intermediário de comunicação. “O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados” (Governo do Brasil, 2021, Art. 13 seção V). A via de interação com o titular de dados foi disponibilizada em todos os documentos elaborados.

O processo de adequação abordado visa aproximar a organização de um estado maior de conformidade com a LGPD não só através da elaboração dos documentos que proporcionam a transparência com o titular, como também por meio do incentivo a execução de boas práticas para proteção dos dados e pela proposta de uma ferramenta que fomente essa segurança. Ainda na fase de implementação, formulou-se um breve guia de boas práticas com o objetivo de instruir uma navegação de forma segura na internet e evitar o vazamento de informações ocasionadas pelos próprios funcionários da empresa. Além disso, sugeriu-se a adoção de um software para agendamento de backup, explicando inclusive seu funcionamento.

Se a organização acatar efetivamente todos os documentos produzidos e sugestões elaboradas, o processo de adequação diminui significativamente as ameaças elencadas na avaliação dos riscos, visto que a companhia contava com riscos de níveis altos, principalmente no tocante a transparência com o titular, conforme a figura 11:

Figura 11: Comparativo entre avaliação de riscos.

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)	Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	5	10	50	R01	Acesso não autorizado.	5	10	50
R02	Modificação não autorizada.	5	5	25	R02	Modificação não autorizada.	5	5	25
R03	Perda.	5	15	75	R03	Perda.	5	10	50
R04	Roubo.	5	15	75	R04	Roubo.	5	10	50
R05	Remoção não autorizada.	5	10	50	R05	Remoção não autorizada.	5	10	50
R06	Coleção excessiva.	5	5	25	R06	Coleção excessiva.	5	5	25
R07	Informação insuficiente sobre a finalidade do tratamento.	15	5	75	R07	Informação insuficiente sobre a finalidade do tratamento.	5	5	25
R08	Tratamento sem consentimento do titular.	15	15	225	R08	Tratamento sem consentimento do titular.	5	15	75
R09	Falha em considerar os direitos do titular.	15	10	150	R09	Falha em considerar os direitos do titular.	5	10	50
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular.	5	5	25	R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular.	5	5	25
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50	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	R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75

Fonte: Autor, 2021.

Constata-se que após as devidas sugestões e documentação elaborada, as medidas de mitigação de riscos se mostraram efetivas para o programa de adequação, visto que houve uma diminuição significativa nas ameaças. Com a implementação da ferramenta de agendamento de backup “SQLBackupAndFTP” diminui-se de 15 para 10 o impacto causado tanto para perda das informações quanto para roubo. A ferramenta cria uma rotina gerenciável de definição dos backups e possui alto nível de usabilidade. Além disso, é compatível com SQL Server, PostgreSQL, MySQL, Azure SQL e Amazon RDS SQL. Os riscos 7, 8 e 9 foram sanados através da documentação produzida, visto que agora por meio da política de privacidade a taxa de falha de considerar os direitos do titular é mínima, assim como a possibilidade de o titular ter informações insuficientes sobre a finalidade do tratamento de seus dados. O risco de tratar os dados sem o consentimento de seu proprietário também diminuiu, já que na base legal elencada o tratamento das informações ocorre a pedido do próprio titular.

Nota-se que as soluções listadas durante o processo de adequação nas fases de conscientização, mapeamento e implementação apresentaram resultados significativos para a pesquisa, como fruto do processo de conformidade mínimo estabelecido.

7 CONCLUSÃO E CONSIDERAÇÕES FINAIS

A Lei Geral de proteção de Dados foi promulgada com o intuito de proteger a privacidade dos dados e proporcionar transparência diante do titular, e tanto pessoas jurídicas quanto pessoas físicas (que tratem dados com viés econômico) precisam estar em conformidade. Entretanto, diversas companhias apresentaram dificuldades em adotar um processo de adequação, visto que a lei é extensa e complexa. Estudos apontam a existência de pessoas que nunca ouviram falar sobre a LGPD, e empresas que sequer iniciaram o processo de adequação. Visando esclarecer e auxiliar na implementação da lei por meio de fases ordenadas, foi apresentado um processo mínimo de conformidade, que conta com a descrição de cada fase, os conceitos da lei e a importância de adotá-la.

O processo mínimo de adequação contribuiu significativamente para o conhecimento e implementação da LGPD na empresa. O entendimento da temática proposta foi ampliado a partir do estudo, o qual possibilitou a solução de determinados problemas. A LGPD possui três papéis principais, sendo o de controlador, operador e encarregado. No entanto, por meio da pesquisa realizada foi possível perceber que as corporações de pequeno porte têm maior necessidade de identificação meramente do controlador (observados os demais princípios da lei e particularidades de cada companhia), visto que nem sempre serão duas pessoas diferentes para decidir sobre o tratamento dos dados (controlador) e realizá-lo de fato (operador). Além disso, no dia 30 de agosto de 2021, a ANPD, que é o órgão responsável pela fiscalização da LGPD, publicou no site do governo uma minuta de resolução da aplicação da lei para órgãos de pequeno porte, isentando organizações pequenas da obrigação de indicar um encarregado dos dados pessoais.

Pode-se informar que todos os objetivos elencados foram devidamente exercidos, uma vez que a compreensão sobre os princípios e diretrizes da lei foi obtida através da demonstração de exemplos, tanto na parte inicial do desenvolvimento quanto na parte de conscientização dos usuários, conforme a figura 8 e 9 do item anterior. A definição do plano de adequação também se mostrou bastante efetiva, de modo que cada uma das fases em particular contribuiu para o processo como um todo, além de auxiliar na organização e exposição de ideias. Depois que o processo foi definido, foi possível estipular os procedimentos necessários para a implementação da lei, já que este objetivo necessita da análise individual da empresa em que o plano será aplicado. Na fase de mapeamento dos dados também foi realizada a avaliação dos riscos, que apontou ameaças de altos níveis dentro da organização. Durante a fase de diagnóstico e planejamento é que foi plausível determinar quais recursos e procedimentos seriam essenciais,

visto que cada empresa possui necessidades diferentes. Após a definição de todos os processos e mecanismos fundamentais para efetivar a lei, ela foi implementada em um cenário real, isto é, em um sistema de gestão. Todos os documentos que se fizeram necessários de elaboração na fase de planejamento foram formulados e apresentados à companhia, assim como a sugestão de boas práticas e a proposta de uma ferramenta de backup com alta usabilidade. Como resultado disso, os riscos diminuíram significativamente, conforme a figura 11 da unidade anterior. Com a adoção de todas as soluções propostas, a organização deixa de ter riscos de níveis altos, passando a ter somente riscos moderados e baixos.

Os métodos apresentados foram suficientes e efetivos, de modo que o plano de adequação proposto pela advogada Mariana de Toledo foi combinado com a avaliação de riscos recomendada pelo Governo Digital. Além disso, o levantamento bibliográfico também contribuiu significativamente para melhor compreensão da lei, permitindo compreender os casos em que ela não se aplica, as penalidades impostas e os diferentes papéis dentro dela.

Além das sugestões da ferramenta e das boas práticas, recomenda-se a implantação do processo de conformidade estabelecido em uma companhia com maiores dimensões, visando analisar a abrangência de cada fase e o desempenho máximo do plano de conformidade em organizações de grande porte.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. **TechTudo**, 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml>. Acesso em: 13 de out. de 2021.

AMBEP. **Confira os riscos de fornecer o CPF em farmácias e drogarias**. Ambep, 2021. Disponível em: <https://www.ambep.org.br/confira-os-riscos-de-fornecer-o-cpf-em-farmacias-e-drogarias/>. Acesso em: 13 de out. de 2021.

ARAÚJO, Eduardo. **A Vulnerabilidade Humana na Segurança da Informação**. [S.l.: s.n.], 2005.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BLUEPEX. **Só 2% das PMEs estão preparadas para a LGPD, aponta pesquisa**. BluePex, 2020. Disponível em: <https://www.bluepex.com.br/noticias/so-2-das-pmes-estao-preparadas-para-a-lgpd-aponta-pesquisa-2/>. Acesso em: 28 de fev. de 2021.

BRASIL. Lei nº 13.709, de 14 de Agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 25 de fev. 2021.

BRASIL. Lei nº 13.787, de 27 de Dezembro de 2018. **Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 05 de out. de 2021.

CARVALHO, W. W. S.; TAGLIAFERRO, E. A influência dos vazamentos de dados pessoais para a construção da legislação atual. **Intraciência**, p. 3-4, dez de 2020. Disponível em: https://uniesp.edu.br/sites/_biblioteca/revistas/20201125003402.pdf. Acesso em: 14 de out. de 2021.

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

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**. 2º Edição. São Paulo: Thomson Reuters Brasil, 2020.

FERNANDES, RODRIGO. Como Facebook ganha dinheiro? 6 perguntas e respostas sobre a rede social. **TechTudo**, 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/02/como-facebook-ganha-dinheiro-6-perguntas-e-respostas-sobre-a-rede-social.ghtml>. Acesso em: 15 de out. de 2021.

GRALHA, Michel Zavagna. **O desafio de implantar a Lei Geral de Proteção de Dados Pessoais**. Âmbito Jurídico, 2020. Disponível em: <https://ambitojuridico.com.br/noticias/o-desafio-de-implantar-a-lei-geral-de-protecao-de-dados-pessoais/>. Acesso em: 28 de fev. de 2021.

GUIAS operacionais para adequação à LGPD. **Governo Digital**, 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>. Acesso em: 25 de set. de 2021.

HELD, Felipe. Estudo: Brasil é o país mais vulnerável para vazamento de dados. **Konduto**, 2016. Disponível em: <https://blog.konduto.com/pt/2016/01/vazamento-dados-estudo-brasil/>. Acesso em: 22 de out. de 2021.

LEI Geral de Proteção de Dados Pessoais – Apresentação. **Cenofisco**, 2021. Disponível em: <https://www.cenofisco.com.br/Especiais/Lgpd>. Acesso em: 22 de out. de 2021.

MACIEL, Rafael Fernandes. **MANUAL PRÁTICO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (Lei nº 13.709/18)**. 1º Edição. Goiânia – GO: RM Digital Education, 2019.

MINUTA de Resolução – Aplicação da LGPD para agentes de tratamento pequeno porte. **Governo do Brasil**, 2021, p. 5. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/minuta_de_resolucao___aplicacao_da_lgpd_para_agentes_de_tratamento_de_pequeno_porte.pdf. Acesso em: 30 de out. de 2021.

NSC, Estúdio. Qual é o valor dos dados para a sua empresa? **NSC Total**. Florianópolis, 15 de julho de 2019. Disponível em: <https://www.nsctotal.com.br/noticias/qual-e-o-valor-dos-dados-para-a-sua-empresa>.

OLIVEIRA, Filipe. O que é um algoritmo e como influencia nossas escolhas. **Trendings**, 2020. Disponível em: <https://trendings.com.br/tecnologia/o-que-e-um-algoritmo-e-como-influencia-nossas-escolhas/>. Acesso em: 10 de out. de 2020.

PALAZZO, José Moreira. **Dados, Informação e Conhecimento**, 2020. Disponível em: <https://www.palazzo.pro.br/Wordpress/dados-informacao-e-conhecimento/>. Acesso em: 14 de out. de 2021.

PESQUISA: O que os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito? **Serasa Experian**, 2019. Disponível em: <https://www.serasaexperian.com.br/conteudos/protecao-de-dados/pesquisa-o-que-os-consumidores-e-as-empresas-sabem-sobre-lgpd-e-o-que-estao-fazendo-a-respeito/>. Acesso em: 23 de abr. de 2021.

PINHEIRO, P. P. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N.13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2020.

POHLMANN, Antônio Sérgio. **LGPD Ninja: Entendendo e implementando a Lei Geral de Proteção de Dados na Empresa**. [S.I]: Fross, 2019.

QUAIS são os principais objetivos do mapeamento de dados? **Jusbrasil**, 2020. Disponível em: <https://blconsultoriadigital.jusbrasil.com.br/artigos/855783756/o-que-e-o-mapeamento-de-dados>. Acesso em: 25 de set. de 2021.

RAPÔSO, Cláudio FL et al. **LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática.** RACE-Revista da Administração, v. 4, p. 58-67, 2019.

REDEMPRESA. **MAPEAMENTO DE DADOS LGPD,** 2020. Disponível em: <https://fj.com.br/mapeamento-de-dados-lgpd/>. Acesso em: 11 de mai. de 2021.

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 19/09/2021.

RIPARI, César. Por que dados são considerados o novo petróleo? **Administradores.com,** 2019. Disponível em: <https://administradores.com.br/noticias/por-que-dados-sao-considerados-o-novo-petroleo>. Acesso em: 14 de out. de 2021

RUSSO, Rogério. Empresas tem seis meses para se preparar para LGPD. **Jornal do comércio,** Porto Alegre, 11 de fev. de 2020. Disponível em: https://www.jornaldocomercio.com/_conteudo/especiais/jornal_da_lei/2020/02/724471-empresas-tem-seis-meses-para-se-preparar-para-lgpd.html. Acesso em 13 de mai. de 2021.

TOLEDO, Mariana. Manual da LGPD Descomplicado. **Empreendedorismo Legal,** Belo Horizonte, 2021. Disponível em: <https://marianadetoledo.com.br/manual-lgpd>. Acesso em: 15 de out. de 2021.

TRIPLA. **As 10 Bases Legais para Tratamento de Dados Permitidas pela LGPD,** 2019. Disponível em: <https://triplait.com/bases-legais-para-tratamento-de-dados-da-lgpd/>. Acesso em: 06 de out. de 2021.

10 BASES legais da LGPD que justificam o tratamento de dados: consentimento, legítimo interesse e mais. **Get Privacy,** 2021. Disponível em: <https://getprivacy.com.br/entenda-as-bases-legais-da-lgpd/>. Acesso em: 26 de out. de 2021.

APÊNDICE A – DOCUMENTO DE IDENTIFICAÇÃO DO CONTROLADOR

De acordo com a Lei Nº 13.709/18 – Lei Geral de Proteção de Dados (LGPD) o controlador é uma pessoa de cunho natural ou jurídico, de direito público ou privado, a quem pertencem as decisões sobre o tratamento de dados pessoais.

Nome: Israel Douglas Costa Calaça Pietrobon

Contato: FTT@unievangelica.edu.br

**FÁBRICA DE TECNOLOGIAS TURING - FUNÇÕES DO CONTROLADOR
CONFORME A LGPD**

1. Caso a base legal seja o consentimento, cabe ao controlador a responsabilidade de provar que este foi obtido em conformidade com os parâmetros da lei.
2. O controlador poderá realizar o tratamento de dados sem o consentimento do titular se o mesmo estiver previsto em obrigações legais ou regulatórias.
3. Em caso de alteração no tratamento de dados, esta deverá ser informada com destaque específico sobre o teor das alterações, e o titular que não concordar poderá revogar seu consentimento.
4. O uso compartilhado de dados sensíveis entre controladores com o objetivo de vantagem econômica pode ser vedado ou regulamentado pela Autoridade Nacional de Proteção de Dados.
5. Quando houver o tratamento de dados de crianças e adolescentes, o controlador deve manter públicas as informações sobre os tipos de dados coletados e sua forma de utilização.

Elaborado por: Camila de Souza Silva

Última revisão: 15/11/2021

Revisado por: Clara Elis Pereira

6. O controlador deve fornecer todas as informações ao titular sobre as entidades públicas e privadas que realizaram o uso compartilhado dos dados.
7. O controlador deve proporcionar ao titular acesso aos seus dados quando solicitado, bem como a correção ou atualização de dados obsoletos.
8. O controlador que, em função do exercício de atividade de tratamento de dados pessoais, causar algum dano, seja ele moral, patrimonial, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
9. Responde pelos danos decorrentes de violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas na lei, causar algum dano.
10. Os controladores no âmbito de suas competências, pelo tratamento de dados pessoais, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, normas de segurança ou padrões técnicos.

Elaborado por: Camila de Souza Silva	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

APÊNDICE B – POLÍTICA DE DESCARTE – FÁBRICA DE TECNOLOGIAS TURING

Este documento engloba as regras aplicáveis ao registro e exclusão de dados pessoais controlados pela Fábrica de Tecnologias Turing, que tem a responsabilidade de garantir o cumprimento à Lei Geral de Proteção de Dados (LGPD) e os requisitos relacionados a coleta, armazenamento, recuperação e destruição de registros de dados pessoais. Esta política complementa, porém não substitui a Política de Privacidade da empresa. A Fábrica de Tecnologias Turing mantém o conjunto de dados pessoais armazenados em conformidade com requisitos contratuais, assim como regulatórios. É essencial que esses conjuntos sejam protegidos contra perda, roubo, acesso não autorizado ou destruição, além de garantir o descarte e eliminação adequados e oportunos de informações e documentos que contenham dados pessoais.

Disposições Gerais para a exclusão de dados:

Todos os dados e informações devem ser excluídos logo após alcançarem a finalidade, ou deixarem de ser úteis ou pertinentes para a finalidade proposta. Compreende-se por exclusão, a eliminação do conjunto de dados armazenados em toda estrutura do banco de dados, tanto em meio físico quanto digital. As informações excessivas ou dispensáveis devem ser excluídas instantaneamente após observada irregularidade ou desconformidade com as políticas internas da FTT, ou com a Lei nº 13.709/18.

Hipóteses para o descarte adequado e seguro:

1. Mediante solicitação do titular;

Ocorrendo requerimento do titular para exclusão de seus dados pessoais, a Fábrica de Tecnologias Turing deverá atender à solicitação dentro de um prazo de 7 (sete) dias, desde que informado ao titular as consequências da eliminação e de acordo com as premissas regulatórias de segurança.

2. Mediante desligamento do titular com a organização;

Quando o proprietário dos dados se desligar por completo da Fábrica de Tecnologias Turing como colaborador e a finalidade da coleta for completamente cumprida, ele se declara ciente que seus dados serão descartados decorrido o período de 6 (seis) meses após seu

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

desligamento total da organização, sendo imprescindível que a solicitação de qualquer informação seja realizada antes deste período.

Direitos do Titular:

A FTT assegura aos colaboradores seus direitos de titular previstos no artigo 18 da Lei Geral de Proteção de Dados. Desse modo, você pode, de maneira gratuita e a qualquer hora:

- I. Confirmar a existência de tratamento de dados;
- II. Acessar seus dados, podendo solicitá-los em uma cópia legível segura;
- III. Corrigir seus dados, ao solicitar a atualização, edição ou correção ou destes.
- IV. Anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade;
- V. Solicitar a portabilidade de seus dados a outro fornecedor de serviços;
- VI. Eliminar dados tratados por meio de seu consentimento, exceto nos casos previstos em lei;
- VII. Informar-se sobre as entidades públicas e privadas com as quais foi realizado uso compartilhado de dados;
- VIII. Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências da negativa.
- IX. Revogar seu consentimento, vetando o tratamento de seus dados.

Para correção e atualização de dados ou exercício de outros direitos do titular recomenda-se entrar em contato no seguinte canal: ftt@unievangelica.edu.br.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

APÊNDICE C – POLÍTICA DE PRIVACIDADE – FÁBRICA DE TECNOLOGIAS TURING

Na Fábrica de Tecnologias Turing a privacidade e a segurança são itens prioritários, portanto nos comprometemos com a transparência do tratamento de dados pessoais dos nossos colaboradores. Logo, o presente documento estabelece como é feita a coleta, transferência e uso de informações de seus funcionários, bem como a descrição dos seus direitos.

Ao utilizar nossos serviços, você entende que coletaremos e utilizaremos suas informações pessoais nas formas descritas nesta Política, sob as normas de Proteção de Dados (LGPD, Lei Federal 13.709/2018).

Dessa forma, a Fábrica de Tecnologias Turing, doravante denominada simplesmente como “FTT”, no papel de Controladora de Dados, obriga-se ao disposto na presente Política de Privacidade.

1. Quem somos?

A Fábrica de Tecnologias Turing é uma unidade do curso superior de Engenharia de Software da Universidade Evangélica de Goiás – UniEVANGÉLICA, que tem por objetivo proporcionar aos alunos a aplicação prática dos conhecimentos adquiridos em sua formação acadêmica. É um ambiente de constante inovação tecnológica onde são realizados projetos reais, possibilitando ao discente a oportunidade de acompanhar todas as etapas do desenvolvimento de software, além de desenvolver as habilidades e competências necessárias ao perfil do profissional que atua com tecnologia da informação.

2. A quem essa política se aplica?

A todos os alunos que ingressaram ou desejam ingressar na equipe de colaboradores da Fábrica de Tecnologias Turing.

3. Quais dados coletamos?

CPF, data de nascimento, e-mail, endereço, estado civil, nome, RG, sexo, telefone.

4. Por que coletamos esses dados?

Os dados são coletados com a finalidade única de cadastrar o colaborador no sistema de registro de ponto.

5. Como coletamos esses dados?

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

Através do sistema da universidade.

6. Existe tratamento de dados sensíveis?

A Fábrica de Tecnologias Turing não solicita o fornecimento de dados sensíveis para fins de cadastro.

7. Existe compartilhamento de dados com terceiros? Se sim, por que?

Os dados fornecidos para cadastro no sistema não são compartilhados com terceiros.

7.1. Existe possibilidade de transferência internacional de dados?

A Fábrica de Tecnologias Turing não presta serviços ou possui instalações fora do país e somente trata dados em solo nacional.

8. Por quanto tempo os dados serão armazenados?

Os dados pessoais serão eliminados quando deixarem de ser úteis para os fins que motivaram o seu fornecimento ou quando o usuário solicitar a sua eliminação, desde que não forem mais necessários para cumprir qualquer obrigação legal. Para mais informações consulte a política de descarte.

9. Quais as medidas adotadas para manter os dados seguros?

Para mantermos as informações pessoais seguras, usamos ferramentas gerenciais e eletrônicas, voltadas para a proteção da sua privacidade.

As ferramentas são aplicadas levando em consideração a natureza dos dados apanhados, a finalidade do tratamento e o contexto inserido. Entre as medidas adotadas, destacam-se:

- a) Somente após firmado o compromisso de confidencialidade o acesso aos dados é realizado;
- b) É estabelecido um rígido controle sobre o acesso aos dados diante da definição de papéis e responsabilidades das pessoas que poderão ter acesso, juntamente com os privilégios de acessos exclusivos.
- c) Os dados são armazenados em ambiente seguro e íntegro.

10. Existe tratamento de dados de menores de idade?

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

Pode ocorrer a admissão de um aluno menor de idade, e quando esse for o caso, o responsável legal deverá preencher o termo de autorização disponibilizado junto com a política de privacidade.

11. Qual a base legal utilizada para atestar o tratamento de dados?

Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Essa base é utilizada, pois os dados são coletados a pedido do próprio titular que deseja ingressar na FTT, e para que o contrato seja firmado e o titular comece registrar devidamente o horário de entrada e saída é anteriormente necessário cadastrar seus dados no sistema.

12. Quais são os seus direitos?

A FTT assegura aos colaboradores seus direitos de titular previstos no artigo 18 da Lei Geral de Proteção de Dados. Desse modo, você pode, de maneira gratuita e a qualquer hora:

- X. Confirmar a existência de tratamento de dados;
- XI. Acessar seus dados, podendo solicitá-los em uma cópia legível segura;
- XII. Corrigir seus dados, ao solicitar a atualização, edição ou correção ou destes.
- XIII. Anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade;
- XIV. Solicitar a portabilidade de seus dados a outro fornecedor de serviços;
- XV. Eliminar dados tratados por meio de seu consentimento, exceto nos casos previstos em lei;
- XVI. Informar-se sobre as entidades públicas e privadas com as quais foi realizado uso compartilhado de dados;
- XVII. Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências da negativa.
- XVIII. Revogar seu consentimento, vetando o tratamento de seus dados.

13. Como exercer seus direitos?

Para correção e atualização de dados ou exercício de outros direitos do titular recomenda-se entrar em contato no seguinte canal: ftt@unievangelica.edu.br.

14. Alteração dessa Política de Privacidade

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

A atual Política de Privacidade foi formulada e revisada pela última vez em novembro de 2021. Reservamos o direito de modificação, principalmente em função da adequação a possíveis alterações realizadas no sistema ou no âmbito legislativo. Nas hipóteses em que as alterações do documento resultarem em modificações no tratamento de dados gerando dependência do consentimento, este será solicitado nos novos termos da política.

15. Responsabilidade

A Fábrica de Tecnologias Turing prevê a responsabilidade dos agentes atuantes no tratamento de dados, conforme o artigo 42 a 45 da Lei Geral de Proteção de Dados. Nos comprometemos a manter o documento constantemente atualizado, observando suas exigências e prezando pelo seu cumprimento. Caso a Autoridade Nacional de Proteção de Dados exija a adoção de outras medidas para manuseio dos dados realizado pela organização, comprometemo-nos a cumpri-las.

16. Isenção de Responsabilidade

Embora sejam adotadas medidas de segurança visando evitar incidentes, as páginas virtuais não são completamente livre de riscos. Nesse sentido, a FTT não se responsabiliza por:

- I. Eventuais negligências ou descuido dos usuários em relação aos seus dados pessoais. Nos responsabilizamos apenas pela segurança dos processos adotados no tratamento de dados, juntamente com o cumprimento da finalidade descrita;
- II. Ações mal intencionadas de terceiros, como ataques *hackers* ou atividades maliciosas, exceto se comprovado conduta culposa;
- III. Inveracidade ou informações equivocadas inseridas pelo usuário nos processos necessários para utilização de serviços. Informações falsas ou inseridas de má-fé são de responsabilidade do usuário.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

APÊNDICE D – SUGESTÃO DE BOAS PRÁTICAS DE SEGURANÇA E PROPOSTA DE FERRAMENTA

VISÃO GERAL

Este documento tem por objetivo fomentar a segurança da informação através do incentivo de usuários a execução de boas práticas e procedimentos padrões, com a finalidade de colaborar com a confidencialidade, integridade, disponibilidade e autenticidade das informações. Teve como embasamento o Guia de Boas Práticas em Tecnologia da Informação da Universidade Federal do Pará, visando o fornecimento de informações para a realização de serviços eficientes e válidos para a segurança dos dados, bem como a proposta de ferramentas preventivas de apoio. As sugestões propostas são inteiramente opcionais e cabe à organização adotá-las.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

BOAS PRÁTICAS DE SEGURANÇA PARA O AMBIENTE CORPORATIVO

As boas práticas de segurança da informação podem ser definidas como um conjunto de atividades simples que auxiliam a proteção dos dados e são extremamente importantes no contexto corporativo. É essencial descrever ao usuário as medidas que evitam o prejuízo causado por golpes, invasões ou vazamentos, o tirando de um estado leigo para um estado prevenido, visando em todas as situações a proteção dos dados pessoais.

- ✓ Restringir o usuário de instalar aplicativos e softwares sem mediação do setor de tecnologia responsável;
- ✓ Impedir o acesso a sites inadequados ou desnecessários ao ambiente de trabalho;
- ✓ Supervisionar a utilização de equipamentos conectados ao computador, como pendrives e celulares, executando sempre a varredura, visando a eliminação de programas maliciosos;
- ✓ Impedir o acesso não autorizado de usuários sem o devido conhecimento de prevenção;
- ✓ Bloquear o computador em caso de necessidade de ausência;
- ✓ Confirmar a existência do protocolo HTTPS (cadeado fechado na URL) em sites de login;
- ✓ Evitar o acesso a URL de bancos recebidas através de e-mail;
- ✓ Impedir que senhas sejam anotadas em locais visíveis;
- ✓ Combinar letras, números e caracteres especiais nas senhas;
- ✓ Executar o backup de arquivos tanto pessoais quanto corporativos;
- ✓ Evitar o acesso a links desconhecidos, principalmente se recebidos por e-mail ou redes sociais;
- ✓ Evitar o compartilhamento das senhas com outras pessoas;
- ✓ Evitar a utilização de informações pessoais nas senhas;
- ✓ Evitar a execução de programas recebidos cuja origem é desconhecida;
- ✓ Verificar através do antivírus os arquivos recebidos antes de executá-los;
- ✓ Desconfiar de bancos ou operadoras de cartão de crédito que entrem em contato por e-mail;
- ✓ Evitar o armazenamento de documentos pessoais ou acadêmicos em ambiente corporativo;

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

- ✓ Suspeitar de mensagens recebidas das quais o conteúdo solicite informações pessoais;
- ✓ Definir senhas diferentes para acesso a sistemas distintos;
- ✓ Alterar as senhas periodicamente;
- ✓ Manter os softwares instalados nas versões mais recentes;
- ✓ Assegurar que todas as contas presentes no computador sejam protegidas por senha;
- ✓ Evitar a utilização de contas compartilhadas;
- ✓ Inibir a memorização de senhas pelo computador;
- ✓ Evitar o acesso a sites sem o protocolo HTTPS;
- ✓ Considerar a proteção criptográfica das informações pessoais.

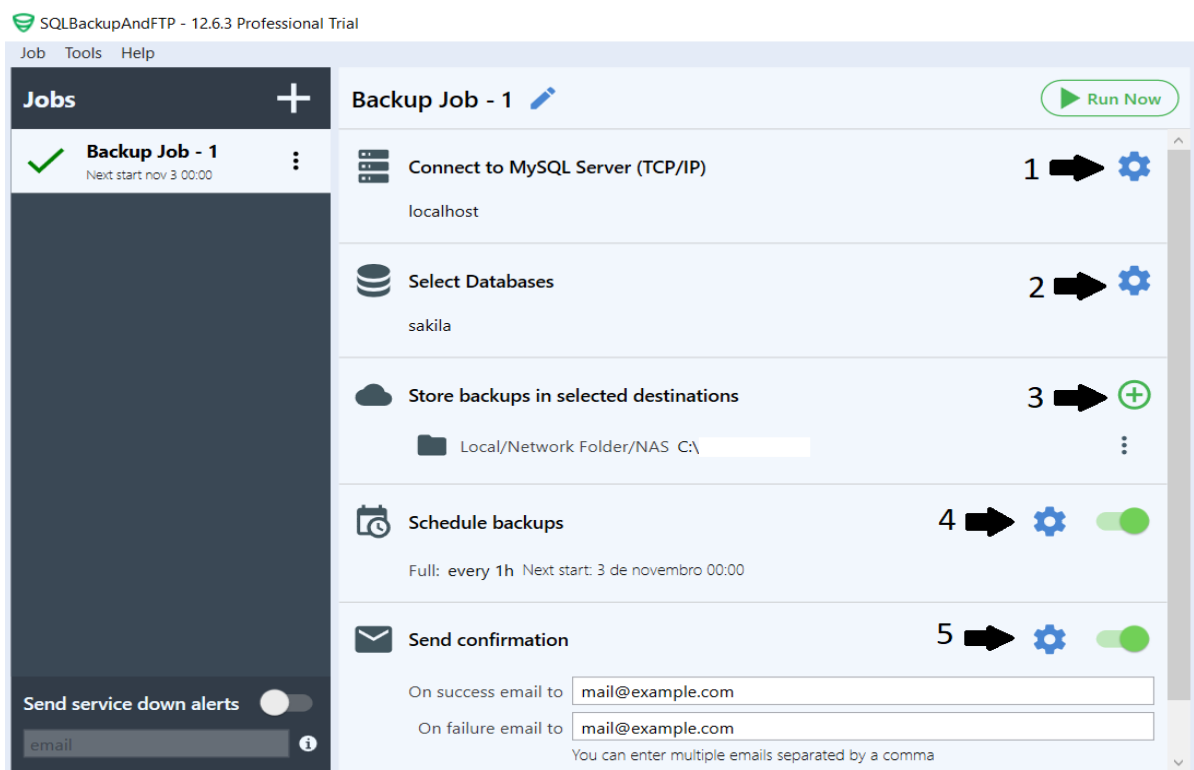
Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

PROPOSTA DE FERRAMENTA

Visando atender ao princípio da segurança e da prevenção do Art. 6º da LGPD, sugere-se a implementação de ferramentas que contribuam para o controle do tratamento de dados. A ferramenta abordada é o “SQLBackupAndFTP”, um software de backup completo por agendamento que executa backups de arquivos e pastas permitindo sua restauração, além de compactá-los e criptografá-los. É compatível com SQL Server, PostgreSQL, MySQL, Azure SQL e Amazon SQL, sendo indicada para um número menor de servidores. Para criar um backup utilizando o SQLBackupAndFTP é necessário efetuar a transferência da ferramenta no site <https://sqlbackupandftp.com/> e seguir as seguintes etapas, conforme a figura 1:

1. Conectar a um servidor banco de dados;
2. Selecionar o banco de dados para backup;
3. Escolher o local de armazenamento para os backups (local, rede, FTP, nuvem);
4. Criar um agendamento de backup;
5. Adicionar e-mail caso desejável a obtenção de informações sobre o backup;

Figura 1: Passo a passo de utilização da ferramenta



Fonte: Autor, 2021.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

REFERÊNCIAS BIBLIOGRÁFICAS

UNIVERSIDADE FEDERAL DO PARÁ. **Guia De Boas Práticas Em Tecnologia Da Informação**. Pará: Abaetetuba, [202?]. 13 p. Disponível em: <https://www.cubt.ufpa.br/publicacoes/documento/tecnologia/CartilhaTI.pdf>. Acesso em: 28 de out. de 2021.

FERRAMENTA de backup de banco de dados. **SQLBackupAndFTP**. [202?]. Disponível em: <https://sqlbackupandftp.com/>. Acesso em: 29 de out. de 2021.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

APÊNDICE E – TERMO DE AUTORIZAÇÃO PARA MENORES DE IDADE

Este documento tem por objetivo registrar a manifestação livre, informada e inequívoca pela qual o responsável legal do titular com menos de 18 (dezoito) anos concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), de forma digital ou manual.

Eu, _____, portador do RG nº _____, responsável legal pelo menor _____, nascido na data __/__/__, estou ciente e concordo que a Fábrica de Tecnologias Turing colete e tome decisões referentes ao tratamento de seus dados pessoais, com a finalidade de cadastrá-lo no sistema SigTuring, utilizado para registro de horário de entrada e saída, assim como o acompanhamento de projetos.

_____, ____ de _____ de _____.

Assinatura do Responsável

Perguntas Frequentes:

1. Quais dados coletamos?

CPF, data de nascimento, e-mail, endereço, estado civil, nome, RG, sexo, telefone.

2. Por que coletamos esses dados?

Os dados são coletados com a finalidade única de cadastrar o colaborador no sistema de registro de ponto.

3. Como coletamos esses dados?

Através do sistema da universidade.

4. Existe compartilhamento de dados com terceiros? Se sim, por que?

Os dados fornecidos para cadastro no sistema não são compartilhados com terceiros.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	

5. Quais são os direitos do titular?

A FTT assegura aos colaboradores seus direitos de titular previstos no artigo 18 da Lei Geral de Proteção de Dados. Desse modo, você pode, de maneira gratuita e a qualquer hora:

- I. Confirmar a existência de tratamento de dados;
- II. Acessar seus dados, podendo solicitá-los em uma cópia legível segura;
- III. Corrigir seus dados, ao solicitar a atualização, edição ou correção ou destes.
- IV. Anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade;
- V. Solicitar a portabilidade de seus dados a outro fornecedor de serviços;
- VI. Eliminar dados tratados por meio de seu consentimento, exceto nos casos previstos em lei;
- VII. Informar-se sobre as entidades públicas e privadas com as quais foi realizado uso compartilhado de dados;
- VIII. Informar-se sobre a possibilidade de não fornecer seu consentimento e sobre as consequências da negativa.
- IX. Revogar seu consentimento, vetando o tratamento de seus dados.

6. Como exercer seus direitos?

Para correção e atualização de dados ou exercício de outros direitos do titular recomenda-se entrar em contato no seguinte canal: ftt@unievangelica.edu.br

Para maiores informações, consulte nossa Política de Privacidade.

Elaborado por: Clara Elis Pereira	Última revisão: 15/11/2021
Revisado por: Clara Elis Pereira	