Universidade Estadual de Londrina

FRANCYELCYO PUSSI FARIAS

GAIA LGPD:

UM FRAMEWORK PARA A PROTEÇÃO DE DADOS PESSOAIS

Londrina
2022

FRANCYELCYO PUSSI FARIAS

GAIA LGPD:

UM FRAMEWORK PARA A PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Rodolfo Miranda de Barros

Londrina
2022

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

F224g Farias, Francyelcyo Pussi.
Gaia lgpd : Um framework para a proteção de dados pessoais / Francyelcyo Pussi Farias. - Londrina, 2022.
103 f. : il.

Orientador: Rodolfo Miranda de Barros.
Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2022.
Inclui bibliografia.

1. Lei Geral de Proteção de Dados Pessoais - Tese. 2. Framework para proteção de dados pessoais - Tese. 3. Privacidade e proteção de dados pessoais - Tese. I. Barros, Rodolfo Miranda de. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 519

FRANCYELCYO PUSSI FARIAS

GAIA LGPD:

UM FRAMEWORK PARA A PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Mestrado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina – UEL

_____

Prof. Dr. Bruno Bogaz Zarpelão
Universidade Estadual de Londrina – UEL

_____

Prof. Dr. Lourival Aparecido de Góis
Universidade Tecnológica Federal do Paraná – UTFPR

Londrina, 22 de fevereiro de 2022.

Este trabalho é dedicado às crianças adultas
que, quando pequenas, sonharam em se
tornar cientistas.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me dado todas as condições necessárias para eu realizar esse Mestrado.

À minha esposa Alanna, quem me apoio de forma incondicional durante toda essa jornada e foi fundamental para não deixar eu desistir no meio do caminho.

À minha filha Livia, quem serviu de motivação para eu buscar novos aprendizados.

Ao meu Orientador, Prof. Dr. Rodolfo Barros, quem acreditou no meu trabalho, me desafiou e me suportou o tempo todo.

Ao meu amigo Wagner Ueno, quem me apresentou o caminho a ser percorrido e serviu como referência para esse trabalho.

"O período de maior ganho em conhecimento e experiência é o período mais difícil da vida de alguém.
(Dalai Lama)

FARIAS, F. P. **GAIA LGPD:** Um framework para a Proteção de Dados Pessoais. 2022. 103 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Londrina, Londrina, 2022.

RESUMO

A recente chegada da LGPD (Lei Geral de Proteção de Dados - Lei 13709) sancionada em setembro de 2020 obriga empresas de diversos setores a adotar práticas voltadas ao tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, ou seja, dos titulares de dados pessoais. A adoção dessas práticas voltadas à proteção dos dados pessoais, ao mesmo tempo em que atende as exigências legais também é capaz de gerar valor aos negócios, uma vez que o aumento do nível de maturidade em segurança de dados pessoais pode se tornar um grande trunfo para atrair novos clientes. Assim sendo, o objetivo deste trabalho é desenvolver um framework que possa ser aplicado para ajudar a organização a identificar seu nível de maturidade em relação às práticas de proteção de dados pessoais e consequentemente ao nível de adesão aos requisitos da LGPD e a partir desse levantamento estabelecer as ações mitigatórias a serem implementadas. Com o uso do framework, esse trabalho é feito através da descoberta das vulnerabilidades relacionadas ao tratamento de dados pessoais, da análise dos riscos atrelados a essas vulnerabilidades e da elaboração de um plano de ação para mitigar os riscos mapeados. Para tanto, o presente trabalho é formado por cinco processos principais, um questionário de autoavaliação, composto por 7 eixos que classificam o nível de maturidade de acordo com as seções dos artigos da LGPD, uma matriz de análise de riscos e templates que poderão ser adotados de forma integral ou parcial, de acordo com a necessidade de cada organização. Dessa forma, espera-se que o plano de ação elaborado a partir da execução do framework, se converta em um robusto Programa de Proteção de Dados e Privacidade, que além de atender às regulamentações, também fortaleça a confiança dos clientes atuais, abrindo assim a possibilidade de atrair novos clientes com apreço pela seriedade com que seus dados pessoais são tratados e protegidos pela organização. Para validar o Framework proposto, foi realizado um estudo de caso em uma multinacional brasileira do setor de Químicos. O trabalho durou 5 meses e contou com a participação de Especialistas da áreas de Segurança da Informação, Tecnologia da Informação (TI) e da área Jurídica. Todas as etapas propostas pelo Framework foram aplicadas. O trabalho resultou em: relatório contendo a lista dos itens de não conformidades com a LGPD; levantamento das vulnerabilidades relacionadas à segurança de dados pessoais; análise e classificação dos riscos; e por fim, a elaboração de um plano de ação alinhado com os requisitos da LGPD. Em adicional, o estudo de caso permitiu identificar oportunidades de melhoria no modelo inicial do Framework e contribuiu para a definição de ações futuras.

Palavras-chave: lei geral de proteção de dados; LGPD; GDPR; programa de privacidade; proteção de dados pessoais; governança de segurança em TI.

FARIAS, F. P. **GAIA LGPD:** The framework for Personal Data Protection. 2022. 103 p. Master's Thesis (Master in Science in Computer Science) - State University of Londrina, Londrina, 2022.

ABSTRACT

The recent arrival of the LGPD (General Data Protection Law - Law 13.709), sanctioned in September 2020, forces companies from various sectors to adopt practices aimed at the processing of personal data, including in digital media, by natural person or legal Entity public or private, with the objective of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person, that is, of the holders of personal data. The adoption of these practices, aimed at protecting personal data, while meeting legal requirements, is also capable of generating business value, since the increase in the level of maturity in personal data security can become a great asset to attract new customers. Therefore, the objective of this work is to develop a framework that can be applied to help the organization identify its level of maturity in relation to personal data protection practices and, consequently, the level of adherence to the requirements of the LGPD and from there provide a survey to establish the mitigating actions to be implemented. Using the framework, this work is done through the discovery of vulnerabilities related to the treatment of personal data, the analysis of the risks linked to these vulnerabilities and the elaboration of an action plan to mitigate the mapped risks. For this purpose, the present work consists of five main processes, a self-assessment ques- tionnaire, composed of 7 axes that classify the level of maturity according to the sections of the LGPD articles, a risk analysis matrix and templates that can be adopted. in Whole or in part, according to the needs of each organization. Thus, it is expected that the action plan elaborated from the execution of the framework, becomes a robust Data Protection and Privacy Program, which in addition to meeting the regulations, also strengthens the trust of current customers, thus opening the possibility of attracting new customers with appreciation for the seriousness with which their personal data is treated and protected by the organization.To validate the proposed Framework, a case study was carried out in a Brazilian multina-tional in the Chemicals sector. The work lasted 5 months and included the participation of Specialists from the Information Security, Information Technology (IT) and Legal ar-eas. All the steps proposed by the Framework were applied. The work resulted in: report containing the list of items of non-compliance with the LGPD; survey of vulnerabilities related to the security of personal data; risk analysis and classification; and finally, the elaboration of an action plan in line with the requirements of the LGPD. In addition, the case study made it possible to identify opportunities for improvement in the Framework's initial model and contributed to the definition of future actions.

Key words: LGPD; data privacy; GDPR; personal data security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

DPIA	Data Protect Impact Assessment
DPO	Data Protector Officer
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
NA	Não se Aplica
OCQ	Oswaldo Cruz Química
PDCA	Plan Check Do Act
PGPD	Programa de Gestão de Proteção de Dados
PPDP	Programa de Proteção de Dados Pessoais
SIPOC	Supplier, Input, Process, Output e Customer
TI	Tecnologia da Informação
UEL	Universidade Estadual de Londrina

SUMÁRIO

1 INTRODUÇÃO

Em setembro de 2020 foi sancionada pelo Congresso Nacional a Lei Geral de Proteção de Dados - Lei 13709, mais conhecida como LGPD. Essa lei dispõe sobre o tratamento de dados pessoais de pessoa física, sejam esses dados físicos (ex.: formulários impressos) ou digitais (ex.: dados armazenados em sistemas), com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade dos cidadãos [4]. Através dos seus 64 artigos, a LGPD estabelece um conjunto de diretrizes voltadas à proteção de dados pessoais, sejam esses dados digitais ou físicos.

Essas diretrizes resultam numa série de práticas de segurança e governança de dados, que devem ser adotadas por todas as organizações que tratam de dados pessoais de pessoa física, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados [4]. Conforme listado no Artigo 52 da LGPD, o não cumprimento das diretrizes estabelecidas na lei poderá acarretar em sanções Administrativas, tais como: advertência seguida de uma indicação e prazo para a adoção de medidas corretivas; multas simples de até 2% do faturamento da empresa (limitada, no total, a R$ 50.000.000 - 50 milhões de Reais); multa diária; bloqueio e eliminação dos dados pessoais aos quais se refere a infração; suspensão do exercício da atividade de tratamento de dados pessoais; proibição do exercício de atividades relacionadas a tratamento de dados [4].

Além das multas, incidentes envolvendo vazamento de dados pessoais poderão gerar efeitos negativos na imagem e reputação da empresa, podendo levar à desconfiança de seus clientes, à desvalorização da marca, entre outras consequências intangíveis [5]. Conforme apontado por [6], quase todas as organizações tratam de dados pessoais; além disso, a quantidade e os tipos de dados pessoais tratados estão aumentando de forma exponencial. A proteção da privacidade no contexto do tratamento de dados pessoais é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo. A demanda por controles de privacidade e segurança vem aumentando muito nos últimos anos, devido à iniciativa de diversos países para que as empresas instaladas em seus territórios estejam adequadas à privacidade [5].

No Brasil, tem-se ouvido o relatos de muitas empresas a respeito das dificuldades de entendimento sobre como implementar os controles previstos na lei [5]. Segundo [7], muitas empresas ainda têm dúvidas em relação à LGPD, mesmo a lei já estando em vigor desde 2020. A RD Station, empresa de tecnologia e marketing digital, realizou uma pesquisa que aponta que as empresas não estão conseguindo se adequar às novas exigências relacionadas à LGPD [7].

Segundo a pesquisa realizada, 93% das quase mil empresas que participaram do

estudo dizem conhecer ou pelo menos já ter ouvido falar da LGPD, mas apenas 15% se mostram prontas ou em processo de preparação, mesmo a lei já prevendo sanções desde o dia 1º de agosto de 2020. Na pesquisa realizada é apontado que 22% das empresas não inseriu nenhuma medida de segurança referente às informações pessoais que armazena, sejam colaboradores, parceiros ou clientes. Segundo o estudo, os fatores que mais pesam para as empresas são ausência de capital para investir em novos processos, falta de profissionais qualificados e confusão sobre quais áreas precisam receber cuidados especiais [7].

Mesmo as organizações que buscam aprofundar seus conhecimentos sobre a lei, a fim de tomar as ações necessárias para se adequar à LGPD, têm esbarrado na complexidade das normas e medidas impostas. Sendo assim, as organizações que enfrentam dificuldades com a LGPD, precisam buscar o quanto antes os auxílios necessários para que possam atingir um resultado satisfatório, de forma a atender tanto às necessidades da empresa, quanto aos requisitos legais [8]. Um dos principais desafios enfrentados pelas empresas está em equilibrar seu orçamento para que se possa implementar as medidas de segurança sem que seja necessário repassar um aumento de custo para o consumidor final [9].

Analisando todos os desafios que a LGPD trouxe para as organizações, ainda assim podemos considerar que o cumprimento dessas novas regulamentações não deve ser visto apenas como um obstáculo, mas, sim, como uma grande oportunidade para atrair novos clientes. A criação da LGPD abriu um novo mercado para profissionais que combinam conhecimentos técnicos em TI, Segurança da Informação e saber jurídico, que além de estarem debatendo em relação ao desenvolvimento e adoção das medidas adequadas, também estão assumindo uma nova função chamada de Encarregado de Dados Pessoais, mais conhecida pela sigla DPO (Data Protection Officer), sendo essa uma das exigências impostas pela nova lei.

Profissionais como Consultores de Segurança, Gestores da Área de Tecnologia da Informação (TI), Fabricantes de soluções de segurança da informação, Autoridades, Escritórios Advocatícios entre outros, têm se unido para promover debates e discutir os impactos esperados com a chegada da LGPD. A oferta de cursos e workshops relacionados ao assunto tem se tornado cada vez mais frequente. Surgiram várias empresas especializadas no assunto de proteção de dados pessoais e privacidade, que visam aplicar as medidas necessárias para que a organização possa estar aderente a LGPD.

Como um exemplo desse tipo de empresa podemos citar a Privacy Tools, que oferece uma gama completa de serviços voltados a atender todos os requisitos da LGPD. A Privacy Tools oferece serviços que vão desde o levantamento das não conformidades até a implementação de soluções exigias pela LGPD. O principal obstáculo para a contratação desse tipo de serviço está nos elevados custos de investimentos. Tendo em vista que o ponto

de partida para uma jornada de adequação a LGPD é saber quais são as deficiências que devem ser corrigidas, os valores cobrados para esse tipo de atividade acabam sendo um impeditivo para empresas de pequeno e médio porte, que por muitas vezes acabam deixando de olhar para a LGPD devido à restrição orçamentária [7].

1.1 OBJETIVOS GERAIS

O objetivo desse trabalho é: desenvolver um modelo de maturidade e capacidade através de um framework que permita às organizações se alinharem à LGPD, através da avaliação dos riscos relacionados com a LGPD e da elaboração de um plano de ação para a mitigação desses riscos.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são:

Estabelecer as categorias para o agrupamento dos requisitos listados na LGPD;

Definir as questões a serem utilizadas no Questionário de autoavaliação;

Definir os níveis de maturidade para o Questionário de autoavaliação;

Definir uma matriz para análise de risco e priorização do Plano de Ação;

Definir um conjunto de templates que será entregue junto com o framework;

Definir um processo para a implantação do framework;

Definir os níveis de maturidade e capacidade técnica do framework;

2 MÉTODO DA PESQUISA

O método de pesquisa utilizado nessa dissertação baseou-se na análise bibliográfica do tema junto a sites especializados, leitura de artigos, livros, revistas, relatórios técnicos publicados em anais de conferências, periódicos nacionais e internacionais, publicações do Congresso Nacional e estudo de caso. Do ponto de vista de seus objetivos, esta pesquisa é classificada como exploratória, uma vez que busca abordar um problema específico pela busca de novo conhecimento, geração de ideias, abrindo hipóteses para novas pesquisas [10]. Do ponto de vista de sua natureza a pesquisa pode ser considerada como pesquisa aplicada, pois visa gerar conhecimento para aplicação prática dirigida à solução de um problema específico [11]. Quanto aos procedimentos técnicos utilizados para a condução da pesquisa, foi aplicado pesquisa bibliográfica e estudo de caso. A pesquisa bibliográfica caracteriza-se pela busca sistemática de conhecimento sobre um determinado assunto, o que já existe comprovado a respeito do assunto abordado, trazendo um comparativo entre o que os autores já discutiram, propuseram ou realizaram. O estudo de caso, investiga fenômenos contemporâneos dentro de seu contexto, caracterizando-se pela coleta de informações de poucas entidades e pela falta de experimentos controlados. [12]. A classificação sumarizada dessa pesquisa está representada na Tabela 1.

CARACTERÍSTICA	CLASSIFICAÇÃO
Objetivo	Pesquisa Exploratória
Natureza	Pesquisa Aplicada
Origem dos dados	Múltiplas Fontes
Procedimentos técnicos	Pesquisa bibliográfica e estudo de caso

Tabela 1 – Classificação da Pesquisa. Fonte: Elaborada pelo autor.

O método aplicado para o desenvolvimento do Framework GAIA LGPD foi adaptado de [1] e está representado na Figura 1. Ele é dividido em 3 etapas: 1) Análise Teórica, 2) Desenvolvimento e 3) Melhoria Contínua. A primeira etapa, Análise Teórica, visa levantar o conhecimento teórico necessário para a construção do modelo proposto. Grande parte desse conhecimento é adquirida através de pesquisas bibliográficas, busca das melhores práticas de mercado, análises comparativas e entrevistas com especialistas. Essa etapa está dividida sequencialmente em três atividades: 1) Análise do Estado da Arte, 2) Análise Comparativa e 3) Fundamentação Teórica.

A segunda etapa, Desenvolvimento, consiste no desenvolvimento e implementação do modelo de trabalho. No início dessa etapa aplica-se a versão inicial do modelo para que seja realizada uma primeira avaliação junto a especialistas. É nessa etapa que as melhorias são desenvolvidas e se entrega a versão final do framework e seus templates. Essa

etapa contempla 3 atividades: 1) Framework GAIA LGPD Versão X (onde X representa o número atual da versão do framework), 2) Aplicação do Framework GAIA LGPD, 3) Versão final do Framework GAIA LGPD.

A terceira etapa visa a melhoria contínua do modelo através da análise dos resultados aferidos na etapa anterior. É aqui que as melhorias são identificadas, analisadas e encaminhadas para correção. Essa etapa consiste em duas atividades: 1) Análise dos resultados e 2) Identificar possíveis correções. A Figura 1 ilustra cada uma dessas etapas.

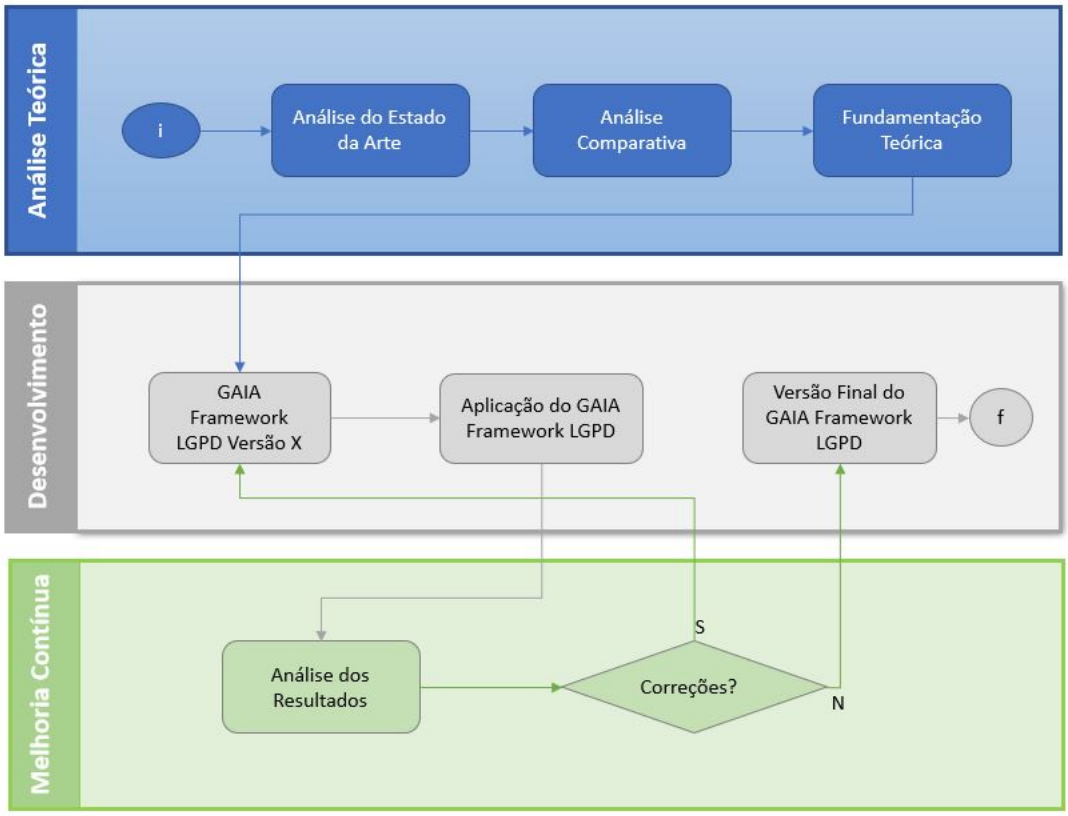

Figura 1 – Método aplicado na pesquisa. Fonte: adaptado de [1].

3 FUNDAMENTAÇÃO TEÓRICA

Nessa seção será apresentado um estudo sobre o real estado da arte para a gestão de dados pessoais voltada a atender os requisitos da LGPD. Serão apresentados os princípios gerais da lei, tais como: estrutura funcional, fundamentos legítimos, finalidade, bases legais e sanções administrativas. Também será exposta uma revisão da literatura e os trabalhos relacionados encontrados durante o processo de pesquisa.

3.1 PRINCÍPIOS GERAIS DA LGPD

Criada com base na GDPR (General Data Protection Regulation) que foi implementada em 23.5.2018 para todos os países da União Europeia, a LGPD entrou em vigência no Brasil no dia 9 de setembro de 2020, registrada como LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Essa lei é composta por 10 capítulos e 65 artigos. A LGPD "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[2].

A lei estabelece diretrizes que resultam na adoção de práticas de segurança e governança de dados, voltadas à proteção de dados pessoais, sejam esses dados digitais ou físicos. Conforme o artigo 3º, a LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados"[4]. Conforme o artigo 4º, a LGPD não se aplica a dados pessoais de pessoa jurídica, autoridades competentes de proteção de segurança pública, defesa nacional, segurança do Estado e pessoas físicas puramente pessoais sem fins lucrativos.

Segundo [2], a LGPD traz transformações importantes para o país no que se refere à privacidade do indivíduo. Para que não haja confusão, a lei deixa claro o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação. A LGPD é bastante rica, tratando desde a definição de conceitos até a sugestão de práticas que devem ser adotadas para evitar falhas de segurança, como o vazamento de dados.

A Figura 2 apresenta, de forma ilustrativa, quais são os direitos dos cidadãos (titulares de dados pessoais) e as obrigações das organizações que tratam de dados pessoais (Controladores e Processadores).

Figura 2 – Visão Geral LGPD. Fonte: [2].

Nos artigos 5º e 55, observa-se que a estrutura funcional da LGPD é composta por: Autoridade Nacional de Proteção de Dados (ANPD), Controlador, Processador, Encarregado de Proteção de Dados (Data Protection Officer / DPO) e o Titular dos Dados, conforme ilustrado na Figura 3.

3.1.1 Autoridade Nacional de Proteção de Dados (ANPD)

O artigo 55 define a ANPD como sendo uma Entidade governamental que reporta diretamente para a Presidência da República. Tem o papel consultivo, liberdade técnica, investigatória e corretiva. Suas principais atribuições são:

1. Estabelecer normas;
2. Definir padrões técnicos;
3. Supervisionar e Auditar Controladores e Processadores;
4. Educar sobre a lei e suas implicações;
5. Lidar com notificações de violações de dados;
6. Aplicar sanções Administrativas;

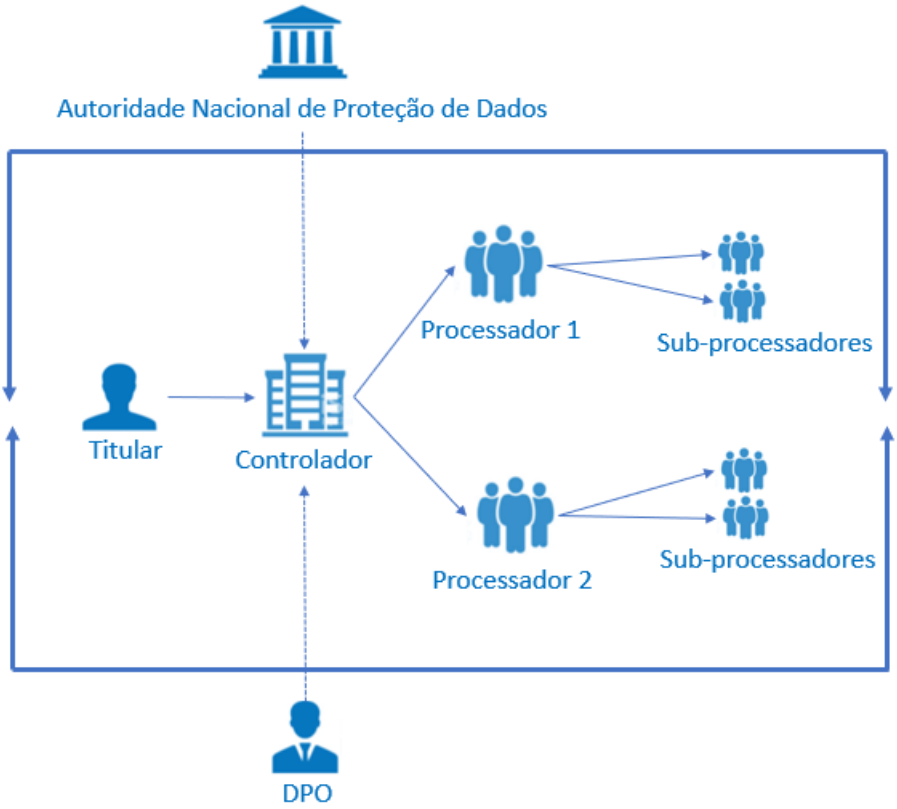

Figura 3 – Estrutura Funcional LGPD. Fonte: Adaptada de TI.Exames.

Para [3], a competência fiscalizatória da ANPD será essencial para todo o firmamento da lei, de modo que a ANPD tem seu protagonismo na discussão e na interpretação perante a LGPD. Porém, deve-se ficar atento quanto à sua função, não antepondo ou misturando outras leis que já estão consolidadas no país, como por exemplo, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet, além de outras regulações específicas existentes para cada propósito em si. Desta maneira, segundo [3], a ANPD se fará presente e atuante, demonstrando sua competência técnica de conhecimentos bem direcionados e com a devida proficiência de causa, sem a interferência de outras entidades de fiscalização que venham a sobrepor ou descontinuar suas decisões, uma vez que a própria ANPD já fez sua interpretação da lei carimbando nesta a sua designação. A ANPD possui dois órgãos: 1) Conselho de Administração, composto por cinco membros com experiência no campo da privacidade e proteção de dados; 2) Conselho Nacional, formado por um conselho consultivo composto por 23 membros, com representação do governo, sociedade civil, instituições de pesquisa e setor privado.

3.1.2 Controlador

Conforme disposto nos artigos 5º, 37, 38 e 42 da LGPD, o Controlador é uma empresa denominada pela lei como “pessoa natural ou jurídica, de direito público ou

privado, a quem competem as decisões referentes ao tratamento de dados pessoais." É quem, de fato, gera a demanda para a coleta e/ou processamento dos dados dos Titulares e é responsável por definir, implementar e monitorar as medidas de segurança voltadas à proteção de dados pessoais. Os deveres do Controlador são:

1. Definir a finalidade de processamento, categorias de dados, titulares e outros;
2. Responsável pelo tratamento e medidas de segurança;
3. Realizar avaliações de impacto de proteção de dados;
4. Manter um registro das atividades de processamento;
5. Garantir a coleta minimizada de dados pessoais;
6. Reparação de danos causados devido a violação de dados;
7. Nomear um DPO (Encarregado de Proteção de Dados Pessoais);
8. Informar a ANPD caso haja violação de dados pessoais.

3.1.3 Processador

Também chamado de Operador, conforme disposto nos artigos 5º, 37, 38 e 42 da LGPD, o Processador é uma empresa denominada como "Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador". Os deveres do Processador são:

1. Manter o registro das atividades de processamento;
2. Detalhar as categorias de processamento de dados;
3. Implementar medidas técnica e organizacionais para proteção de dados;
4. Informar o Controlador caso haja uma violação de dados pessoais;
5. Reparação de danos causados devido à violação de dados.

Vale ressaltar que a LGPD isenta o Processador da obrigatoriedade de nomer um DPO. Contudo, considerando a abrangência do tratamento de dados feito pelo Processador, é recomendado que esse indique um DPO para que possa atuar junto a todas as partes envolvidas.

3.1.4 Encarregado de Proteção de Dados (DPO)

Conforme disposto nos artigos 5º e 41 da LGPD, o DPO é "Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)." As atribuições e características do DPO são:

1. Atuar como interlocutor entre o Controlador, os Titulares e a ANPD;
2. Pode ser Colaborador ou Terceiro (desde que não haja conflito de interesse);
3. Deve ter seu contato divulgado para os Titulares e ANPD;
4. Deve ser envolvido em todas as questões de proteção de dados pessoais;
5. Deve se reportar diretamente à alta Diretoria;
6. Deve monitorar conformidade legal e aconselhar o Controlador quanto a isso;
7. Deve orientar quanto à realização de avaliação de impacto sobre dados pessoais (AIPD);
8. Deve promover programas de treinamento para pessoal.

A LGPD determina a obrigatoriedade da nomeção de um (ou mais) DPO, para todas as organizações que realizam o tratamento de dados pessoais. Para [13], a exigência do DPO, acaba por criar mais dúvidas que certezas. Isso porque o texto da LGPD não é claro sobre o porte das empresas que deverão obrigatoriamente contratar um DPO.

3.1.5 Titular

Conforme disposto nos artigos 5º, 9, 17 e 18 da LGPD, o Titular é "Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". É o indivíduo cujos dados estão sendo coletados e/ou tratados pelo Controlador. Os direitos dos Titulares são:

1. Confirmação da existência de tratamento;
2. Acesso aos dados;
3. Correção de dados incompletos, inexatos ou desatualizados;
4. Anonimização, bloqueio ou eliminação de dados;
5. Portabilidade dos dados a outro fornecedor;
6. Eliminação dos dados (esquecimento);

7. Informações sobre o compartilhamento de dados com terceiros;
8. Informações sobre a possibilidade de não fornecer o consentimento;
9. Revogação do consentimento.

3.1.6 Fundamentos legítimos

Conforme descrito no artigo 6º da LGPD, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

1. Finalidade: Propósito legítimo, específico, explícito e informado ao Titular;
2. Adequação: Processamento restrito apenas à finalidade informada ao Titular;
3. Necessidade: Processar o mínimo necessário de acordo com a finalidade;
4. Livre acesso: Garantir ao Titular acesso facilitado e gratuito aos seus dados;
5. Qualidade dos dados: Os dados devem ser claros, exatos e atualizados;
6. Transparência: Informações claras e precisas quanto aos tratamentos aplicados;
7. Segurança: Adoção de medidas técnicas e organizacionais para proteção dos dados;
8. Prevenção: Ações preventivas quanto a violações de segurança;
9. Não discriminação: Proibido uso de dados para fins discriminatório, ilícitos ou abusivo;
10. Responsabilização: Demonstração das medidas adotadas para o cumprimento da LGPD.

Para [2], a boa-fé no tratamento de dados pessoais é premissa básica para que as organizações possam coletar e/ou processar dados pessoais. Preocupações como tratar os dados para atingir um objetivo específico e limitado, coletar o mínimo de dados necessários, ter o consentimento do titular dos dados, avaliar as consequências de possíveis violações de dados, são exemplos de ações que a organização pode tomar para poder comprovar o princípio da boa-fé. Segundo o Tribunal de Justiça do Distrito Federal, “a boa-fé objetiva é um princípio basilar do direito do consumidor, segundo o qual as partes possuem o dever de agir com base em valores éticos e morais da sociedade. Desse comportamento, decorrem outros deveres anexos, como lealdade, transparência e colaboração, a serem observados em todas as fases do contrato.” Isso demostra que mesmo antes da LGPD, o princípio da boa-fé, no que abrange o consumo de bens e serviços, já é, por lei, um direito do consumidor. Para a LGPD, esse direito passa a ser premissa para o tratamento de dados pessoais.

3.1.7 Finalidade

Conforme disposto no artigo 7º da LGPD, o tratamento de dados pessoais só poderá ser realizado em pelo menos uma das seguintes hipóteses:

1. Consentimento do Titular;
2. Cumprimento de obrigação legal ou regulatória;
3. Pela Administração Pública para a execução de política pública;
4. Pesquisa científica, garantindo a anonimização do dados;
5. Execução de contrato;
6. Processo judicial, administrativo ou arbitral;
7. Proteção da vida (quando há risco de morte);
8. Tutela da saúde realizado por serviço de saúde ou autoridade sanitária;
9. Interesse legítimo do Controlador (*maior margem para discussão);
10. Proteção de crédito.

Para [2], a base da LGPD é o consentimento, ou seja, é necessário solicitar a autorização do titular dos dados, antes do tratamento ser realizado. Esse consentimento deve ser recebido de forma explícita e inequívoca. O não consentimento é a exceção. Só é possível processar dados, sem autorização do cidadão, quando isso for indispensável para cumprir situações legais, previstas na LGPD e/ou em legislações anteriores, como a Lei de Acesso à Informação (LAI). Caberá ao Controlador comprovar qual das bases legais suporta o tratamento de dados por ele realizado. O consentimento é considerado uma das bases mais difíceis de ser implementada, pois demanda que a organização comprove quando e como o titular consentiu com o tratamento de seus dados. Além disso, a organização também terá que adotar mecanismos para permitir que o titular revogue seu consentimento a qualquer momento.

3.1.8 Dados Sensíveis

Segundo [5] a LGPD através da padronização de normas e práticas voltadas a segurança e governança de dados pessoais, pretende estabelecer um cenário de segurança jurídica para promover a proteção aos dados pessoais de todo cidadão, de forma justa, clara e igualitária. Para isso, a fim de evitar confusão, a lei estabelece o que são dados pessoais e cria uma subdivisão chamada de dados pessoais sensíveis. Para esses dados, a lei traz exigências ainda mais restritivas, conforme disposto nos artigos 5º e 11 da

LGPD. São considerados dados pessoais sensíveis as informações que contenham a origem racial ou ética, opção religiosa, filosófica, política, sexual, filiação sindical, dados de saúde, biológicos ou genéticos. Esse conjunto de dados só poderá ser tratados pelas organizações caso cumpra com um dos critérios abaixo:

1. Consentimento do Titular para finalidade específica;
2. Cumprimento de obrigação legal ou regulatória;
3. Execução de políticas públicas;
4. Pesquisa científica (homologada por academias);
5. Declaração de defesa em processo judicial;
6. Proteção da vida do Titular;
7. Tutela da saúde, realizado por autoridade sanitária;
8. Prevenção à fraude e à segurança do Titular;

3.1.9 Governança

Conforme estabelecido no artigo 50 da LGPD, os Controladores e/ou Processadores, no exercício de atividades que envolvam a coleta, armazenamento e/ou processamento de dados pessoais, deverão comprovar a adoção de medidas de governança que:

1. Demonstrem comprometimento em adotar práticas de proteção de dados;
2. Abranjam todos os dados pessoais independente de quem realizou a coleta;
3. Sejam compatível a estrutura e volume de suas operações;
4. Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação de impacto e risco a privacidade;
5. Estabeleçam relação de confiança com o Titular por meio de atuação transparente;
6. Integrem plano de proteção de privacidade à estrutura geral de governança;
7. Estabeleçam plano de resposta a violações e remediações;
8. Promovam o monitoramento e melhoria contínua do programa de privacidade;

3.1.10 Penalidades

Caso a organização não esteja em conformidade com a LGPD, poderá sofrer sanções administrativas que vão desde uma advertência, multas e até a suspensão do serviço que envolva tratamento de dados pessoais. Essas penalidades poderão ser aplicadas tanto no caso em que haja uma violação envolvendo dados pessoais, como por exemplo, no vazamento de dados pessoais, quanto no caso da não adoção das normas e práticas estabelecidas pela LGPD, como por exemplo, no caso de uma fiscalização na qual a ANPD encontre indícios de não conformidade com a LGPD. Em outras palavras, não precisa necessariamente ocorrer um vazamento de dados pessoais para que a organização seja penalizada pela ANPD. Conforme o artigo 52, as sanções administrativas passíveis de serem aplicadas são:

1. Advertência;
2. Multa simples de até 2% do faturamento da empresa ou grupo econômico, limitada à R$ 50.000.000,00 (cinquenta milhões de Reais) por infração;
3. Publicização da infração;
4. Bloqueio dos dados pessoais a que se refere a infração;
5. Eliminação dos dados pessoais a que se refere a infração;
6. Eventuais sanções administrativas, civis e penais definidas em legislação específica.

Conforme publicado no site da Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) [3], até o dia 4 de junho de 2022, as multas aplicadas pela ANPD por não conformidade com a LGPD, superaram a marca dos 4 milhões de reais. A Figura 4 relaciona as multas com os valores mais expressivos.

Data	Estado	Emissor	Valor [R$]	Condenações	Segmento	Descrição
18/03/2021	SP	TRF3	R$2.500.000,00	Obrigação de Fazer e Indenização pecuniária ao Fundo de Direitos Difusos	Mercado de software	Proteção ao titular de coleta automática de dados pessoas quando do uso do sistema Operacional Windows 10 da Ré, tornando as informações sob seu controle. (LGPD, art. 6º, II; Cf, art. 5º,X, MCI, art. 7, II e IX)
25/09/2020	RS	TRT4	R$1.000.000,00	Indenização por Danos Morais Coletivo	Seguradora	Desvio de Finalidade. Compartilhamento indevido de dados pessoais a terceiro. Art 198 do CTN; art. 13-A da Lei 11.442/2007. (Art.5,X)
16/01/2019	DF	MP/DFT	R$500.000,00	Indenização por Danos Morais Coletivo	Vendas On-Line	Incidente de segurança que gerou o comprometimento de dados pessoais de clientes. (Art.7,I,VII)
12/05/2021	SP	TJ/SP	R$100.000,00	Indenização por Danos Morais Coletivo	Metrô	Coleta e armazenamento ilícitos de dados sensíveis (dados biométricos) em plataforma digital do Metrô sem consentimento de usuários para fins comerciais que beneficiam exclusivamente a Re e empresa terceira. (art. 17, ECA; Art. 227, da CF/88; Art. 6º, I e Art. 11, II e art. 14 da LGPD; Art. 5, X da CF/88; art. 6, III e IV e 31 do CDC)
04/06/2018	RJ	TJ/RJ	R$50.000,00	Indenização por Danos Morais	Empresa de Comunicação e Estado	Vazamento de dados pessoais sigilosos em posse do Estado por empresa de comunicação. (art.5,X)

Figura 4 – Multas aplicadas pela ANPD. Fonte: Adaptada de [3].

3.2 REVISÃO DA LITERATURA

A análise da literatura levou em consideração os temas discutidos pelos autores, suas propostas e realizações. Os trabalhos analisados foram comparados entre si, a partir dessa comparação, pode-se observar que a LGPD passou a ser uma preocupação em diversos segmentos e em diferentes organizações.

Considerando que a LGPD passou a vigorar em 2020, estamos tratando de uma situação totalmente nova, mas que dispõe de alguns casos que podemos utilizar como referência. Para isso, foi feita uma busca na literatura sobre trabalhos relacionados em diferentes bases científicas, como o IEEE, Scopus e ACM.

Observou-se a publicação de trabalhos que apresentaram os impactos da LGPD no setor Médico [14], Financeiro [10], Mídias Sociais [15], E-Commerce [16], entre outros. Em comum, esses trabalhos apresentaram a preocupação de adotar medidas capazes de elevar o nível de segurança, voltado à proteção de dados pessoais, para um nível de maturidade alinhado com a LGPD. Os estudos analisados indicam o receio das empresas quanto à aplicação de multas, entre outras penalidades relacionadas ao descumprimento da LGPD. As não conformidades em relação a LGPD poderão surgir, não necessariamente, pela má-fé das organizações em negligenciar a lei, mas também pela falta de conhecimento em relação às novas exigências legais.

Os trabalhos analisados, apontam que as organizações estão preocupadas em compreender os impactos da LGPD, os altos custos com a implementação de medidas mitigatórias e as penalidades que poderão ser aplicadas pela ANPD pela não conformidade com a lei. Se por um lado as preocupações são de aspectos negativos, por outro lado, a pesquisa realizada por [17], aponta que muitas organizações estão enxergando novas oportunidades de negócio justamente por conta da nova lei. De acordo com a pesquisa feita por [17], 84% das pessoas entrevistadas indicaram que a regulamentação voltada à proteção de dados pessoais e privacidade trouxe impactos positivos aos seus negócios. Segundo o autor, muitas empresas estão entendendo que investir em proteção de dados e privacidade pode gerar valor agregado aos negócios, se tornando um diferencial relevante na hora da escolha do consumidor.

A Figura 5 apresenta os pontos de convergência entre os trabalhos analisados. Na coluna “CONTRIBUÇÕES DOS AUTORES” lista as principais contribuições do(s) autor(es), enquanto na coluna “RELAÇÃO COM O FRAMEWORK GAIA LGPD” é feito um relacionamento entre os pontos tratados pelo(s) autor(es) com o Framework GAIA LGPD.

Estabelecer um modelo de trabalho para que as organizações possam estar alinhadas com a LGPD é um assunto relativamente novo. Apesar da lei ter sido criada em 2018 e sancionada em 2020, a Autoridade Nacional de Proteção de Dados (ANDP) só começou

TÍTULO	AUTORES	REFERENCIA	CONTRIBUÇÕES DOS AUTORES	RELAÇÃO COM O FRAMEWORK GAIA LGPD
A Telemedicina na Saúde Suplementar e a Responsabilidade Civil do Médico	Guilherme Magalhães Martins Carlos Andre Coutinho Telles	7 Journal of Institutional Studies Revista Estudos Institucionais, v. 7, n. 1, p. 182-197, jan./abr. 2021	1) A necessidade de **tratamento de grandes volumes de dados sensíveis** faz com que a LGPD seja objeto de observância pelos prestadores de serviços médicos. 2) Os autores sustentam que o legislador optou por um regime de **responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente causador de danos a seus titulares.** **3) Responsabilidade proativa,** impondo a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. 4) Os **desafios da sociedade moderna na proteção de dados,** principalmente no que tange à **relação de confiabilidade do titular de dados.**	1) O Framework pode ser aplicado em empresas de diferentes portes e setores, inclusive para prestadores da área de saúde. 2) O princípio da minimização dos dados é observado pelo Framework na etapa de levantamento do nível de maturidade segue todo o ciclo do PDCA. 3) O Framework atende todos os artigos da LGPD, e os entregáveis de cada etapa server como evidência de demonstração da boa-fé no cumprimento da LGPD. 4) O Framework dispõe de uma categoria que trata exclusivamente dos direitos dos titulares.
Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira	Tiago Celidonio Paulo Sergio Neves Claudio Melim Doná	Brazilian Journals of Business, 20/08/2020 Braz. J. of Bus., Curitiba, v. 2, n. 4, p. 3626-3648 out. /dez. 2020	1) Dificuldade de entendimento sobre como implementar os controles da LGPD. 2) O mapeamento dos requisitos da LGPD voltado a instituição Financeira. 3) A experiência de especialistas em diferentes áreas permitiu a concepção de uma metodologia eficiente que pode se validada em empresa de grande porte. 4) Plano de resposta a incidentes que atenda o direito dos titulares. 5) Revisão dos modelos de negócio para a implementação de produtos e serviços dentro dos conceitos "Privacy by design e Privacy by default". 6) O método de pesquisa-ação utilizado chama-se Metodologia para a Conformidade com o SGPI – Sistema de Gestão da Privacidade da Informação. 7) A necessidade de criar um roteiro de ação totalmente baseado em riscos, estabelecendo objetivos claros em colaboração com as áreas de negócios. 8) Formalizar a governança do programa de gerenciamento de privacidade, fornecendo orientações sobre os papéis e as responsabilidades de cada um.	1 e 2) O Framework pode ser aplicado em qualquer tipo de organização. 3) O Framework foi desenvolvido a partir da entrevista com especialistas em áreas correlatas, que responderam positivamente para o uso do Framework. 4) O Framework oferece métodos para a adoção de um plano de resposas as violações envolvendo dados pessoais. 5) O Framework identifica o nível de maturidade da empresa em realação ao "privacy by design" e oferece métodos para a implementação de novos projetos. 6) O Framework utiliza o ciclo do PDCA para o planejamento, implementação e melhoria de um Programa de Proteção de Dados Pessoais (PPDP). 7) Uso de questionário para análise do nível de maturidade, riscos e elaboração do plano de ação. 8) O Framework possui uma atividade e template específico para a definição de papéis e responsabilidades dos envolvidos.
Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações	Luiz Paulo Carvalho Jonice Oliveira Claudia Cappelli	Programa de Pós Graduação em Informática Universidade Federal do Rio de Janeiro (UFRJ) Rio de Janeiro RJ Brasil - 2019	1) Os dados estão sendo considerados o recurso mais valioso do mundo. 2) Questões éticas emergiram para tratar das ascenção da geração de dados. 3) Governos reforçaram legislações sobre o tratamento de seus próprios dados. 4) Desinformação, como fake news, utilizando dados pessoais são disseminadas e espalhadas de forma rápida e descontrolada. 5) A relevancia da LGPD em relação aos dados utilizados nas Redes Sociais. 6) Recomendação para não negligenciar a LGPD a fim de tirar vantagem ou para garantir o seu bem próprio.	Os temas abordados pelos autores desse artigo estão diretamente relacionado com a motivação inicial para o desenvolvimento do Framework, uma vez que a proteção de dados pessoais e privacidade tem se tornada cada vez mais relevantes para a sociedade de forma geral.
Uma Análise Sobre o Uso de DLTs no Tratamento de Dados Pessoais: Aderência aos Princípios e Direitos elencados na LGPD	Anderson Boa Morte Anália Meira Rostand Costa Dênio Mariz	Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB) - 2020	1) Uso de DLT (Distributed Ledger Technology), mais especificamente a blockchain, para tratamento de dados pessoais em conformidade com a LGPD. 2) Análise de documentos regulatórios relacionados com o GDPR, para compilar definições, destacar problemas e desafios inerentes ao processo de utilização da DLT visando estabelecer a conformidade com as normas. 3) Situação de tratamento de dados pessoais utilizando-se de blockchain deve ser analisada individualmente, caso a caso. 5) Devido a características como segurança, transparência e descentralização, DLTs podem ser bastante úteis para o tratamento de dados pessoais em conformidade com LGPD.	Apesar do Framework não fazer uso do DLT para a criação de um Programa de Proteção de Dados Pessoais, as preocupações, que levaram os autores desse artigo a considerarem o uso do DLT para a proteção de dados pessoais, são as mesmas preocupações que foram consideradas para o desenvolvimento do Framework. Um outro aspecto também aponta para a necessidade da adoção de serviços e tecnologias existentes para cobrir requisitos técnicos listados na LGPD.
A Framework for Information Security Governance and Management	Marian Carcary Karen Renaud Stephen McLaughlin Conor O'Brien	Maynooth University, Ireland - 2016	1) Orientações práticas e um kit de templates para implementação da governança da segurança da informação. 2) A governança de segurança da informação passa a ter papel essencial nas orgnizações; 3) Os frameworks atuais são mais teóricos e de alto nível, não oferencendo informações práticas; 4) Utiliza práticas de governança do COBIT para fazer a governança de segurança da informação. 5) Questionário para levantamento do nível de maturidade. 6) Uso do resultado do questionário para análise das vulnerabilidades e criação e Plano de Ação.	1) Questionário para levantamento do nível de maturidade; 2) Uso de métodos do COBIT na etapa de classificação do nível de maturidade e definição de plano de governança voltado a privacidade e proteção de dados pessoais; 3) O Framework oferece um kit de templates contendo ferramentas práticas para a correção das não conformidades.
Effective frameworks for delivering compliance with personal data privacy regulatory requirements	Ilya Kabanov	CDI Corporation, Cambridge, MA, USA 2016	1) As adequações a GDPR agrega valor aos negócios através da vinda de novos clientes. 2) Necessidade das empresas adotarem um framework voltados a análie e mitigação de riscos e conformidades. 3) As 4 fases do framework: Análise de Riscos; Mitigação de Riscos; Validação das evidências de correção; Auditoria. 4) Os sistemas de TI deverão observar os aspectos de conformidade durante todo seu ciclo de vida (privacy by desing). 5) O framework é um componente chave para que as empresas possam adotar um plano de governança de privacidade "privacy by desing". 6) Papel fundamental do framework para reduzir o tempo de entrega de novos projetos e serviços uma vez que ele estabelece uma sequência de etapas e resulta nas ações necessárias para a conformidade com a GDPR.	1) Implementação de um plano de comunicação público externo. 2 e 3) O Framework contempla as etapas de: Levantamento do nível de maturidade; Análise das vulnerabilidades; Classificação dos riscos; Definição do Plano de Ação. 4 e 5) O Framework aplica o "privacy by desing" e utiliza o método PDCA em busca da melhoria contínua e agregar valor ao negócio. 6) A complexidade e esforço para alinhamento com a LGPD, foi o desafio central que resultou no Framework Gaia.

Figura 5 – Comparativo entre artigos. Fonte: Próprio Autor.

a vigorar em 2021, de forma que sua atuação ainda não é amplamente conhecida.

O que podemos tomar como base são os 64 artigos da LGPD, os trabalhos analisados na pesquisa literária dessa dissertação, informações de websites especializados e da própria ANPD. Oberva-se em [18] um modelo muito similar ao que foi adotado pelo Framework GAIA LGPD, onde se utilizou de práticas voltadas a Gestão de Serviços de

TI, para se desenvolver um framework voltado a atender os requisitos da LGPD. Em seu trabalho, o autor de [18] discorre sobre a importância da adoção de um framework para a implementação de um Programa de Gestão de Privacidade. O autor defende que o framework é fundamental para que as ações de adequações às exigências da LGPD possam ser implementadas rapidamente, de forma a reduzir custos com a implementação de novos produtos e serviços.

Outra similaridade entre o Framework GAIA LGPD e o modelo apresentado por [18], está no uso do COBIT, que serviu como referência para a adoção de uma etapa inicial de levantamento do nível de maturidade. Além disso, o COBIT também serviu como base para o modelo de Governança proposto, tanto no trabalho apresentado por [18], quanto para o desenvolvimento do Framework GAIA LGPD. Outro ponto em comum entre os trabalhos, está na definição de uma etapa de análise de riscos, que antecede a etapa da elaboração do Plano de Ação. Assim como no Framework GAIA LGPD, o autor de [18] também desenvolveu um kit de ferramentas que irá ajudar as empresas na jornada de alinhamento com a LGPD, porém, esse kit não foi apresentado no artigo publicado por [18], inviabilizando sua comparação com o Framework GAIA LGPD.

A principal diferença entre esses dois trabalhos, está no método utilizado como base da autoavaliação e consequentemente, na definição das ações de adequação. Enquanto o Framework GAIA LGPD utilizou, para o desenvolvimento da etapa de autoavaliação, os 64 artigos da LGPD [4], que antecede a etapa de análise de vulnerabilidades, o autor de [18], adotou a ISO/IEC 27701:2019. A diferença entre essas duas abordagens é que a ISO/IEC 27701:2019 foi elaborada com base na ISO 27001 e ISSO 27002 e trata de aspectos gerais de segurança da informação, enquanto que referenciar os artigos da LGPD, implica em fazer uma referência direta com a lei, de forma que é possível assegurar que ao atender aos requisitos listados no questionário do Framework GAIA LGPD, a empresa estará alinhada com a LGPD.

O trabalho [9] também apresentou uma grande similaridade com o Framework GAIA LGPD. Nesse trabalho o autor defende o uso de um framework para guiar a organização na estruturação das ações necessárias para aderir ao nível de conformidade com a GDPR (General Data Protection Regulation), que é a lei utilizada pelos países da União Europeia, para regulamentar o tratamento de dados pessoais em território Europeu.

Em seu trabalho, o autor de [9] estabelece 4 fases para o seu framework: Análise de Riscos; Mitigação de Riscos; Validação das evidências de correção; Auditoria. O que é muito similar às etapas adotadas pelo Framework GAIA LGPD, apresentadas acima nesse capítulo. Uma das diferenças entre os trabalhos é que no Framework GAIA LGPD a etapa de Auditoria faz parte de uma atividade que acontece na etapa de levantamento de melhorias, e a Auditoria pode ou não acontecer, dependendo da necessidade de cada organização, enquanto que para [9], a Auditoria é a única ação da etapa final.

Outra diferença é que no Framework GAIA LGPD o método utiliza o ciclo do PDCA, fazendo com que ao final da última etapa, o ciclo seja iniciado novamente. Por fim, o trabalho apresentado por [9] tem como objetivo atender os requisitos da GDPR, enquanto o Framework GAIA LGPD tem como objetivo atender à LGPD.

Apesar da similaridade entre ambas as leis (GDPR e LGPD) ainda é possível observar aspectos diferentes entre elas, como a ANDP, que na GDPR tem um papel mais independente e uma ação mais orientativa, em compração com a LGPD, conforme aponta [19].

Além da comparação com as publicações analisadas na pesquisa literária, o Framework GAIA LGPD também foi comparado com ferramentas oferecidas por empresas como a PrivacyTools (www.privacytools.com.br). A vantagem em se utilizar o Framework GAIA LGPD em relação a outras ferramentas ofertadas, como por exemplo a PrivacyTools, está no baixo custo, na transparência e na escalabilidade que o Framework GAIA LGPD oferece. O custo das ferramentas como a PrivacyTools, é relativamente alto, uma vez que além de pagar pelo uso do serviço, a organização também deverá contratar um serviço de Consultoria e/ou adquirir outros serviços ofertados.

Ao contrário do Framework GAIA LGPD, as demais ferramentas não trazem de forma aberta os critérios adotados para resultar no plano de ação. Outra diferença está no fato de que o serviço de levantamento de maturidade normalmente, vem acompanhado com a venda de soluções voltadas a atender a LGPD, caracterizando a falta de segregação de funções, uma vez que o mesmo fornecedor que identifica as vulnerabilidades, também oferece a venda da solução de mitigação.

Por fim, ao contrário do Framework GAIA LGPD, que é oferecido em código aberto e que pode ser facilmente customizado pela organização, as ferramentas de mercado são em código fechado, não permitindo alterações no nível de calibração da maturidade e, muitas vezes, tratam a etapa de autoavaliação de forma superficial, se preocupando mais na venda de serviços do que em detalhar as vulnerabilidades identificadas.

O Framework GAIA LGPD se diferencia das demais soluções similares encontradas até então por combinar em um único processo: Questões jurídicas relacionadas à LGPD; As melhores práticas de Governança de TI; Soluções de Segurança da Informação alinhadas com as melhores práticas do mercado; Um kit contendo 19 templates customizáveis, que podem ser adotados integralmente, parcialmente e/ou utilizados como referência pelas Organizações. Por esses motivos o Framework GAIA LGPD pode ser considerado como uma solução de baixo custo, pois permite às organizações utilizarem seus próprios recursos para elaborar um Plano de Ação que seja dimensionado de acordo com suas necessidades.

4 FRAMEWORK GAIA LGPD

Neste capítulo é apresentado o Framework GAIA LGPD, que tem como objetivo principal guiar as organizações na jornada de adequação à LGPD. Esse processo acontecerá por meio de levantamento do nível de maturidade, análise das vulnerabilidades, classificação dos riscos, elaboração e execução do plano de ações.

Para atingir este objetivo, o processo seguirá cinco etapas macro, que são: 1) Preparação; 2) Organização; 3) Desenvolvimento e Implementação; 4) Governança; 5) Avaliação e melhoria. A Figura 6 apresenta o fluxograma para as macro etapas do Framework GAIA LGPD.

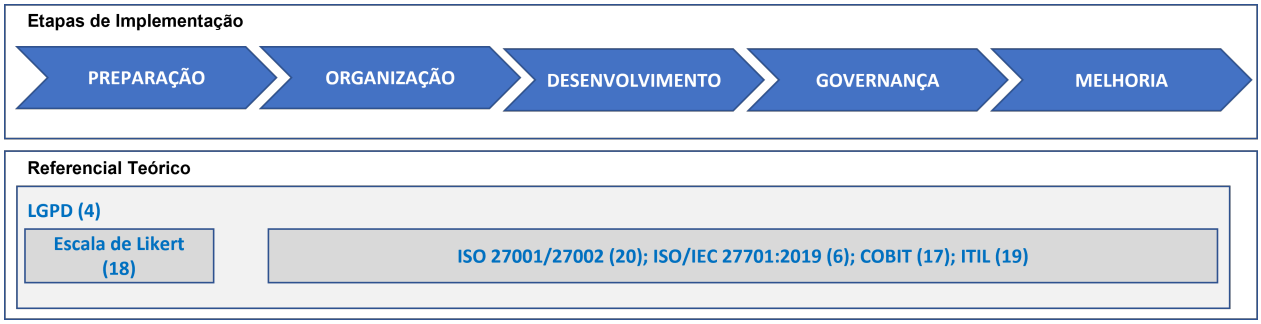

Figura 6 – Estrutura do Modelo da Framework GAIA LGPD. Fonte: Próprio Autor.

Conforme apresentado na Figura 6, o desenvolvimento das etapas de implementação, tomou como referencial teórico os seguintes métodos e conceitos: LGPD [4], Escala de Likert [20], ISO 27001/27002 [21], ISO/IEC 27701:2019 [6], COBIT [22] e ITIL [23], detalhados no Capítulo 3 dessa dissertação (Fundamentação Teórica).

4.1 PREPARAÇÃO (Etapa 1 de 5)

O propósito da etapa de Preparação, é preparar a organização para proteger os dados pessoais através da adoção das práticas e medidas listadas na LGPD. Essa etapa passa pela aplicação do questionário de autoavaliação, análise dos riscos e definição do plano de ação, conforme demonstrado na Figura 7.

4.1.1 Questionário de Autoavaliação

O objetivo do Questionário de Autoavaliação é fazer com que a empresa compare seu nível de maturidade, relacionada à proteção de dados pessoais e privacidade, com os requisitos exigidos pela LGPD. A finalidade das questões é verificar se as práticas do cotidiano ocorrem e em qual grau a organização se encontra. As opções dispostas nas

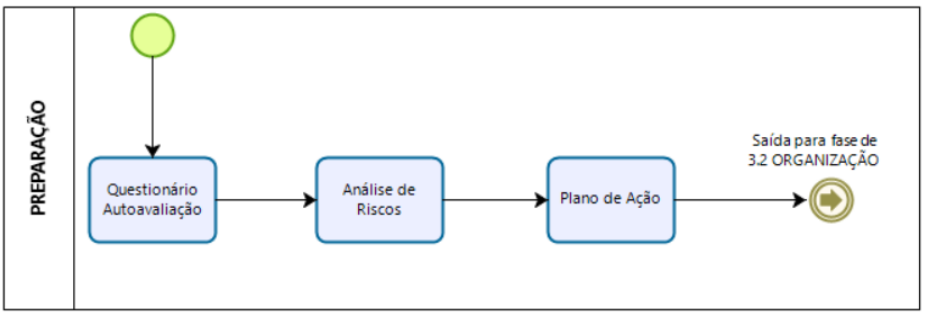

Figura 7 – Fluxograma Etapa Preparação. Fonte: Próprio Autor.

perguntas do questionário mostram situações voltadas à operação real, que ditam os níveis de implementação.

As perguntas do Questionário foram elaboradas a partir de todos os requisitos listados em todos os artigos da LGPD [4], de forma que, ao responder todas as perguntas, o entrevistado terá passado por todos os requisitos da LGPD.

O modelo da estrutura do questionário foi desenvolvido tendo como base os métodos do COBIT [22] e o escalonamento das opções de respostas utilizou a escala de Likert [20].

Para simplificar a análise da maturidade da empresa em relação à LGPD, foi adotado o uso de sete categorias, que seguiram a mesma nomenclatura adotada pela LGPD, sendo elas:

1. GOVERNANÇA: Tem por objetivo identificar em qual nível de governança a empresa se encontra em relação à proteção de dados pessoais. As questões foram elaboradas considerando as melhores práticas de Governança indicadas pelo ITIL [23], ISO 27001/27002 [21], COBIT [22], dentre outras.

   As perguntas nessa categoria visam atender aos artigos 46, 47 e 50 da LGPD.

2. TRATAMENTO DE DADOS PESSOAIS: Têm por objetivo entender como a empresa realiza o tratamento dos dados pessoais dos Titulares das informações. Esses Titulares podem ser funcionários, parceiros, clientes, entre outras pessoas que têm seus dados tratados pela empresa.

   As perguntas nessa categoria visam atender aos artigos 7º, 8º, 9º, 10, 11, 14, 15 e 16 da LGPD.

3. DIREITOS DO TITULAR: Têm por objetivo identificar qual o nível de conformidade da empresa em relação aos direitos dos Titulares de dados.

   As perguntas nessa categoria visam atender aos artigos 15, 17, 18 e 19 da LGPD.

4. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO: As questões tratadas nessa categoria se aplicam exclusivamente ao tratamento de dados pessoais realizados pelo Poder Público.

   As perguntas nessa categoria visam atender aos artigos 23, 25 e 27 da LGPD.

   Caso a empresa não trate dados pessoais em nome do Poder Público, não precisará atender a esses requisitos e deverá responder a essas questões como “Não se Aplica”.

5. TRANSFERÊNCIA DE DADOS: Tem por objetivo identificar quais as medidas de segurança adotadas pela empresa no caso de transferência de dados pessoais a outras entidades nacionais ou internacionais.

   As perguntas nessa categoria visam atender os artigos 33 e 36 da LGPD.

6. AGENTES DE TRATAMENTO DE DADOS PESSOAIS: Tem por objetivo identificar como é feito o processo de análise de privacidade, nomeação do Encarregado de Dados (DPO) e programa de treinamento no Controlador e/ou Processador(es) que tratam dados pessoais.

   As perguntas nessa categoria visam atender aos artigos 37, 38, 41 e 46 da LGPD.

7. SEGURANÇA E BOAS PRÁTICAS: Tem por objetivo identificar a adoção de medidas técnicas, físicas e organizacionais, voltadas à Segurança da informação. O levantamento desses requisitos foi embasado na ISO27001/27002 [21].

As perguntas nessa categoria visam atender aos artigos 6º, 13, 42, 48, 49 e 50 da LGPD.

Para medir o nível de maturidade em cada uma das perguntas, o respondente deverá selecionar uma resposta distribuída numa escala de 1 (não se aplica) a 5 (adota totalmente), conforme detalhado na Figura 8.

O Questionário de Autoavaliação deve ser aplicada por um Entrevistador que tenha amplo conhecimento nas práticas relacionadas a LGPD [4], ISO 27001/27002 [21], ISO/IEC 27701:2019 [6], COBIT [22] e ITIL [23]. Em adicional, o Entrevistador deverá ter habilidades para que possa orientar os Entrevistados no esclarecimento e aprofundamento de cada uma das questões. Caso a Empresa não disponha de alguém com essas habilidades, recomenda-se a contratação de especialista externo, que poderá ser encontrado no mercado como "DPO Consultor"ou "DPO As a Service".

O respondente deverá ser indicado pela Empresa conforme sua experiência nas práticas de governança de TI, Segurança da Informação, conhecimento dos processos internos, conhecimento dos contratos, conhecimento jurídico, entre outros. A Empresa poderá optar por designar um ou mais respondentes.

NÍVEL DE ADOÇÃO DA PRÁTICA	PESO	DEFINIÇÃO
Não se aplica	0	A organização entende que a prática não se aplica à sua realidade, apresentando a justificativa no campo "Comentários" ao final do questionário.
Não adota	1	A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la. Exemplo: 1) a organização sabe da necessidade de adotar a prática "dispõe de uma política de segurança da informação, formalmente instituída", mas não tomou ainda qualquer decisão no sentido de formalizar sua adoção.
Iniciou plano para adotar	2	A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares etc). Exemplo: 1) para adotar a prática "dispõe de uma política de segurança da informação, formalmente instituída", a organização elaborou plano de ação formal que estabelece as atividades, cronograma e responsáveis relativos à elaboração da política.
Adota parcialmente	3	A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização. Há, pelo menos, uma instância de execução da prática e os artefatos produzidos são evidências dessa execução. Exemplo: 1) a prática apresentada é "a organização executa processo de gerenciamento de projetos de TI". A organização, por sua vez, executa o processo de gerenciamento apenas para alguns projetos de TI, ou o processo não é executado por todas as suas unidades.
Adota integralmente	4	A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução. Exemplo: 1) para atender à prática "a organização executa processo de gerenciamento de projetos de TI", a organização possui e executa um processo de gerenciamento de projetos de TI em todas as suas unidades, ainda que o processo não esteja formalmente instituído como norma de cumprimento obrigatório.

Figura 8 – Nível de adoção das alternativas apresentadas para as questões do Questionário e Plano de Ação. Fonte: Próprio Autor.

A Figura 9 exemplifica uma questão. O questionário completo pode ser encontrado no apêndice A.

NO.	ARTIGO	CATEGORIA	REQUERIMENTO	STATUS	NOTA
1	47, 50	GOVERNANÇA	Você tem Políticas para tratar a proteção de dados? (ex.: Política de Segurança da Informação, Política Mesa Limpa, Acesso Remoto, Código de Conduta, Pol. De Privacidade, etc...)	Selecione	0

Selecione
Não se aplica
Não adota
Iniciou plano para adotar
Adota parcialmente
Adota integralmente

Figura 9 – Modelo do Questionário de Autoavaliação. Fonte: Próprio Autor.

Para apresentar o resultado do Questionário foi adotado o Gráfico Radar que contempla duas avaliações: 1º) Levantamento do nível de maturidade atual; 2º) Levanta-

mento do nível de maturidade futuro, após a implementação do Plano de Ação, conforme apresentado na Figura 10.

Figura 10 – Gráfico do Resultado da Autoavaliação. Fonte: Próprio Autor.

Um baixo nível de adesão em uma determinada categoria significa que a empresa está fora de conformidade em relação à LGPD para aquela categoria.

4.1.2 Análise de Riscos

Para a análise e classificação dos riscos levantados durante a aplicação do Questionário de Autoavaliação, foi incorporado ao Framework GAIA LGPD uma ferramenta de gerenciamento de riscos chamada "Matriz de Probabilidade versus Impacto". Essa ferramenta visual possibilita identificar rapidamente quais são os riscos que devem receber mais atenção, o que torna muito mais fácil o entendimento e engajamento das equipes nessa etapa do processo [21]. Dessa forma, a identificação dos riscos é uma etapa que deve ser feita após responder ao Questionário de Autoavaliação e antes da elaboração do Plano de Ação.

A principal vantagem do uso dessa Matriz está na facilidade que ela proporciona para visualizar informações sobre um determinado conjunto de riscos, possibilitando a tomada de decisões e a realização de medidas preventivas para tratar cada um dos riscos.

A matriz de risco consiste em uma tabela orientada por dois eixos: 1) Probabilidade; 2) Impacto. A classificação do risco é feita através da avaliação do impacto que o

risco representa para a organização, versus a probabilidade do risco se concretizar, conforme demonstrado na Figura 11.

		IMPACTO				
		5.Extremo	4.Alto	3.Moderado	2.Baixo	1.Irrelevante
PROBABILIDADE	5.Quase Certo	Muito Crítico	Muito Crítico	Crítico	Pouco Crítico	Significante
	4.Muito Provável	Muito Crítico	Crítico	Pouco Crítico	Muito Significante	Significante
	3.Pouco Provável	Crítico	Pouco Crítico	Muito Significante	Significante	Pouco Significante
	2.Improvável	Pouco Crítico	Muito Significante	Significante	Pouco Significante	Insignificante
	1.Raro	Significante	Pouco Significante	Pouco Significante	Insignificante	Insignificante

Figura 11 – Matriz de Probabilidade vs Impacto para classificação de riscos. Fonte: Próprio Autor.

A seguir esses dois eixos serão apresentados em maiores detalhes.

1) Probabilidade: A probabilidade (eixo vertical) consiste na medição de o quão provável é a ocorrência do risco. Deve-se analisar o quão fácil ou difícil é a probabilidade de que determinado risco se concretize. A probabilidade deve ser medida adotando-se os seguintes níveis: raro; improvável, pouco provável, muito provável; e quase certo. Para permitir o cálculo da classificação do risco, essas probabilidades foram convertidas em números sendo:

Quase Certo = 5

Muito Provável = 4

Pouco Provável = 3

Improvável = 2

Raro = 1

2) Impacto: O impacto (eixo horizontal) se refere às consequências do risco caso ele venha a se concretizar, ou seja, quais serão os prejuízos ou danos causados caso o risco incida de fato. O impacto também é medido em níveis, sendo eles: irrelevante, baixo, moderado, alto e extremo.

Para permitir o cálculo da classificação do risco, esses impactos foram convertidos em números, conforme apresentado a seguir:

Extremo = 5

Alto = 4

Moderado = 3

Baixo = 2

Irrelevante = 1

A classificação do risco deve ser feita comparando o resultado da multiplicação da "probabilidade x impacto", com a tabela apresentada na Figura 12.

20 a 25	Muito Crítico
16 a 15	Crítico
12 a 10	Pouco Crítico
8 a 9	Muito Significante
6 a 5	Significante
4 a 3	Pouco Significante
2 a 1	Insignificante

Figura 12 – Tabela de valores para a classificação do risco de acordo com o resultado da Probabilidade vs Impacto. Fonte: Próprio Autor.

A Figura 13 exemplifica a análise de risco para uma não conformidade. O Template completo para a Análise de Risco encontra-se no apêndice A.

						ANÁLISE ANTES DO PLANO DE AÇÃO			
NO.	ARTIGO	CATEGORIA	REQUERIMENTO	STATUS ATUAL	VULNERABILIDADE	PROBABILIDADE	IMPACTO	PESO	CRITICIDADE
1	47, 50	GOVERNANÇA	Política de Segurança	Não adota	Não conformidade com os artigos 47 e 50 da LGPD e problemas relacionados a conduta dos usuários.	Quase Certo	Extremo	25	Muito Crítico

Figura 13 – Modelo de Análise de Risco. Fonte: Próprio Autor

4.1.3 Plano de Ação

Para os riscos de maior criticidade, o Especialista pela Análise de Riscos e demais profissionais envolvidos nesse processo, deverão definir quais serão as ações mitigatórias para cada risco. Para isso, é fundamental levar em consideração as exigências da LGPD, as necessidades da Empresa, a capacidade de investimento, os recursos disponíveis, a priorização das ações, entre outros fatores que terão impactos diretos na elaboração do Plano de Ação.

A elaboração do Plano de Ação é fundamental para guiar a empresa na jornada de adequação à LGPD e também para evidenciar junto à ANPD, caso a organização venha a ser solicitada, a adoção de ações mitigatórias alinhadas com os requisitos da LGPD.

4.2 ORGANIZAÇÃO (Etapa 2 de 5)

O propósito da etapa de Organização é estabelecer as estruturas organizacionais e os mecanismos necessários para a execução do Plano de ação. Os principais entregáveis dessa etapa são:

a) Aprovar o Plano de Ação junto ao alto escalão da empresa;

b) Definir Papéis e Responsabilidades;

c) Designar e anunciar o DPO;

d) Elaborar uma "Política de Proteção de Dados Pessoais e Privacidade";

e) Estabelecer um plano de Comunicação relacionado à Proteção de Dados pessoais;

A figura 14 ilustra o fluxograma referente à etapa de Organização.

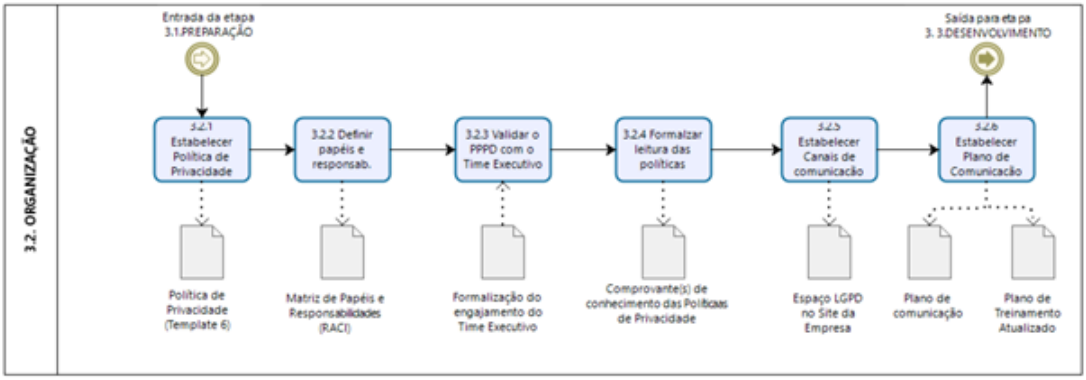

Figura 14 – Fluxograma Etapa Organização. Fonte: Próprio Autor

4.3 DESENVOLVIMENTO E IMPLEMENTAÇÃO (Etapa 3 de 5)

O propósito dessa etapa é desenvolver e implementar as ações aprovadas no Plano de Ação. A lista abaixo resume os principais, porém não os únicos, entregáveis dessa etapa:

a) Implementação das medidas técnicas e organizacionais voltadas ao controle de segurança;

b) Definir e adotar cláusulas contratuais voltadas ao cumprimento da LGPD;

c) Atualizar a Política de Segurança e códigos de conduta, com itens específicos à proteção de dados pessoais;

d) Treinar o pessoal;

e) Estabelecer, implementar e divulgar Política de Privacidade;

f) Divulgar os canais de contato do DPO;

g) Implementar procedimento para gestão do consentimento dos titulares de dados pessoais.

A figura 15 ilustra o fluxograma referente a etapa de Desenvolvimento e Implementação.

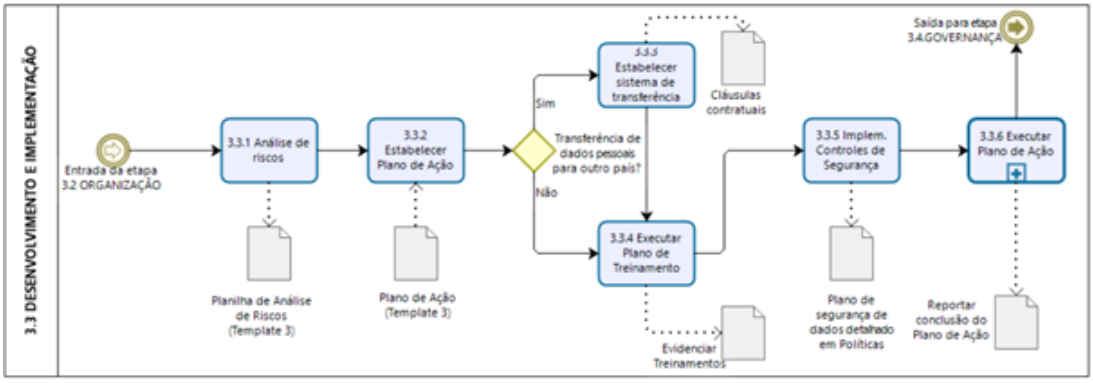

Figura 15 – Fluxograma Etapa Desenvolvimento e Implementação. Fonte: Próprio Autor

4.4 GOVERNANÇA (Etapa 4 de 5)

O propósito da etapa de Governança é estabelecer mecanismos de governança voltados à proteção de dados pessoais e privacidade. Os principais entregáveis dessa etapa são:

a) Aviso de Privacidade (para Clientes, Funcionários e Parceiros);

b) Gestão dos termos de consentimento dos titulares de dados pessoais;

c) Implementar procedimento para coleta e armazenamento de dados pessoais;

d) Implementar procedimento para coleta e armazenamento das evidência de avisos aos titulares de dados pessoais;

e) Implementar procedimento para gerenciar as solicitações dos titulares dos dados;

f) Implementar procedimento para a avaliação de riscos sobre proteção de dados (AIPDs) para novos projetos e definir em que momento essa avaliação deverá ser realizada;

g) Implementar um plano de resposta a incidentes que envolvam a violação de dados pessoais.

A figura 16 ilustra o fluxograma referente a etapa de Governança.

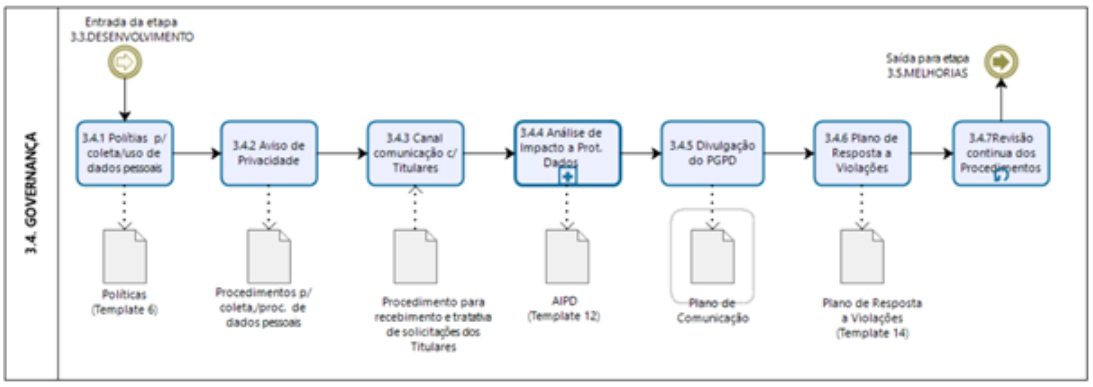

Figura 16 – Fluxograma Etapa Governança. Fonte: Próprio Autor

4.5 MELHORIA E AVALIAÇÃO (Etapa 5 de 5)

O propósito da etapa de Melhoria e Avaliação consiste em avaliar e melhorar todos os aspectos específicos de proteção de dados e privacidade da organização (controles, políticas, procedimentos, práticas, etc.). Os principais entregáveis dessa etapa são:

a) Monitorar a operação e a resolução de todas as questões relacionadas à privacidade;

b) Avaliar regularmente a conformidade com processos e políticas internas;

c) Melhorar a proteção de dados e as medidas de privacidade;

d) Implementar procedimentos para manter atualizada a política de privacidade, canais de contato com os titulares, gestão do consentimento e demais serviços relacionados à proteção de dados pessoais;

e) Implementar plano de auditoria (interna e externa) voltada à proteção de dados pessoais e privacidade.

f) Realizar autoavaliações, comparar os resultados com avaliações anteriores e atuar em relação aos itens divergentes.

A figura 17 ilustra o fluxograma referente à etapa de Melhoria e Avaliação.

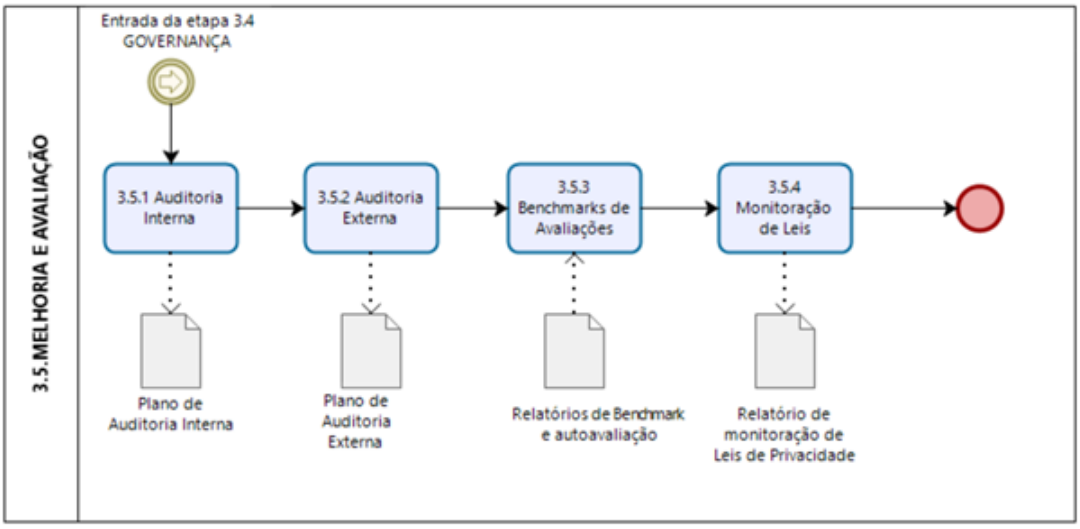

Figura 17 – Fluxograma Etapa Melhoria e Avaliação. Fonte: Próprio Autor

5 ESTUDO DE CASO

A validação do framework GAIA LGPD foi realizada através de um estudo de caso, feito com uma versão do framework e seus Templates já finalizados.

Esse trabalho foi realizado entre os meses de outubro/2021 e feveveiro/2022. Nele, o framework foi aplicado em uma empresa do setor Químico, sediada no Brasil (São Paulo) e com subsidiárias espalhadas pela América Latina, totalizando um conglomerado de 21 empresas no grupo. Essa empresa será tratada aqui como “Empresa X”.

O objetivo foi utilizar o Framework GAIA LGPD para identificar os itens de não conformidade (NC) da Empresa X em relação à LGPD, e estabelecer um plano de ação com base na análise das vulnerabilidades e classificação dos riscos das NC.

Não fez parte do estudo de caso aplicar o plano de ação proposto. Consequentemente, as etapas do framework relacionadas a implementação das ações, governança e melhoria contínua, não foram aplicadas nesse trabalho.

Esse estudo de caso contou com o acompanhamento de uma empresa especializada na área de cibersegurança, tratada aqui como “Empresa Sec”. Essa empresa está sediada em São Paulo e atua na área de segurança da informação há mais de 10 anos. A Empresa Sec alocou um especialista da área de Segurança da Informação para acompanhar todas as etapas do trabalho conforme apresentado a seguir.

5.1 ESTUDO DE CASO - AUTOAVALIAÇÃO

A autoavaliação faz parte da etapa de Preparação. Seu objetivo é verificar como se aplicam no cotidiano as práticas de proteção de dados pessoais, e com isso identificar os itens de não conformidade (NC) da Empresa X em relação à LGPD.

Essa etapa contou com a presença do Gerente de TI, de um Analista da Empresa X, de um Especialista em Segurança da Informação da Empresa Sec e do DPO Consultor, que utilizou o Framework GAIA LGPD para conduzir os trabalhos. Foram necessárias aproximadamente 10 horas para coletar todas as respostas do questionário de autoavaliação.

Um aspecto positivo que se identificou foi que a estrutura do questionário, dividido em categorias, serviu como um roteiro para as entrevistas. Outra vantagem com o agrupamento das perguntas, foi que ao se discutir um determinado assunto, uma mesma conversa captou respostas para múltiplas perguntas, otimizando assim o tempo para coletar todas as respostas.

Uma desvantagem que foi percebida com o agrupamento das perguntas, é que

tivemos perguntas com o mesmo sentido aparecendo em mais do que uma categoria, ou seja, nesses casos tivemos resposta duplicadas. Para resolver essa situação, foi mantida a pergunta na categoria com a qual ela tinha maior afinidade e removida a pergunta das categorias com menos afinidade; assim, essa situação foi resolvida de forma definitiva.

Quanto aos resultados apresentados pela Empresa X em relação à adoção das medidas de seguranças exigidas pela LGPD, podemos observar uma lacuna enorme. Um dos pontos que mais chamaram a atenção, foi de que a Empresa X não só estava desalinhada em relação a LGPD, mas também com a ISO 27001/27002, pois não adotava boas práticas de segurança já existentes no mercado e consideradas básicas, como por exemplo a adoção de uma Política de Segurança da Informação, que já é algo esperado muito antes da LGPP. O gráfico da Figura 18 mostra que a Empresa X adota apenas 3 dos 43 controles esperados para um total alinhamento com a LGPD.

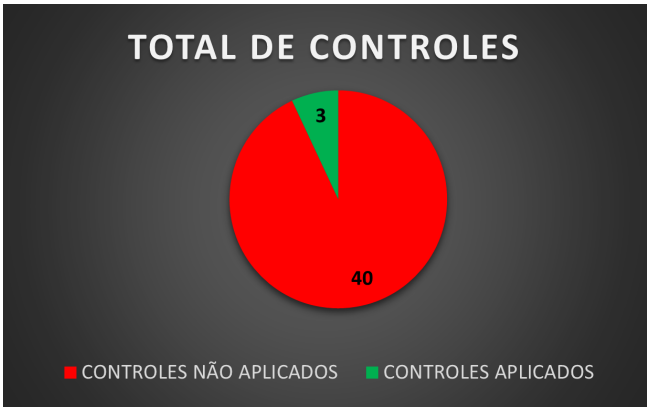

Figura 18 – Estudo de caso - Total de Controles Existentes e Faltantes.

Conforme observado no gráfico da Figura 19, apenas 1 das 11 salvaguardas prévias à LGPD estava sendo aplicada, o que leva a entender que a Empresa X fazia pouquíssimos investimentos relacionados à segurança da informação.

Em adicional aos 11 controles prévios à LGPD, temos outras 32 medidas de salvaguardas que passaram a ser legalmente exigidas a partir do momento que a LGPD entrou em vigor. Dessas 32 salvaguardas, apenas 1 estava sendo aplicada pela Empresa X.

Contabilizando os itens de não conformidade por categorias, podemos observar pelo gráfico da Figura 20 que a Empresa X está muito aquém de atender as exigências da LGPD. A pontuação ideal para cada categoria é de 4 pontos. O gráfico mostra que o maior nível de maturidade da Empresa X está na categoria de “Segurança e Boas Práticas”, no qual recebeu uma pontuação de 1,7, valor esse muito aquém do que os 4 pontos esperados.

Nas demais categorias, como Tratamento de Dados, Direito dos Titulares e Transferência de Dados, o nível de maturidade da Empresa X está muito próximo de 1, indicando assim a maior concentração dos itens de não conformidade.

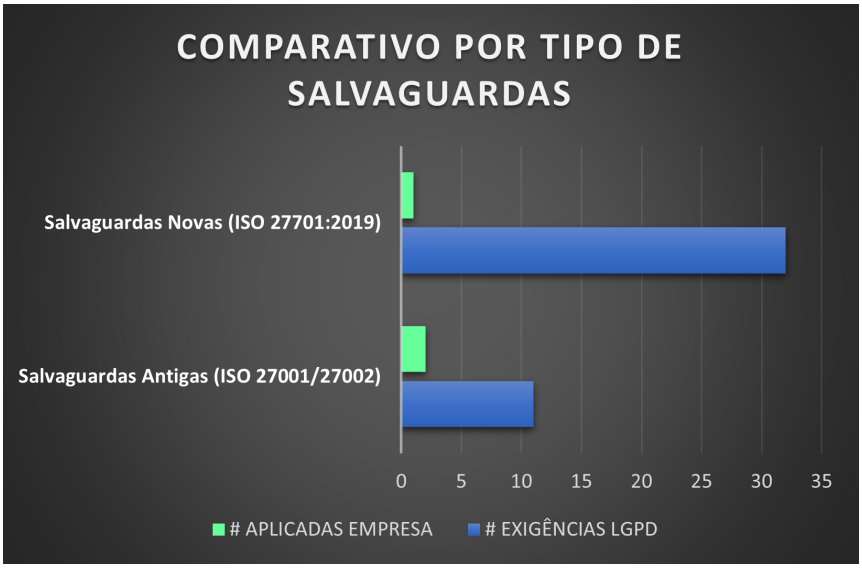

Figura 19 – Estudo de caso - Nível de Adoção das Salvaguardas Existentes antes da LGPD.

Já na categoria Tratamento de Dados Pelo Poder Público, o resultado está zerado pois essas exigências não se aplicam à Empresa X, uma vez que essa não trata dados pessoais em nome do Poder Público.

Figura 20 – Estudo de caso - Nível de Adoção por Categoria.

5.2 ESTUDO DE CASO - ANÁLISE DE RISCOS

O objetivo da análise das vulnerabilidades é identificar quais são os riscos inerentes a cada uma das não conformidades. Essa etapa foi executada pelo mesmo time que atuou na etapa da autoavaliação. Um diferencial positivo foi que pudemos contar com a contribuição de um Especialista em Segurança de TI, que pôde confirmar a existência das vulnerabilidades identificadas na etapa anterior e ajudou no levantamento dos riscos referentes às não conformidades.

Ao todo, foram 42 vulnerabilidades analisadas 43% desse total são não conformidades relacionadas às categorias de Governança e Segurança. O que chama a atenção para esse indicador é que a maioria dos controles tratados nessas duas categorias (Governança e Segurança) eram boas práticas que deveriam ser aplicadas pela empresa antes mesmo da LGPD. A Figura 21 mostra a distribuição das vulnerabilidades por categoria.

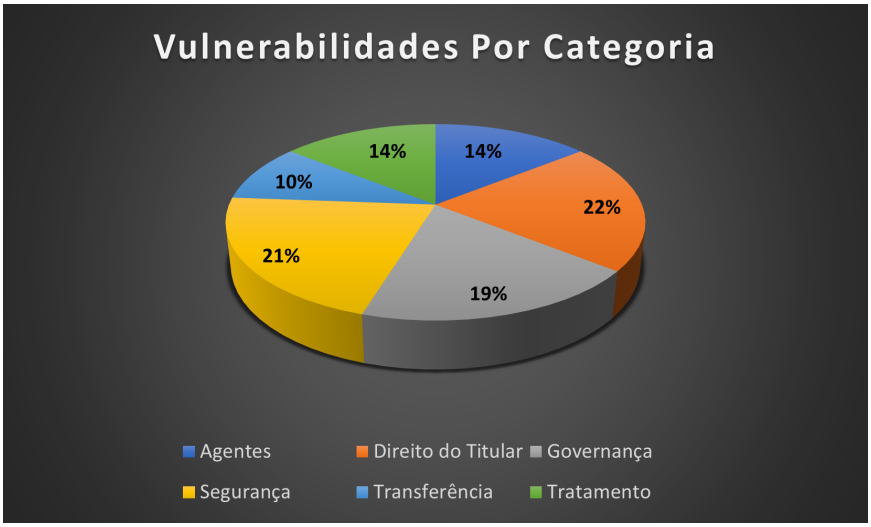

Figura 21 – Estudo de caso - Nível de Adoção por Categoria.

5.3 ESTUDO DE CASO - CLASSIFICAÇÃO DOS RISCOS

O objetivo dessa etapa é classificar os riscos que foram apontados na etapa anterior (Análise das Vulnerabilidades) para permitir que a Empresa X tenha uma visão de quais são as principais ameaças que envolvem a proteção de dados pessoais e assim priorizar um plano de ação para a mitigação dos riscos apontados.

O trabalho contou com a participação de um Especialista em Segurança da Informação, o que contribuiu na validação da matriz de análise de riscos adotada pelo Framework GAIA LGPD e resultou na classificação dos riscos conforme apresentado na Figura 18.

O resultado mostra que 65% dos riscos mapeados são críticos ou muito críticos, o que indica que, do ponto de vista da segurança da informação, a Empresa X apresenta graves fragilidades e por isso deverá tomar ações imediatas para a mitigação dos riscos identificados, conforme demonstrado na Figura 22.

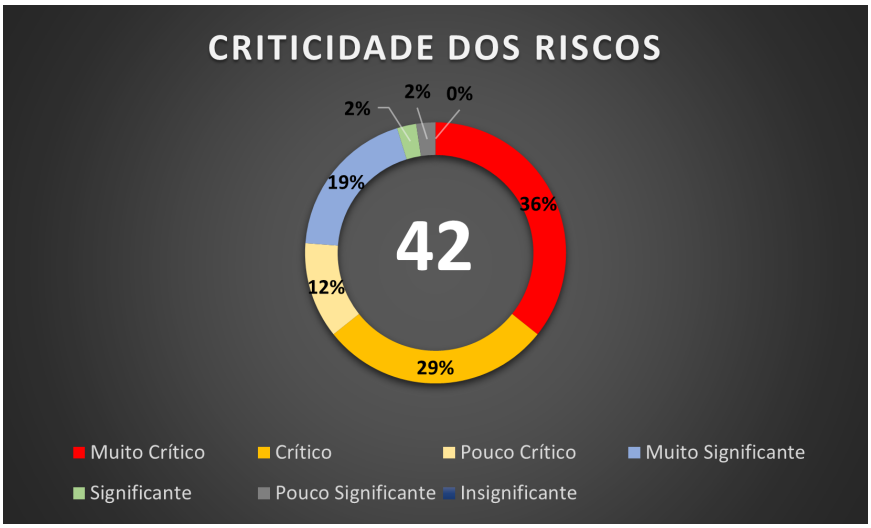

Figura 22 – Estudo de caso - Classificaçaõ dos Riscos.

5.4 ESTUDO DE CASO - PLANO DE AÇÃO

Essa etapa consiste em definir um plano de ação para cada risco identificado. Apesar do entendimento de que riscos de baixa criticidade (Insignificante ou Pouco Significante), não necessariamente demandem uma ação de mitigação, o estudo de caso realizou a classificação de todos esses riscos.

Um diferencial positivo observado nessa etapa, foi de que a participação do Analista e Gerente da TI indicados pela Empresa X, contribuiu muito para estabelecer as ações de mitigação, que foram propostas considerando as características das áreas de negócio, os recursos disponíveis da Empresa X, projetos em andamento e planejamento de melhorias futuras.

A entrega do plano de ação com os resultados obtidos nesse estudo de caso ocorreu em março de 2022, após cinco meses de projeto. O resultado trouxe como recomendação um conjunto de 59 ações para mitigar ao máximo a exposição do ambiente da Empresa X ao risco de não conformidade com os requisitos da LGPD. Cada ação de mitigação proposta visa anular e, quando não possível, reduzir ao máximo determinado risco mapeado. Caberá exclusivamente à Empresa X a decisão de aplicar ou não, total ou parcialmente, as recomendações propostas por este trabalho.

Após a execução total ou parcial do plano de ação, é recomendado que a Empresa X execute novamente o Framework GAIA LGPD, para que possa acompanhar o nível de evolução em relação à adesão à LGPD.

5.5 ESTUDO DE CASO - CONCLUSÃO

Observou-se que a execução de todas as etapas do framework, demanda do Entrevistador no mínimo duas habilidades essencias, que podem estar centralizadas em um único profissional ou, podem estar presentes em uma Equipe multifuncional. São elas:

1) Conhecimento da LGPD:

O amplo conhecimento da LGPD é fundamental para que o Entrevistador consiga confrontar as respostas com os requisitos de cada artigo; porém, sem se limitar apenas às questões listadas no Questionário e sim, buscando explorar as informações recebidas e os detalhes, que muitas vezes não aparecem de forma clara e que demandaram perguntas adicionais.

2) Experiência com Segurança da Informação:

A maioria das questões estão relacionadas a medidas técnicas e organizacionais que são adotas pela empresa para tratar cada item avalidado. Por isso é fundamental que o Entrevistado esteja familiarizado com as boas práticas de segurança da informação para que tenha um entendimento do nível de segurança de cada serviço avaliado de acordo com a resposta dos Entrevistados.

Como resultado, o estudo de caso foi capaz de entregar para a Empresa X um plano de ação estruturado, totalmente aderente às exigências da LGPD e capaz de ser aplicado pela empresa.

O plano de ação proposto foi revisado por dois experientes Especialistas em Segurança da Informação, que contribuiram com sugestões de ações mitigatórias relacionadas às deficiências apontadas na análise de riscos, além de chancelar as próprias ações indicadas com base na análise feita utilizando o framework.

Outro ponto imporante que resultou na elaboração de um plano viável de ser aplicado, foi a participação direta do Gerente de TI da Empresa X, que durante o processo de elaboração do plano de ação pôde priorizar as ações de correção que estão alinhadas com a estratégia de governança da Empresa X.

Os envolvidos nesse estudo comentaram que, após participarem da execução do framework adquiriram maior entendimento quanto aos requisitos impostos pela lei e os respectivos impactos em serviços internos e externos. Isso porque, durante a execução do questionário de avaliação, todos os artigos da LGPD são abordados e explicados, o que trouxe maior clareza quanto às exigências da LGPD para cada serviço e/ou situação

abordada.

Todo o material utilizado durante as etapas do framework e principalmente o Plano de Ação, poderão ser utilizados para evidenciar que a Empresa X está buscando um programa voltado a aumentar o nível de segurança e proteção de dados pessoais e da privacidade de seus clientes, colaboradores e demais parceiros.

Para ajudar na validação do Framework, após o estudo de caso, o framework foi compartilhado com profissionais de outras 8 empresas de diferentes portes e setores. Entre elas 1 do setor Comercial, 1 Industrial, 4 Prestadoras de serviços e 2 da Educação. Depois de analisarem o Framework, os profissionais envolvidos responderam a um questionário, que combinou perguntas qualitativas abertas e fechadas, no qual as respostas poderiam ser escolhidas entre o “discordo plenamente” e “concordo plenamente”, com o objetivo de validar o nível de aceitação e eficiência do framework. A Figura 23 apresenta o porte das empresas que participaram da avaliação do Framework e a Figura 24 informa a área de atuação dos especialistas envolvidos nessa análise.

De forma geral, 95% dos profissionais entrevistados se mostraram dispostos a utiliz o framework em suas empresas para criarem um plano de proteção de dados pessoais voltado a atender à LGPD. Outros quesitos relacionados à eficiência, clareza e recursos disponibilizados através do framerok também foram avaliados de forma muito satisfatória, conforme os resultados apresentados na Figura 25.

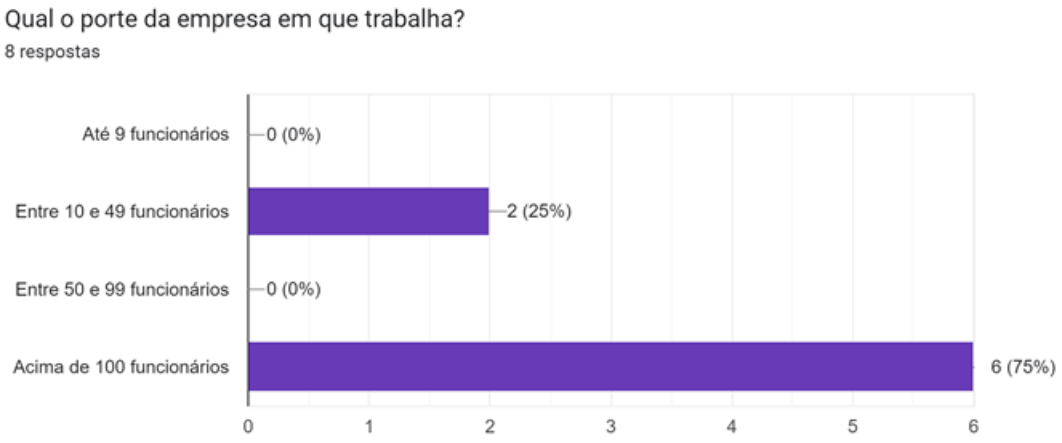

Figura 23 – Porte das empresas que avaliaram o framework.

Figura 24 – Função dos profissionais que avaliaram o framework.

Figura 25 – Avaliação da adesão do framework.

6 CONCLUSÕES E TRABALHOS FUTUROS

6.1 CONCLUSÕES

Esse estudo buscou estabelecer um modelo de trabalho que possa servir como referência para os profissionais responsáveis pela definição e implementação de medidas técnicas e organizacionais, voltadas a atender às exigências estabelecidas pela LGPD, a fim de respeitar o direito à vida privada de cada cidadão em seu âmbito familiar, garantindo, assim, seu amplo direito à liberdade.

Os resultados apresentados indicam que é possível utilizar o Framework GAIA LGPD para desenvolver e implementar um Programa de Privacidade dimensionado de acordo com a necessidade de cada organização.

Sua execução demanda, por parte do Executor, conhecimento técnico e habilidades relacionadas à LGPD, Governança de TI, Segurança da Informação, Gestão de Incidentes, Gerenciamento de Projetos, entre outras. A execução desse material, por parte de uma pessoa leiga nesse assunto, poderá causar um efeito contrário ao esperado, uma vez que a análise do nível de maturidade, levantamento das vulnerabilidades, classificação dos riscos e elaboração do plano de ação, poderão não estar em conformidade com a LGPD. Por isso, é essencial que esse framework seja aplicado por profissionais que detenham os conhecimentos listados acima.

Além das habilidades mencionadas, é recomendado que esse framework seja aplicado por uma pessoa externa à Organização, com total autonomia e liberdade para explorar a fundo todos os processos e serviços envolvidos e a partir desse levantamento inicial, poder apontar toda e qualquer vulnerabilidade de forma neutra e imporcial aos resultados identificados.

Além do objetivo principal, o Framework GAIA LGPD, também trouxe as seguintes contribuições:

1. Gerou evidências de que a empresa possui uma estratégia para a adequação a LGPD. O material entregue no estudo de caso, como a análise das vulnerabilidades e principalmente o plano de ação, poderá ser utilizado para comprovar a boa intenção da empresa em buscar um alinhamento com à LGPD.

2. O estudo de caso apontou que a Empresa X carece de medidas básicas de segurança da informação. Um exemplo disso é a falta de uma política de segurança da informação. Antes mesmo de se buscar ações para a proteção de dados pessoais, a Empresa X precisa adotar ações para a segurança de dados de forma geral.

3. Desenvolvimento técnico de todos os colaboradores da Empresa X que participaram do estudo de caso. O Analista e Gerente de TI, que participaram de todas as etapas do processo, receberam, mesmo que indiretamente, um treinamento voltado à LGPD. Como o Framework GAIA LGPD aborda todos os artigos da LGPD, ao final da aplicação do framework, esses profissionais haviam conhecido todos os controles exigidos pela LGPD.

4. Levantamento dos processos internos. Como parte da execução do Framework GAIA LGPD resulta na revisão dos processos internos, espera-se que ao final da execução do plano de ação, a empresa tenha mapeado todos os seus processos.

5. Gerar valor ao negócio. Além da otimização de atividades resultantes da revisão dos processos internos, a adoção de práticas de segurança propostas pelo Framework GAIA LGPD, aumentará a disponibilidade, integridade e confidencialidade das informações, o que é fundamental para a execução das atividades de qualquer empresa. Além disso, a execução do plano de ação proposto pelo framework, trará uma maior transparência em relação a como a organização trata seus dados pessoais, o que nos dias de hoje pode ser um diferencial na escolha do consumidor quanto aos produtos e serviços ofertados pela empresa. Benefícios com a valorização da marca, também é outro legado que poderá ser deixado pelo framework.

TRABALHOS FUTUROS

Observou-se durantes os estudos, que as vulnerabilidades atreladas às questões da autoavaliação do Framework GAIA LGPD, muitas vezes são comuns mesmo para organizações com diferentes características. Por exemplo, a vulnerabilidade gerada pela não adoção da medida que trata da Gestão do Consentimento do Titular é a mesma para todas as empresas que não adotam essa medida, independente do porte ou do seto de atuação dessa empresa. Da mesma forma, as ações de mitigação, também acabam se repetindo.

Utilizando o exemplo anterior, a ação para mitigar a vulnerabilidade relacionada à falta da Gestão do Consentimento do Titular seria a adoção de um processo para a Gestão do Consentimento, independentemente do tipo da organização.

Por isso, esse trabalho contempla uma base que armazena a lista de todas as vulnerabilidades e suas respectivas ações de mitigação, obtidas através da aplicação do Framework GAIA LGPD, de forma que essa base pode ser facilmente atualizada sempre que o framework for executado.

Tendo uma base robusta das vulnerabilidades e ações, como trabalho futuro, o Framework GAIA LGPD irá evoluir para uma versão automatizada, que contará com uso de RPA (Robotic Process Automation) e IA (Inteligencia Artificial), para que possa ser

executado com o mínimo de dependência humana, reduzindo assim ações manuais, que atualmente tem uma grande dependência de conhecimentos especializados nos diversos assuntos que tange à LGPD.

..

REFERÊNCIAS

[1] HORITA, F. E.; BARROS, R. M. GAIA human resources-an approach to integrate itil and maturity levels focused on improving the human resource management in software development. In: *25th International Conference on Computer Applications in Industry and Engineering, CAINE 2012 and 4th International Symposium on Sensor Network and Application, SNA 2012*. [S.l.: s.n.], 2012. v. 1, p. 51–56. ISBN 9781880843888.

[2] SERPRO. *Glossário LGPD*. 2020. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd>.

[3] ANPPD, A. N. d. P. d. P. d. D. *Manifesto pela tecnicidade dos membros do conselho diretor da Autoridade Nacional de Proteção de Dados*. 2020. Disponível em: <https://anppd.org/parecer/manifesto-pela-tecnicidade-da-anpd>.

[4] BRASILEIRO, C. *Lei Geral de Proteção de Dados (LGPD)*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

[5] CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso / Methodology for mapping and adequacy of the requireme. *Brazilian Journal of Business*, v. 2, n. 4, p. 3626–3648, 2020. ISSN 25961934. Disponível em: <https://www.brazilianjournals.com/index.php/BJB/article/view/18382/14839>.

[6] ABNT. *ISO/IEC 27701:2019*. 2019.

[7] CLIN, C. d. S. ao empresário. *Principais dificuldades das empresas para se adaptarem à lei de proteção de dados.* 2021. Disponível em: <https://clinsindihospa.com.br/principais-dificuldades-das-empresas-para-se-adaptarem-a-lei-de-protecao-de-dados/#:$\sim$:text=Dificuldadedeadequa{ç}{~{a}}o,{á}reasprecisamreceberc>.

[8] CUNHA, B. E. d. M. et al. AS DIFICULDADES DE IMPLEMENTAÇÃO DA LGPD NOBRASIL. *Revista Projetos Extensionistas | Faculdade de Pará de Minas -FAPAM*, 2021. Disponível em: <https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249>.

[9] KABANOV, I. Effective frameworks for delivering compliance with personal data privacy regulatory requirements. In: . [S.l.: s.n.], 2016. p. 551–554.

[10] COLIN, R. *Real World Research*. 2º. ed. [S.l.: s.n.], 2002.

[11] GIL, A. C. *Como elaborar projetos de pesquisa*. 4º. ed. São Paulo: [s.n.], 2002.

[12] RUNESON, P.; HöST, M. Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, v. 14, 4 2009. ISSN 1382-3256.

[13] FERREIRA, F. *LGPD: por que você não pode mais esperar para se adaptar*. 2020. Disponível em: <https://lozinskyconsultoria.com.br/estrategia-e-gestao-de-ti/lgpd-por-que-voce-nao-pode-mais-esperar-para-se-adaptar/>.

[14] MARTINS, G. M.; TELES, C. A. C. A TELEMEDICINA NA SAÚDE SUPLEMENTAR E A RESPONSABILIDADE CIVIL DO MÉDICO NO TRATAMENTO DE DADOS À LUZ DA LGPD. *REI - REVISTA ESTUDOS INSTITUCIONAIS*, v. 7, n. 1, p. 182–197, apr 2021. ISSN 2447-5467. Disponível em: <https://estudosinstitucionais.emnuvens.com.br/REI/article/view/608>.

[15] CARVALHO, L. P.; OLIVEIRA, J.; CAPPELLI, C. Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendaçõesNo Title. 2019.

[16] SAUER, A. C.; MOREIRA, J. P. LGPD - Lei Geral de Proteção de Dados. In: 6º Seminário de Tecnologia, G. e. E.; EGRESSOS, I. J. A. . S. de (Ed.). [S.l.: s.n.], 2021.

[17] MCKENZIE, B. . *Preparing for new Privacy Regimes: Privacy Professionals View on the General Data Protection Regulation and Privacy Shield*. 2016. Disponível em: <http://f.datasrvr.com/fr1/416/76165/IAPP_GDPR_and_Privacy_Shield_Survey_Report.pdf>.

[18] CARCARY, M. et al. A framework for information security governance and management. *IT Professional*, v. 18, p. 22–30, 2016.

[19] LORENZON, L. N. ANÁLISE COMPARADA ENTRE REGULAMENTAÇÕES DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA (LGPD E GDPR) E SEUS RESPECTIVOS INSTRUMENTOS DE ENFORCEMENT. 2020.

[20] VIEIRA, S. *Como Elaborar Questionários*. [S.l.: s.n.], 2009.

[21] TÉCNICAS, A. B. D. N. *ISO/IEC 27001:2013*. 2013. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306580>.

[22] BLOKDYK, G. *COBIT 5 A Complete Guide*. [S.l.]: 5STARCooks, 2019. ISBN B07XK81S2B.

[23] AXELOS. *Itil Foundation*. 4th. ed. [S.l.: s.n.], 2019.

Apêndices

APÊNDICE A – TEMPLATE: CLÁUSULAS CONTRATUAIS

• TERMO DE ACORDO e RECIBO DE QUITAÇÃO: O CLIENTE ratifica a autorização à NOME DA EMPRESA para coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais, conforme os fins do presente termo, de exercícios de direitos da NOME DA EMPRESA e da Lei Federal nº 13.709/2018 (LGPD). O DISTRIBUIDOR assegura a NOME DA EMPRESA que detém meios suficientes e recursos necessários para tratar os dados pessoais, bem como obteve do respectivo titular a autorização para tratá-los, conforme determina a Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO DE AGÊNCIA: O AGENTE, para a execução do presente contrato, poderá acessar documentos, arquivos ou sistemas contendo Dados Pessoais, caso seja necessário. O AGENTE obriga-se a tratar os Dados Pessoais com segurança, dentro da necessidade, limite e adequação por si, seus administradores, sócios, prepostos, funcionários e terceiros. O AGENTE também se obriga a: a) estar em conformidade com a legislação específica sobre privacidade e proteção de dados vigente; b) adotar controles técnicos, administrativos, físicos e/ou digitais para proteger quaisquer Dados Pessoais a que possa ter acesso, visando a proteção contra a perda, danos, alteração, destruição, uso não autorizado, ilícito ou inadequado, acesso ou divulgação; c) tratar todo e qualquer Dado Pessoal em razão deste Contrato nos estritos termos do presente instrumento, sendo vedado qualquer tratamento de Dado Pessoal para outras finalidades que não as previstas nos termos do Contrato, aditivos ou orientações formais e por escrito da NOME DA EMPRESA; d) expor aos titulares ou outros controladores de Dados Pessoais as condições do tratamento dos dados, necessidade, finalidade e término do tratamento; e) manter registro das operações de tratamento de Dados Pessoais, incluindo-se eventuais compartilhamentos desses Dados a terceiros; f) adotar as medidas de exclusão, correção e/ou anonimização de Dados Pessoais transmitidos pela NOME DA EMPRESA, bem como replicar e exigir tais medidas de eventuais terceiros para os quais os Dados Pessoais forem compartilhados; g) obter prévia e expressa autorização da NOME DA EMPRESA para transmitir dados pessoais a quaisquer terceiros, mantendo-se em todas as hipóteses a responsabilidade do AGENTE, que se obriga a impor ao terceiro obrigações não menos rigorosas para proteção desses dados. h) permitir a auditoria por parte de autoridades governamentais competentes ou pela NOME DA EMPRESA, mediante aviso prévio, acerca do registro das operações de tratamento de Dados Pessoais, das práticas de privacidade, segurança e proteção de Dados Pessoais que sejam adotadas pelo AGENTE; i) no prazo máximo de 24 (vinte e quatro) horas de

eventual incidente ou suspeita dele, informar à NOME DA EMPRESA: (i) qualquer uso indevido, ilegal ou inadequado de Dados Pessoais; (ii) situações de acesso, uso ou aquisição de Dados Pessoais por pessoa não autorizada ou (iii) qualquer forma de comprometimento de Dados Pessoais ("Incidente"); j) cooperar totalmente com a NOME DA EMPRESA na investigação de eventual Incidente envolvendo Dados Pessoais. 1.2. Para os fins deste Contrato, "Dados Pessoais" significam as informações fornecidas ou coletadas em nome ou pela NOME DA EMPRESA e fornecidas à - ou acessadas pelo - AGENTE em razão deste Contrato, que podem ser usadas para identificar ou tornar identificável, localizar ou entrar em contato com uma pessoa natural como, por exemplo, mas não limitado a: (i) nome, idade ou sexo; (ii) endereço físico ou localização geográfica (e-mail); (iii) número de telefone; (iv) endereço de e-mail ou identificador on-line (IP); (v) dados cadastrais e números de segurança social ou identificador governamental similar (CPF, PIS/PASEP, etc.); (vi) atividade laboral exercida, informações financeiras ou da saúde; (vii) origem racial ou étnica, crenças religiosas ou filosóficas, associações a sindicatos, opiniões políticas, vida sexual, registro ou histórico criminal ou (vii) qualquer outra informação relacionada ou relacionável a uma pessoa física que seja combinada com qualquer um dos itens acima. 1.3. Ao término da relação entre as partes, deverá o AGENTE se abster de utilizar os dados pessoais que lhe tiverem sido transmitidos e/ou disponibilizados pela NOME DA EMPRESA durante a vigência do Contrato, bem como devolver ou excluir, mediante comprovação à NOME DA EMPRESA, as informações ou Dados Pessoais de funcionários, diretores, clientes ou outras pessoas da - ou fornecidos pela – NOME DA EMPRESA que estiverem em sua posse direta ou indireta. 1.4. Em caso de descumprimento de qualquer obrigação prevista nesta Cláusula, ficará o AGENTE sujeito a reparação civil e criminal, além de eventuais perdas e danos havidos pela NOME DA EMPRESA. 1.5. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO DE ARMAZENAGEM: As partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 ("LGPD"), assumindo integral responsabilidade por toda operação de tratamento de dados pessoais, desde a coleta, tratamento, armazenamento e eliminação, assegurando que o tratamento dos dados pessoais seja realizado de acordo com as finalidades específicas e consentidas pelos titulares, nos termos da legislação vigente e da Lei nº 13.709/2018 ("LGPD"). As partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, observando sua privacidade e proteção, tratando os dados pessoais coletados para fins lícitos e expressamente previstos em lei, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO

DE ARRENDAMENTO E SUBARRENDAMENTO: As partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 (“LGPD”), assumindo integral responsabilidade por toda operação de tratamento de dados pessoais, desde a coleta, tratamento, armazenamento e eliminação, assegurando que o tratamento dos dados pessoais seja realizado de acordo com as finalidades específicas e consentidas pelos titulares, nos termos da legislação vigente e da Lei nº 13.709/2018 (“LGPD”). As partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, observando sua privacidade e proteção, tratando os dados pessoais coletados para fins lícitos e expressamente previstos em lei, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO DE COMPRA E VENDA: Para as finalidades de financiamento e comercialização de insumos e produtos, conforme a Lei Federal nº 13.709/2018 (LGPD), o CLIENTE: a) autoriza a NOME DA EMPRESA a coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais, bem como repassá-los a terceiros necessariamente envolvidos na cadeia do agronegócio para avaliação, auditoria, securitização, cumprimento e execução do presente contrato; b) assegura à NOME DA EMPRESA que detém meios suficientes e recursos necessários para tratar os dados pessoais, c) assegura à NOME DA EMPRESA que obteve do respectivo titular a autorização para tratar seus dados pessoais nos termos da alínea (a).

As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO DE CESSÃO DE CRÉDITO: Para as finalidades de financiamento e comercialização de insumos e produtos, conforme a Lei Federal nº 13.709/2018 (LGPD), o CEDENTE: a) autoriza a NOME DA EMPRESA a coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais, bem como repassá-los a terceiros necessariamente envolvidos na cadeia do agronegócio para avaliação, auditoria, securitização, cumprimento e execução do presente contrato; b) assegura à NOME DA EMPRESA que detém meios suficientes e recursos necessários para tratar os dados pessoais, c) assegura à NOME DA EMPRESA que obteve do respectivo titular a autorização para tratar seus dados pessoais nos termos da alínea (a).

As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente. • CONTRATO DE CONFIDENCIALIDADE: As Partes asseguram que detém meios suficientes e recursos necessários para tratar os dados coletados conforme determina a Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). A Parte Reveladora comunicará imediatamente a Parte Receptora a respeito de qualquer solicitação do titular da informação, que diga res-

peito aos direitos assegurados pela LGPD. A Parte infratora se responsabiliza, de forma exclusiva, por toda e qualquer infração à LGPD que decorra da coleta e tratamento de dados sem a expressa autorização do titular da informação, com resguardo do direito de regresso da Parte prejudicada por eventuais prejuízos ocasionados pela não observância da LGPD. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente. (Cláusula completa) A Parte Receptora, para a execução do presente contrato, poderá acessar documentos, arquivos ou sistemas contendo Dados Pessoais, caso seja necessário. A Parte Receptora obriga-se a tratar os Dados Pessoais com segurança, dentro da necessidade, limite e adequação por si, seus administradores, sócios, prepostos, funcionários e terceiros. A Parte Receptora também se obriga a: a) estar em conformidade com a legislação específica sobre privacidade e proteção de dados vigente; b) adotar controles técnicos, administrativos, físicos e/ou digitais para proteger quaisquer Dados Pessoais a que possa ter acesso, visando a proteção contra a perda, danos, alteração, destruição, uso não autorizado, ilícito ou inadequado, acesso ou divulgação; c) tratar todo e qualquer Dado Pessoal em razão deste Contrato nos estritos termos do presente instrumento, sendo vedado qualquer tratamento de Dado Pessoal para outras finalidades que não as previstas nos termos do Contrato, aditivos ou orientações formais e por escrito da NOME DA EMPRESA; d) expor aos titulares ou outros controladores de Dados Pessoais as condições do tratamento dos dados, necessidade, finalidade e término do tratamento; e) manter registro das operações de tratamento de Dados Pessoais, incluindo-se eventuais compartilhamentos desses Dados a terceiros; f) adotar as medidas de exclusão, correção e/ou anonimização de Dados Pessoais transmitidos pela NOME DA EMPRESA, bem como replicar e exigir tais medidas de eventuais terceiros para os quais os Dados Pessoais forem compartilhados; g) obter prévia e expressa autorização da NOME DA EMPRESA para transmitir dados pessoais a quaisquer terceiros, mantendo-se em todas as hipóteses a responsabilidade da Parte Receptora, que se obriga a impor ao terceiro obrigações não menos rigorosas para proteção desses dados. h) permitir a auditoria por parte de autoridades governamentais competentes ou pela NOME DA EMPRESA, mediante aviso prévio, acerca do registro das operações de tratamento de Dados Pessoais, das práticas de privacidade, segurança e proteção de Dados Pessoais que sejam adotadas pela Parte Receptora; i) no prazo máximo de 24 (vinte e quatro) horas de eventual incidente ou suspeita dele, informar à NOME DA EMPRESA: (i) qualquer uso indevido, ilegal ou inadequado de Dados Pessoais; (ii) situações de acesso, uso ou aquisição de Dados Pessoais por pessoa não autorizada ou (iii) qualquer forma de comprometimento de Dados Pessoais ("Incidente"); j) cooperar totalmente com a NOME DA EMPRESA na investigação de eventual Incidente envolvendo Dados Pessoais. 1.2. Para os fins deste Contrato, "Dados Pessoais" significam as informações fornecidas ou coletadas em nome ou pela NOME DA EMPRESA e fornecidas à - ou acessadas pela - Parte Receptora em razão deste Contrato, que podem ser usadas para identificar ou tornar

identificável, localizar ou entrar em contato com uma pessoa natural como, por exemplo, mas não limitado a: (i) nome, idade ou sexo; (ii) endereço físico ou localização geográfica (e-mail); (iii) número de telefone; (iv) endereço de e-mail ou identificador on-line (IP); (v) dados cadastrais e números de segurança social ou identificador governamental similar (CPF, PIS/PASEP, etc.); (vi) atividade laboral exercida, informações financeiras ou da saúde; (vii) origem racial ou étnica, crenças religiosas ou filosóficas, associações a sindicatos, opiniões políticas, vida sexual, registro ou histórico criminal ou (vii) qualquer outra informação relacionada ou relacionável a uma pessoa física que seja combinada com qualquer um dos itens acima. 1.3. Ao término da relação entre as partes, deverá a Parte Receptora se abster de utilizar os dados pessoais que lhe tiverem sido transmitidos e/ou disponibilizados pela NOME DA EMPRESA durante a vigência do Contrato, bem como devolver ou excluir, mediante comprovação à NOME DA EMPRESA, as informações ou Dados Pessoais de funcionários, diretores, clientes ou outras pessoas da - ou fornecidos pela – NOME DA EMPRESA que estiverem em sua posse direta ou indireta. 1.4. Em caso de descumprimento de qualquer obrigação prevista nesta Cláusula, ficará a Parte Reveladora sujeito a reparação civil e criminal, além de eventuais perdas e danos havidos pela NOME DA EMPRESA. 1.5. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato, por qualquer motivo, pelo prazo da legislação pertinente.

• CONTRATO DE EVENTO: As partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 (“LGPD”), assumindo integral responsabilidade por toda operação de tratamento de dados pessoais, desde a coleta, tratamento, armazenamento e eliminação, assegurando que o tratamento dos dados pessoais seja realizado de acordo com as finalidades específicas e consentidas pelos titulares, nos termos da legislação vigente e da Lei nº 13.709/2018 (“LGPD”). As partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, observando sua privacidade e proteção, tratando os dados pessoais coletados para fins lícitos e expressamente previstos em lei, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • FORNECIMENTO: As Partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 (“LGPD”), assumindo cada qual, sem solidariedade, integral responsabilidade por suas respectivas operações de tratamento de dados pessoais, assegurando uma à outra que esse tratamento será realizado de acordo com a LGPD e com as finalidades expressamente consentidas pelos titulares. A Parte assegura que detém, e compartilhará com a NOME DA EMPRESA quando solicitado, a autorização do titular

para ceder e transmitir à NOME DA EMPRESA os dados pessoais pertinentes à execução do presente instrumento. As Partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • LOCAÇÃO: A LOCADORA e os seus FIADORES autorizam a NOME DA EMPRESA a coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais, para todas as finalidades relacionadas ao exercício de direitos e obrigações decorrentes do presente instrumento e em conformidade com a Lei Federal n. 13.709/2018 (LGPD), incluindo exemplificativamente a gestão de cobranças de alugueis, de despesas condominiais e encargos locatícios, de consumo de serviços públicos, de tributos, e de apólices de seguros. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • PATROCÍNIO: As Partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 ("LGPD"), assumindo cada qual, sem solidariedade, integral responsabilidade por suas respectivas operações de tratamento de dados pessoais, assegurando uma à outra que esse tratamento será realizado de acordo com a LGPD e com as finalidades expressamente consentidas pelos titulares. A Parte assegura que detém, e compartilhará com a NOME DA EMPRESA quando solicitado, a autorização do titular para ceder e transmitir à NOME DA EMPRESA os dados pessoais pertinentes à execução do presente instrumento. As Partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • PERMUTA: Para as finalidades do presente instrumento, conforme a Lei Federal nº 13.709/2018 (LGPD), PERMUTANTE e PRODUTOR RURAL, emitente da CPR, autorizam a NOME DA EMPRESA a coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais, bem como repassá-los a terceiros necessariamente envolvidos na cadeia do agronegócio para avaliação, auditoria, securitização, cumprimento e execução do presente contrato. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • PESQUISA:

As Partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 ("LGPD"), assumindo cada qual, sem solidariedade, integral responsabilidade por suas respectivas operações de tratamento de dados pessoais, assegurando uma à outra que esse tratamento

será realizado de acordo com a LGPD e com as finalidades expressamente consentidas pelos titulares. A Parte assegura que detém, e compartilhará com a NOME DA EMPRESA quando solicitado, a autorização do titular para ceder e transmitir à NOME DA EMPRESA os dados pessoais pertinentes à execução do presente instrumento. As Partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito.

As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente.

• PRESTAÇÃO DE SERVIÇOS:

As Partes obrigam-se a estar em conformidade com a legislação sobre privacidade e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 ("LGPD"), assumindo cada qual, sem solidariedade, integral responsabilidade por suas respectivas operações de tratamento de dados pessoais, assegurando uma à outra que esse tratamento será realizado de acordo com a LGPD e com as finalidades expressamente consentidas pelos titulares. A Parte assegura que detém, e compartilhará com a NOME DA EMPRESA quando solicitado, a autorização do titular para ceder e transmitir à NOME DA EMPRESA os dados pessoais pertinentes à execução do presente instrumento. As Partes obrigam-se, ainda, a não ceder ou compartilhar a qualquer título com terceiros os dados pessoais a que tiverem acesso, empregando as melhores práticas e medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de qualquer forma de tratamento inadequado ou ilícito.

As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente.

• REPRESENTAÇÃO COMERCIAL: Para as finalidades de representação e comercialização de insumos e produtos agrícolas, conforme a Lei Federal nº 13.709/2018 (LGPD), o REPRESENTANTE: a) autoriza a NOME DA EMPRESA a coletar, tratar, utilizar, armazenar, transmitir e eliminar seus dados pessoais e dos clientes com quem mantém relacionamento, bem como repassá-los a terceiros necessariamente envolvidos na cadeia do agronegócio para avaliação, auditoria, securitização, cumprimento e execução do presente contrato; b) assegura à NOME DA EMPRESA que detém meios suficientes e recursos necessários para tratar os dados pessoais, assegura à NOME DA EMPRESA que obteve do respectivo titular a autorização para tratar seus dados pessoais nos termos da alínea (a). As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente. • TRANSPORTE:

As Partes obrigam-se a estar em conformidade com a legislação sobre privacidade

e proteção de dados vigente, em particular a Lei Federal n. 13.709/2018 (“LGPD”), assumindo cada qual, sem solidariedade, integral responsabilidade por suas respectivas operações de tratamento de dados pessoais, assegurando uma à outra que esse tratamento será realizado de acordo com a LGPD e com as finalidades expressamente consentidas pelos titulares. As obrigações de proteção de dados pessoais sobreviverão à rescisão ou término do contrato por qualquer motivo, pelo prazo da legislação pertinente.

APÊNDICE B – TEMPLATE: PLANO DE CONTINUIDADE DO NEGÓCIO

1. OBJETIVO: O objetivo deste Plano de Continuidade é fornecer diretrizes para a rápida normalização dos serviços. Este tem como premissa a liberação de um ambiente contingencial onde os sistemas de NOMES DOS SISTEMAS. 2. APLICAÇÃO: Este procedimento se aplica a área de Tecnologia da Informação. 3. TERMOS E DEFINIÇÕES: • DRP: Disaster Recover Plan (Plano recuperação de desastre) • ERP: Enterprise Resource Planning (Planejamento de recurso corporativo) 4. DESCRIÇÃO DAS ATIVIDADES: 4.1. Avaliação dos Danos 4.1.1. No caso de ocorrer um incidente que venha a paralisar totalmente os sistemas, deverão ser adotados os seguintes passos: • Acionar Gestores de Departamento Tecnologia e Informação (NOME DOS GESTORES); • Acionar Equipe de Infraestrutura (NOME DO RESPONSÁVEL); • Acionar Equipe de Sistemas (NOME DO RESPONSÁVEL); • Acionar Comitê de Gestão de Crises (CASO APLICÁVEL); 4.1.2. No caso de ocorrer um incidente que venha a paralisar parcialmente os sistemas, deverão ser adotados os seguintes passos: • Acionar Gestores de Departamento Tecnologia e Informação (NOME DO RESPONSÁVEL); • Acionar Equipe de Infraestrutura (NOME DO RESPONSÁVEL); • Acionar Equipe de Sistemas (NOME DO RESPONSÁVEL); 4.1.3. Para uma correta avaliação do cenário é imprescindível a presença dos acima citados. 4.1.4. Na estrutura atual é inviável a recuperação de todos os sistemas de uma só vez. Com isto optou-se pela recuperação dos sistemas mais críticos para a Organização.

Ordem de prioridade	Servidor/Equipamento/ Info	Aplicação
1		
1		

4.2. Cronograma de Recuperação 4.2.1. Caso ocorram incidentes que venham a paralisar todos os sistemas Corporativos adotaremos a seguinte estratégia: 4.2.2. Toda a estrutura de contingência será montada no NOME DO DATACENTER, onde já se encontram alguns servidores e um storage instalados como backup. 4.2.3. Esta sala já tem estrutura para suportar os novos servidores e demais equipamentos necessários para a execução deste plano de Continuidade. 4.2.4. Os principais recursos como o sistema ERP (SAP ECC) estão sincronizados com o NOME DO DATACENTER, ou seja, temos uma cópia desses sistemas disponíveis para utilização no NOME DO DATACENTER. 4.2.5. O tempo médio das atividades são descritas abaixo:

4.2.6. Muitas das atividades listadas acima poderão ser feitas de forma simultânea.

Itens para instalação	Tempo de instalação, configuração e recuperação das informações
Preparação de Ambiente	3 horas (Contato com fornecedores, solicitação de equipamentos e demais necessidades)
Servidores	5 horas
Telefonia	2 horas
Internet	1 horas
Switchs 3750	1 hora
Active Directory	1 hora
SAP	3 horas
Instalação de 10 Notebooks	4 horas
Tempo Total em sequência: 21 horas Estimativa de tempo geral: 12 horas	

Em 12 horas, com toda a equipe de TI trabalhando, todos os serviços listados estarão operacionais. 4.3. Ativação do Plano 4.3.1. Este plano apenas será ativado em 2 ocasiões: 4.3.2. No caso de parada Parcial dos sistemas entrar em contato com um dos Gestores da Área de Tecnologia e Informação. 4.3.3. No caso de parada Total dos sistemas entrar em contato com os Gestores do Departamento de Tecnologia e Informação e estes deverão efetuar uma avaliação dos danos para apenas na sequência comunicar o fato ao Gestor do Comitê de Crises. 4.4. Notificação 4.4.1. Este plano deve ser de conhecimento de todos os representantes do Comitê de Gestão de Crises, bem como de toda a equipe de Segurança patrimonial da empresa. 4.4.2. Estes serão os responsáveis em contatar tanto os Gestores do Comitê de Crises bem como os Gestores do Departamento de Tecnologia e Informação. 4.5. Responsabilidades 4.5.1. Em caso de qualquer incidente no ambiente de Tecnologia e Informação a responsabilidade de recuperação dos sistemas fica a cargo de toda a equipe do Departamento de Tecnologia e Informação. 4.6. Revisão 4.6.1. Este Plano deve ser revisado obrigatoriamente a cada alteração, seja referente a Links, Fornecedores, Atualizações de Infraestrutura ou qualquer item que se faça necessário. 4.6.2. Caso isto não ocorra, ao menos uma vez por ano este deverá ser revisto e atualizado, se necessário. 4.7. Teste Obrigatório 4.7.1. A cada ano (Q1) deverá ocorrer um teste deste Plano, simulando uma situação de desastre. 4.7.2. Durante este teste deve ser elaborado um documento descrevendo quais foram os resultados obtidos. 4.8. Inventário de Mídias de Backup 4.8.1. O inventario das Mídias ficam no sistema de backup localizados no NOME DO DATACENTER. 4.9. Armazenamento das mídias • COFRE – NOME DO DATACENTER • MIDIAS DO POOL ANUAIS • MIDIAS DO POOL MENSAL • Storage – NOME DO DATACENTER • MIDIAS VIRTUAIS DO POOL DIARIO

4.10. Contatos

4.11. Procedimentos DETALHAR PROCEDIMENTOS Texto e telas explicando o passo a passo dos procedimentos que devem ser aplicados em cada sistema envolvido.....

Contato	Empresa	Telefone	Descrição

4.11.1. Active Directory 4.11.2. Rede de dados 4.11.3. Internet 4.11.4. Telefonia - Ligações de Saída: 4.11.5. Telefonia - Ligações de Entrada: 4.11.6. Servidor de Arquivos/Impressora 4.11.7. Estações de Trabalho 4.11.8. SAP ECC e DEMAIS SISTEMAS ENVOLVIDOS

APÊNDICE C – TEMPLATE: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5. OBJETIVO: O objetivo deste procedimento é definir e documentar os procedimentos e métodos de prevenção voltados a segurança da informação na Rede Corporativa, Computadores, Banco de Dados e Sistemas de Informação. 6. APLICAÇÃO: A fim de manter um nível adequado de segurança para a rede da empresa e Sistemas de Informação, continuamente são aplicados controles e rastreamento de eventos relacionados à segurança da informação. O Departamento de Tecnologia da Informação (TI), instalou ferramentas automatizadas que monitoram a rede corporativa, os computadores e o comportamento dos sistemas. Essas ferramentas são capazes de identificar e tomar ações automaticamente quando alguns eventos e comportamentos suspeitos são identificados. O não cumprimento desta política será reportado ao Comitê de TI, Diretor da Área Usuária, Diretor de RH, DPO e Departamento Jurídico, os quais, em conjunto, analisarão a gravidade da infração e aplicarão as medidas cabíveis (que pode variar entre advertência verbal, formal ou demissão por justa causa). 7. TERMOS E DEFINIÇÕES: • Primeiro Perímetro de Defesa: Separação total entre a Internet e a Rede corporativa através de um Firewall e o filtro da entrada de e-mail no servidor de correio (SMTP) com base na lista de extensões de arquivos bloqueados listados no Anexo A. • Segundo Perímetro de Defesa: Inclui várias ferramentas de monitoração, detecção e prevenção, tais como: Filtro de conteúdo de URLs que incluam sites com conteúdo proibido de acordo com os critérios definidos no Anexo B Software antivírus instalado em todos os computadores da empresa (desktops, notebook e servidores), incluindo servidor dedicado de antivírus para monitoração de e-mail, responsável por verificar a caixa de e-mail de todos os usuários e bloquear acesso a conteúdo proibidos, descrito no Anexo C Monitoração de serviços na Nuvem Monitoração de smartphones

• Firewall Pessoal: Um servidor para a distribuição de atualizações de softwares e patches de segurança para servidores e estações de trabalho. • Eventos de menor criticidade: incluem violação da política de segurança da informação de forma que não comprometa os recursos e sistemas corporativos, que não tragam prejuízos financeiros nem danos a reputação e a marca da NOME DA EMPRESA. • Eventos Críticos: incluem violação da política de segurança da informação de forma que comprometa os recursos e sistemas corporativos, que não tragam prejuízos financeiros nem danos a reputação e a marca da NOME DA EMPRESA.

• Centro SOC (Security Operating Center): Centro de monitoração responsável por gerenciar e controlar os eventos relacionados à segurança da informação. O Centro SOC monitora, coleta e analisa dados provenientes de Sistema Operacional e Sistemas re-

lacionados à Segurança da Informação. 8. RESPONSABILIDADE: Gerente de Segurança da Informação Global – Responsável pelos critérios de filtragem e definição da lista de arquivos proibidos; responsável pela definição dos padrões mínimos de segurança mandatórios para todas as subsidiárias; Responsável pela definição dos softwares de segurança mandatórios para todas as subsidiárias; Responsável pelo 'road map' (plano de atualização) dos softwares de segurança adotados como padrão global da NOME DA EMPRESA; Gerente da TI Local - Responsável pela implementação de processos e ferramentas automatizadas para monitorar; Responsável reportar eventos relacionados à segurança da informação documentados e informados pela equipe local; Responsável por comunicar as áreas de negócio em sua respectiva subsidiária, os eventos relacionados à segurança da informação que cheguem ao seu conhecimento e e tenham impactos diretos a rotina de trabalho e as operações da NOME DA EMPRESA; Responsável por reportar ao Comitê Executivo Local a ocorrência de eventos de segurança considerados críticos as operações.

Item / Papel	Gerente de Segurança Global	Gerente TI (local)	Equipe de Infraestrutura (local)	Áreas de Negócios
Padrões de softwares/ferramentas de segurança madatórios para todas as subsidiárias da Adama	A	C	R/C	I
Regars de Firewall madatórias para todas as subsidiárias da Adama	A	C	R/C	I
Lista de restrição de arquivos e sites	A	C	R/C	I
Realização de teste de penetração local (Penteste).	C/I	A	R/C	
Software padrão de antivirus e atualização do antivirus nos computadores.	A	C	R/C	
Regra do antivirus para varredura dos dados nos computadores.	A	C	R/C	
Lista de acessos dos usuários nos sistemas.	I	C	R/C	A
Plano de comunicação ao Comitê Executivo.	A/R	A/R	C	I
Atualização do Windows nos computadores.	A	C/I	R/C	
Campanhas de comunicação	A/R	A/R	C/R	I

R = Responsible | A = Accountable | C = Consult | I = Inform

9. GERAL 9.1. Eventos cibernéticos relacionados à segurança da informação causados por indivíduos externos incluem: • Tentativa de acesso à rede corporativa de pessoas não autorizadas usando Interfaces externas como internet, conexão de provedor de serviços, etc. • Implantação de 'malware' em computadores e/ou sistemas corporativos. • Interrupção de serviços corporativos através de "Denial of Service Attack". • Roubo de senha permitindo a invasores acesso a sistemas corporativos. • Danos a integridade e confiabilidade das informações armazenadas em banco de dados. • Uso de permissão elevada para atividade maliciosa • Roubo de informação de sistema corporativo ou de computadores pessoais (ex.: informações financeiras, pessoais, clientes, etc.). • Alteração em configurações de rede, ou encriptação de arquivos/dados, que restrinjam o acesso a recursos corporativo e/ou que desviem a comunicação de dados corporativos. • Uso de

Engenharia Social para realização de atividades maliciosas. 9.2. As violações de segurança da informação geradas pelos Colaboradores da empresa incluem: • O colaborador utilizar a senha de outro colaborador. • Uso não autorizado do computador de outro colaborador. • Utilizar privilégios elevados de usuário para acesso a arquivos e caixas de e-mail de outro usuário. • Compartilhamento de suas credenciais (usuário e senha) com outras pessoas; • Responder enquetes, pesquisas via telefone e/ou e-mails de fontes não comprovadas; • Conversar sobre assuntos de acesso restrito em ambientes públicos e/ou onde possa ser ouvido por pessoas não autorizadas a acessar tais assuntos; • Acesso não autorizado a arquivos restritos (ex.: acesso a chaves de registros). • Desligamento intencional do sistema de segurança da informação sem receber permissão do Gestor de Segurança da Informação.

10. PREPARAÇÃO PARA DETECÇÃO E PREVENÇÃO DE EVENTOS DE SEGURANÇA DA INFORAMÇÃO 10.1. Gerenciando o Primeiro Perímetro Defesa • O Gerente de TI deve garantir que as regras de Firewall sejam aplicadas seguindo as orientações do Time de Segurança Global alinhadas com as necessidades das áreas de negócio em sua respectiva localidade. A manutenção nas regras de Firewall é de responsabilidade do Coordenador de TI da subsidiária. • O Gerente Global de Segurança da Informação é o responsável pela definição da lista de arquivos bloqueados (listados no Anexo A e C). Sempre que essa lista for atualizada deverá ser enviada por e-mail para o Gerente da TI em cada subsidiária. • É recomendado pelo Gerente de Segurança Global, que a cada dois anos, uma empresa especializada em Segurança da Informação, seja contratada localmente para realizar um "Teste de Penetração" (Pentest) para validar os níveis de segurança no primeiro perímetro de defesa (ambiente externo e interno). Idealmente, tal teste deve ser realizado uma vez por ano. A contratação desse serviço incluindo alocação de verba é de responsabilidade do Gerente de TI Local. 10.2. Gerenciando o segundo Perímetro de Defesa • O Gerente de Segurança Global é responsável por definir a solução padrão de Antivírus assim como suas rotinas de atualização de varredura de dados para os servidores, desktops e notebooks. • O Gerente de TI é responsável por garantir que o software de antivírus esteja instalado e atualizado em todos os servidores e estações de trabalho de sua localidade. Uma vez por semana todos os computadores serão varridos (scan disk) em busca de máquinas com antivírus desatualizado ou inativo. • O Gerente de TI é responsável por conceder a cada usuário final somente as permissões necessárias para executar suas tarefas diárias, garantindo que esses usuários não tenham permissões elevadas nas estações de trabalho e demais serviços fornecidos pela TI. O Gestor da Área responsável pelas informações disponíveis em sistema(s), é o responsável por passara para a TI a lista de acessos que cada usuário deverá receber para que realize suas atividades diárias no(s) respectivo(s) sistema(s). • Gerente de Segurança Global é responsável por garantir que, quando um vírus for detectado a ferramenta de antivírus, enviará um alerta para o Gerente de TI e demais Administradores da Rede Em adicional, a Equipe de Se-

gurança Global também deverá reportar qualquer suspeita de vírus para a Equipe de TI local. • Durante o final de semana o antivírus executará uma varredura automática em busca de vírus em todos os servidores e estações de trabalho (desktops e notebooks), caso alguma estação de trabalho esteja desligada, essa varredura será feita imediatamente após o equipamento ser ligado. O Gerente de Segurança Global é responsável por garantir que as rotinas de varreduras nos computadores estejam devidamente aplicadas na console de gerenciamento central do software de antivírus. • Uma vez por dia o antivírus que roda nos servidores e estações de trabalho (desktops e notebooks) é atualizado. O Gerente de Segurança Global é responsável por garantir que as últimas atualizações do antivírus estejam disponíveis no repositório central, e o Gerente de TI Local é responsável por garantir que os computadores recebam a atualização do antivírus disponível no repositório central. • É mandatório que os servidores e estações de trabalho recebam as atualizações do Windows classificadas como críticas (critical Windows update and security issue). O Gerente de TI Local é responsável por garantir que os computadores em sua respectiva subsidiária estejam com as atualizações mandatórias do Windows. • Os notebooks deverão ter instalado um serviço de Firewall. O Gerente de TI Local é responsável por garantir que os computadores em sua respectiva subsidiária estejam com o serviço de FW instalado. • O Gerente de TI em conjunto com o Gerente Global de Segurança da Informação são responsáveis por realizarem periodicamente campanhas alertando os usuários sobre os riscos relacionados à segurança da informação e os métodos de mitigação de riscos adotados pela NOME DA EMPRESA. • O Gerente Global de Segurança da Informação integrará ferramentas globais de monitoração que irão automaticamente verificar as estações de trabalho e alertar ao Gerente de TI quando possíveis ameaças foram identificadas.

10.3. DETECÇÃO DE ATAQUE CIBERNÉTICO E EVENTOS DE SEGURANÇA DA INFORMAÇÃO Ataques cibernéticos e eventos relacionados à segurança da informação são detectados da seguinte forma: • Alerta gerado pelo centro SOC (Anexo D). • Alerta gerado pelos sistemas de monitoração (Anexo D). • Relatórios de produção (centro de suporte, usuários, etc.). 10.3.1. Relatório de Eventos Suspeitos referente a Segurança da Informação • Em todos os casos de suspeita de evento relacionado a Segurança da Informação, os detalhes referentes ao evento deverão ser levados ao conhecimento do Gerente de TI. • Dependendo do tipo do evento e de sua análise inicial, o evento deverá ser reportado para o Diretor de TI, CEO, DPO, CFO ou outra pessoa do Time Executivo. 10.3.2. Análise de Evento relacionado a Segurança da Informação • O Gerente de TI alocará equipe local para a primeira investigação do evento para identificar sua origem e nível de contaminação. • Caso necessário, o Gerente de TI deverá consultar o Gerente Global de Segurança da Informação ou uma Empresa Externa Especializada em Segurança da Informação, para que o evento seja analisado e uma solução seja definida e aplicada. 10.3.3. Contenção de eventos relacionados à Segurança da Informação • Com base na primeira investigação do evento, o Gerente de TI irá definir as ações necessárias para controlar o

evento. • As ações de contenção podem variar de acordo com cada evento, mas sempre deverá incluir um dos seguintes itens: Desligar o computador ou desconectá-lo da rede Desabilitar o usuário da rede Desativar o serviço de VPN Desconectar a NOME DA EMPRESA da Internet Uso de inteligência cibernética Aplicar bloqueio de portas no Firewall • Caso um evento de segurança desconhecido seja identificado na rede, deverá ser tratado como uma possível ameaça que poderá se propagar rapidamente para as estações de trabalho e servidores, nesse caso um plano de ação rápido e eficiente deverá ser definido e aplicado pelo Gerente de TI. • Quando um evento de segurança da informação é causado por uma conduta indevida de um Colaborador, o Gerente de IT deverá analisar detalhadamente o evento e definir como lidar com isso, levando em consideração a reincidência de uma conduta indevida desse mesmo Colaborador. Nesse caso o Departamento de Recursos Humanos e Jurídico (além do DPO, se envolver dados pessoais) deverão ser consultados para se aplicar as medidas cabíveis a esse Colaborador. • Quando, como resultado de um evento de Segurança da Informação, ações legais sejam aplicadas contra um indivíduo ou Organização, a evidência deve ser coletada, preservada e apresentada de acordo com a orientação do Departamento Jurídico. 10.3.4. Remediação e Recuperação de Evento de Segurança da Informação • O Gerente de TI, com base nas investigações, deverá definir e recomendar a aplicação das ações necessárias de acordo com cada caso. As ações de remediação deverão ser baseadas nos seguintes critérios, conforme anexo X utilizado pela equipe de investigação para reportar a conclusão final sobre o evento: Nível de severidade do incidente Severidade do dano (conhecido) causado Causa do incidente Aplicação de uma ação imediata Resposta adequada para ações a longo prazo (corretiva e preventiva). O Sistema contém informações sensíveis aos negócios? Existe exposição, alteração, interrupção ou remoção de informação confidencial? Há dados pessoais envolvidos? • As ações de remediação deverão ser aplicadas de acordo com cada evento, e deverão incluir no mínimo uma das seguintes ações: Varredura da área infectada e remoção do vírus, malware, etc... Remoção do hardware infectado Formatação da estação de trabalho infectada, podendo esse ser realizada sem backup prévio Recuperação de arquivos de backup 10.3.5. Métodos para Reportar Eventos de Segurança da Informação • Evento de baixa severidade: Nestes casos, os eventos serão tratados localmente onde foram gerados, de forma pontual e localizada. O Gerente de TI local deverá ser informado. • Evento de média/alta severidade: Assim que recebido o reporte, o Gerente de TI deverá comunicar de forma imediata o Gerente Global de Segurança da Informação a existência de um novo evento (ver contatos no Anexo 1 desse documento). Além disso, e para receber instruções para ações adicionais, O Gerente de TI deverá informar e consultar o Diretor de TI, CFO, DPO ou CEO local sobre os passos necessários a serem aplicados (ex.: comunicado para o Departamento Financeiro Global, Relações Públicas da empresa, ou outros Órgãos relevantes). Eventos graves que afetem relatórios de finanças, deverão ter um plano específico de reporte e documentação referente ao evento ocorrido.

10.3.6. Documentação, Acompanhamento e Esclarecimento referente a Evento de Segurança de Informação • A equipe de investigação deverá documentar e resumir o evento de segurança da informação conforme template do ANEXO x, provendo detalhes sobre o ocorrido e o Gerente de TI complementará com as conclusões, recomendações e decisões. • Em caso de eventos graves, o Gerente de TI deverá informar o Gerente Global de Segurança da Informação, o Diretor de TI, CFO, CEO, e se necessário o Líder Direto do Colaborador (quando esse tenha causado o evento), além do DPO se o evento envolver dados pessoais. • O Gerente de TI deverá consolidar todos os eventos relacionados à segurança da informação em um documento central conforme template do ANEXO x, que deverá conter os detalhes dos eventos, as decisões tomadas em relação aos eventos e o status atualizado de cada ação recomendada. 11. SENHA • O acesso aos sistemas da NOME DA EMPRESA, será concedido mediante a autenticação do usuário, que é feito através de usuário e senha (e preferencialmente com um segundo fator de autenticação – autenticação em duas etapas). • A senha é de uso individual e de total responsabilidade do Colaborador É fundamental que não seja divulgada e nem exposta de forma que outros possam ter acesso a ela. • É expressamente proibido o compartilhamento dessa senha para qualquer finalidade. • A senha deverá ser composta por, no mínimo, 6 caracteres e deverá conter letra maiúscula, letra minúscula, número e caractere especial (ex.: P@ssw0rd). • A troca da senha deverá acontecer no máximo a cada 90 dias, exceto para os usuários classificados como Conta de Serviço*, que deverão ser configurados para que a senha não expire. * = A Conta de Serviço é o usuário utilizado para a execução de serviços de TI, esse usuário deve ser utilizado apenas para a execução do serviço de TI, o login com esse usuário deverá acontecer apenas para fins gerenciais nos serviços envolvidos e deverá estar devidamente formalizado e aprovado pelo Gestor de TI através de um chamado. A senha desse tipo de usuário deve ser de conhecimento apenas do Analista de TI responsável pelo serviço em questão e deve ser configurada para nunca expirar a fim de evitar a ruptura do serviço por conta de falha na autenticação. • Após 6 (seis) tentativas de logon com senha inválida a conta do usuário deverá ser bloqueada.

12. AUTENTICAÇÃO EM DUAS ETAPAS • Para que o usuário possa realizar o acesso de serviços da NOME DA EMPRESA hospedados na Nuvem, como o Office365, Intranet, SuccessFactors entre outros, é obrigatório a autenticação em duas etapas. Esse processo consiste na combinação da autenticação do usuário no Active Directory, com uma aprovação da conexão através de um segundo dispositivo cadastrado pelo usuário no serviço de autenticação global da NOME DA EMPRESA. Para que o usuário tenha acesso ao serviço desejado, é obrigatório que esses dois processos de autenticação sejam realizados com sucesso, do contrário o usuário não terá o acesso autorizado.

• Esse mesmo processo de autenticação em duas etapas, também é mandatório para estabelecer a conexão VPN.

Obs.: O procedimento de como cadastrar o segundo fator de autenticação está disponível no Sharepoint da TI na Intranet. 13. POLÍTICA DE PRIVACIDADE • Aspectos relacionados a Proteção de Dados Pessoais e Privacidade são tratados pela NOME DA EMPRESA através de sua política de privacidade, disponível para todo o público através da página da NOME DA EMPRESA na Internet: https://www.sitedaempresa. LISTA DOS ARQUIVOS BLOQUEADOS

asf	mod	pl	bat
divx	mp2	scr	com
emf	mp3	sh	csc
mpe	mpeg	shs	csh
wmf	snd	vbs	dll
wpf	stm	wsf	exe
wsf	voc	avi	js
mpg	wav	mid	perl
mpe			pif

LISTA DOS SITES BLOQUEADOS Abortion, Alcohol, "Audio/Video Clips", "Chat/Instant Messaging", Gambling, Games, Hacking, "Illegal Drugs", Illegal/Questionable, Newsgroups/Forums, Nudity, "Open/Mixed Content", "Pay to Surf", "Peer-to-Peer (P2P)", Phishing, Pornography, "Proxy Avoidance", "Remote Access Tools", "Sex Education", "Social Networking", "Software Downloads", "Spyware Effects/Privacy Concerns", "Spyware/Malware Sources", Suspicious, Violence/Hate/Racism, Weapons.

LISTA DE ARQUIVOS BLOQUEADOS NO SERVIDOR DE E-MAIL

*.VSW	*.PRF	*.MDW	*.HLP	*.AD?
*.WS?	*.REG	*.MDZ	*.HTA	*.APP
*.mp?	*.SCF	*.MSC	*.INF	*.ASP
*.avi	*.SCR	*.MSI	*.INS	*.ASX
*.dll	*.SCT	*.MSP	*.ISP	*.BAS
*.mpeg	*.SH?	*.MST	*.JS?	*.BAT
*.mpg	*.VB	*.MDB	*.KSH	*.CHM
*.mp3	*.OPS	*.MDE	*.LNK	*.CMD
*.VSD	*.PCD	*.MDT	*.MDA	*.COM
*.VSS	*.PIF	*.CSH	*.EXE	*.CPL
*.VST	?		*.FXP	*.CRT

APÊNDICE D – TEMPLATE: TERMO DE CONSENTIMENTO DO TITULAR

1. OBJETIVO Este termo é um modelo para utilização pela [Inserir nome da Empresa] interessadas, nos casos em que seja necessária a obtenção de consentimento do Titular para coleta e tratamento de dados pessoais, devendo e podendo ser adaptado a depender do caso concreto. TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a legislação vigente.

TITULAR

Nome:

RG:

CPF:

A presente autorização é concedida a título gratuito e, ao assinar o presente Termo, o TITULAR consente e concorda que a [Inserir o nome da Empresa]., inscrita no CNPJ sob n. [Inserir o CNPJ da Empresa], com sede na [Inserir o Endereço da Empresa], realize as seguintes operações de tratamento com seus dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Identificação dos dados pessoais: O TITULAR autoriza a [Inserir nome da Empresa]. a coletar e tratar seus dados pessoais a seguir listados: [inserir os dados pessoais necessários no caso concreto] Finalidade do tratamento: O tratamento dos dados pessoais identificados neste termo tem a seguinte finalidade determinada, legítima, específica e explícita: [inserir a finalidade de tratamento no caso concreto] Compartilhamento dos dados pessoais: O TITULAR autoriza a [Inserir nome da Empresa] a compartilhar seus dados pessoais identificados neste termo com outros agentes de tratamento para as mesmas finalidades aqui listadas, de acordo com a legislação de proteção de dados, e observados os princípios e fundamentos listados na legislação vigente. Medidas de segurança e proteção dos dados pessoais: A [Inserir nome da Empresa]. adotará medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais do TITULAR de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e, na ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao TITULAR, comunicará ao TITULAR

e à Autoridade Nacional de Proteção de Dados (ANPD). Término do tratamento dos dados pessoais: [A depender da finalidade listada e dos dados pessoais coletados, o prazo de retenção dos dados variará. Ajustar no caso concreto]. Os dados pessoais anonimizados – ou seja, sem possibilidade de associação ao Titular – poderão ser mantidos pela [Inserir nome da Empresa]. por tempo indeterminado. Direitos do TITULAR: O TITULAR dos dados pessoais tem direito a obter da [Inserir nome da Empresa], em relação aos seus dados pessoais, a qualquer momento e mediante requisição: a confirmação da existência de tratamento; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; a 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; a eliminação dos dados pessoais aqui listados; a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; a revogação do consentimento. Direito de revogação do consentimento: Este consentimento poderá ser revogado pelo TITULAR, a qualquer momento, mediante solicitação formal e expressa à [Inserir nome da Empresa]. [Havendo Encarregado de Proteção de Dados (DPO) nomeado e endereço de e-mail estabelecido, é interessante direcionar as solicitações do titular a esse profissional, de acordo com o art. 41, da LGPD].

Local e data:

Assinatura do Titular:

APÊNDICE E – TEMPLATE: TERMO DE CONSENTIMENTO PARA COOKIES

A nome da empresa utiliza cookies e outras tecnologias em seu site para melhorar a sua experiência e para compreender melhor a forma como você utiliza o nosso servidor. Os dados capturados são processados para as seguintes finalidades: análise e melhoria da experiência de navegação do usuário, viabilização da nossa oferta de produtos e serviços, medição e análise de audiência, interação com redes sociais, exibição de anúncios e conteúdo personalizados, medição do desempenho e atratividade de anúncios e conteúdo. A nome da empresa pode compartilhar suas informações com terceiros prestadores de serviços necessários para viabilizar ou apoiar as finalidades acima descritas. Os terceiros prestadores de serviços da nome da empresa não estão autorizados a divulgar quaisquer informações suas, exceto cumprir exigências legais. Você poderá a qualquer momento revogar sua autorização para coleta e processamento de seus dados por meio de envio de e-mail para: email ou outros canais de contato. Visite nossa Política de Privacidade para saber mais sobre como a nome da empresa utiliza cookies e, se preferir, como os desativar. Ao clicar em "Aceito" e ao continuar a utilizar este website, você concorda com a nossa Política de Privacidade e com utilização de cookies pela nome da empresa.

APÊNDICE F – TEMPLATE: AVISO DE PRIVACIDADE PARA COLABORADORES

1. SOBRE A EMPRESA (inserir nome da empresa) coletamos e processamos suas informações pessoais de acordo com este aviso de privacidade e em conformidade com os regulamentos e leis de proteção de dados relevantes. Este aviso fornece as informações necessárias sobre seus direitos e nossas obrigações, e explica como, por que e quando processamos seus dados pessoais. A sede da [inserir nome da organização] é em [inserir endereço da organização] e somos uma empresa registrada no Brasil com o CNPJ [inserir número do CNPJ]. Estamos legalmente autorizados a atuar como [controlador de dados / processador de dados] ao processar seus dados. Nosso responsável pela proteção de dados / pessoa designada é [inserir nome do Encarregado LGPD / DPO], que pode ser contatado em [inserir endereço relevante e detalhes de contato do DPO]. 2. INFORMAÇÕES COLETADAS [Inserir nome da organização] processa suas informações pessoais para cumprir nossas obrigações legais, estatutárias e contratuais e para nos permitir recrutar, empregar e capacitar para trabalhar conosco. Nunca coletaremos quaisquer dados pessoais desnecessários seus e não processaremos suas informações de nenhuma forma, exceto conforme especificado neste aviso. Os dados pessoais que coletamos são: • Nome • Data de nascimento • Endereço residencial • Email pessoal • Número de telefone residencial • Número de telefone celular • Número da Carteira de Trabalho e Previdência Social (CTPS) • Formação acadêmica • Detalhes bancários • Dados de categoria especial (ou seja, informações médicas / de saúde, etnia racial, deficiências, etc.) • [adicionar quaisquer outros tipos]

3. COLETAMOS INFORMAÇÕES DAS SEGUINTES FORMAS A [Inserir nome da organização] coleta dados pessoais através de um ou mais dos seguintes canais: • Cadastro em plataforma digital para processo seletivo • Cadastro no site da empresa • Currículos enviados • Fóruns de empregos e agências de recrutamento • Direto de candidatos e funcionários • Solicitações de vagas eletrônicas • Aplicativos postais e de e-mail • [adicionar quaisquer outros métodos]

4. COMO USAMOS SEUS DADOS PESSOAIS A [Inserir nome da organização] leva sua privacidade muito a sério e nunca divulgará, compartilhará ou venderá seus dados sem o seu consentimento; a menos que seja exigido por lei. Retemos seus dados apenas pelo tempo necessário e para os fins especificados neste aviso. Os objetivos e razões para o processamento dos seus dados pessoais são detalhados a seguir: • Processamos seus dados pessoais na execução de um contrato como seu empregador, para garantir que cumpramos nossas obrigações legais de empregador e os requisitos da legislação trabalhista; • Processamos seus dados pessoais como parte de nossa obrigação legal para fins de contabilidade

comercial, folha de pagamento e impostos; • Processamos dados de categorias especiais sobre você como parte de nossas obrigações de emprego, para garantir que quaisquer deficiências, condições de saúde e requisitos religiosos sejam conhecidos; • Processamos seus dados pessoais sob interesses legítimos para realizar nossas verificações de referência de crédito como parte de nossas medidas de devida diligência; • [adicionar qualquer outra base e motivos]

5. SEUS DIREITOS Você tem o direito de acessar qualquer informação pessoal que a [inserir nome da organização] processe sobre você e de solicitar informações sobre: • Quais dados pessoais mantemos sobre você; • Os objetivos do processamento; • As categorias de dados pessoais em questão; • Os destinatários a quem os dados pessoais foram / serão divulgados; • Por quanto tempo pretendemos armazenar seus dados pessoais; • Se não coletamos os dados diretamente de você, informações sobre a fonte;

Se você acredita que mantemos quaisquer dados incompletos ou imprecisos sobre você, você tem o direito de nos pedir para corrigir e / ou completar as informações e nós nos esforçaremos para fazer isso o mais rápido possível, a menos que haja um motivo válido para não fazê-lo, nesse ponto você será notificado.

Você também tem o direito de solicitar o apagamento de seus dados pessoais ou de restringir o processamento (quando aplicável) de acordo com Lei Geral de Proteção de Dados (LGPD), bem como se opor a qualquer marketing direto de nossa parte. Quando aplicável, você tem o direito de portabilidade de dados de suas informações e o direito de ser informado sobre qualquer tomada de decisão automatizada que possamos usar.

Se recebermos uma solicitação sua para exercer qualquer um dos direitos acima, podemos solicitar que você verifique sua identidade antes de atender à solicitação, isso é para garantir que seus dados sejam protegidos e mantidos seguros.

6. COMPARTILHAMENTO E DIVULGAÇÃO DE DADOS PESSOAIS Não compartilhamos ou divulgamos nenhuma de suas informações pessoais sem o seu consentimento, exceto para os fins especificados neste aviso ou quando houver uma exigência legal.

[Inserir Nome da Organização] usa [inserir nome de Terceiros] para fornecer os serviços e funções comerciais abaixo, no entanto, todos os processadores agindo em nosso nome apenas processam seus dados de acordo com nossas instruções e cumprem integralmente este aviso de privacidade, as leis de proteção de dados e quaisquer outras medidas de confidencialidade e segurança apropriadas.

[Insira o nome da organização] [Insira os motivos para usar a empresa, o que ela processa, como o processa e forneça um link para seu aviso de privacidade]

[Documente quaisquer terceiros para os quais você envia dados de funcionários, como contadores externos para folha de pagamento, etc. ou, se você não usar nenhum

processador externo, deixe apenas o primeiro parágrafo sob este título.]

7. MEDIDAS DE PROTEÇÃO [Insira o nome da organização] leva a sua privacidade a sério e toma todas as medidas e precauções razoáveis para proteger e proteger seus dados pessoais. Trabalhamos muito para proteger você e suas informações de acesso não autorizado, alteração, divulgação ou destruição e temos várias camadas de medidas de segurança em vigor, incluindo:

[inserir medidas como SSL, TLS, criptografias, pseudonimização, acesso restrito, autenticação de TI, firewalls, antivírus / malware etc.]

8. TRANSFERÊNCIA PARA FORA DO BRASIL Os dados pessoais no Brasil são protegidos Lei Geral de Proteção de Dados (LGPD), mas alguns outros países podem não ter necessariamente o mesmo alto padrão de proteção para seus dados pessoais. [Inserir nome da organização] não transfere nem armazena dados pessoais fora do Brasil. OU; [Inserir nome da organização] transfere dados pessoais para fora o Brasil para os fins abaixo: - • [Insira o motivo da transferência para fora da UE e para quem] • [Insira o motivo da transferência para fora da UE e para quem] • [Insira o motivo da transferência para fora da UE e para quem]

Quando transferimos informações pessoais pelos motivos acima, utilizamos as medidas e mecanismos de proteção abaixo para garantir que seus dados pessoais estejam sempre protegidos: • [Insira as medidas de proteção tomadas] • [Insira as medidas de proteção tomadas] • [Insira as medidas de proteção tomadas]

9. CONSEQUÊNCIAS DE NÃO FORNECER SEUS DADOS Você não é obrigado a fornecer suas informações pessoais para [inserir nome da organização], no entanto, como essas informações são necessárias para que possamos contratá-lo, não poderemos oferecer emprego sem certas informações pessoais. 10. TEMPO DE RETENÇÃO DOS DADOS PESSOAIS A [inserir nome da organização] apenas retém informações pessoais pelo tempo necessário e temos políticas rígidas de revisão e retenção para cumprir essas obrigações. De acordo com a legislação tributária do Brasil, somos obrigados a manter seus dados pessoais básicos (nome, endereço, detalhes de contato) por um período mínimo de 5 anos, após o qual serão destruídos. 11. CATEGORIAS DE DADOS ESPECIAIS Como seu empregador, temos um interesse legítimo e, em alguns casos, uma obrigação legal de processar certos dados de categorias especiais sobre você. Isso pode incluir, mas não está limitado a informações sobre quaisquer deficiências, condições de saúde e requisitos religiosos. Quando coletamos essas informações, o fazemos de acordo com o Artigo 11 da Lei Geral de Proteção de Dados (LGPD). Solicitaremos e processaremos apenas o mínimo necessário para o propósito especificado e garantiremos que as medidas de proteção e segurança necessárias sejam colocadas em todos os dados de categoria especial. 12. APRESENTAÇÃO DE RECLAMAÇÕES [Inserir nome da organização] apenas processa suas informações pessoais em conformidade com este aviso de privacidade e de acordo

com as leis de proteção de dados relevantes. Se, no entanto, desejar apresentar uma reclamação em relação ao processamento dos seus dados pessoais ou não estiver satisfeito com a forma como tratámos as suas informações, tem o direito de apresentar uma reclamação à Agência Nacional de Proteção de Dados (ANPD). [Insira o nome da organização] [Insira o nome do responsável pela proteção de dados] [Insira o endereço da organização] [Inserir telefone e e-mail da organização] [Inserir ANPD] [Insira o endereço da ANPD] [Insira o telefone e e-mail da ANPD]

APÊNDICE G – TEMPLATE: POLÍTICA DE PRIVACIDADE

Importante: Guia de Uso para esse Template Este é um modelo geral para um Aviso de Privacidade em conformidade com o LGPD, que pode ser personalizado para atender às suas necessidades de negócios e oferece orientações genéricas de uso. É importante compreender suas responsabilidades de notificação e personalizar este modelo para garantir que seja relevante e compatível. Aviso de privacidade x Política de privacidade - os dois termos são usados alternadamente e não há diferença definida universalmente, no entanto, algumas definições sugerem que um Aviso de Privacidade é o conteúdo apresentado no momento da obtenção dos dados pessoais (pop-up, na tela, formulário em papel etc.); Já a Política de Privacidade é um comunicado constante, página do site, link que está sempre disponível para leitura do visitante / indivíduo - ambos com o mesmo conteúdo. LEMBRE-SE: Você é obrigado a fornecer um aviso de privacidade a TODOS os indivíduos ao processar seus dados pessoais, mas o contexto / conteúdo do aviso irá variar dependendo da base legal sob a qual você está processando os dados. Consentimento: Se estiver usando o consentimento como base legal para o processamento, você deve comprovar que o consentimento foi obtido por meio de uma ação afirmativa (ex.: assinatura, aceite em sistema passível de rastreamento, outros similares). Você também pode usar seu próprio formulário de consentimento para cada titular dos dados, com uma caixa de opção desmarcada ou mecanismo de ação afirmativa para cada atividade de processamento. Se seus serviços forem prestados a crianças e/ou adolecentes, você deve usar uma linguagem amigável em sua notificação, incluir quaisquer riscos de fornecer dados e, se depender do consentimento, verificar a idade e obter o consentimento dos pais quando aplicável. Legítimo Interesse (Marketing) Ao enviar materiais de marketing aos clientes, você tem a opção de usar consentimento ou interesses legítimos, portanto, adicionamos exemplos para cada um (que você pode remover se não enviar marketing). Você só pode usar interesses legítimos para marketing se avaliou que as informações enviadas são relativas e benéficas para o cliente, que pesou os interesses deles em relação aos seus, há pouco ou nenhum risco, o método e o conteúdo não são intrusivo, e o material enviado é algo que um cliente normalmente espera receber e você oferece a opção de cancelar. Aviso de isenção de responsabilidade: este documento tem o objetivo de ser um modelo de aviso de privacidade e não é um documento jurídico ou um substituto para aconselhamento jurídico. É sua responsabilidade garantir o cumprimento de todos os requisitos legais, estatutários e regulamentares que se aplicam à sua organização. 13. SOBRE A EMPRESA (inserir nome da empresa) coletamos e processamos suas informações pessoais de acordo com este aviso de privacidade e em conformidade com os regulamentos e leis de proteção

de dados relevantes. Este aviso fornece as informações necessárias sobre seus direitos e nossas obrigações, e explica como, por que e quando processamos seus dados pessoais. A sede da [inserir nome da organização] é em [inserir endereço da organização] e somos uma empresa registrada no Brasil com o CNPJ [inserir número do CNPJ]. Estamos legalmente autorizados a atuar como [controlador de dados / processador de dados] ao processar seus dados. Nosso responsável pela proteção de dados / pessoa designada é [inserir nome do Encarregado LGPD / DPO], que pode ser contatado em [inserir endereço relevante e detalhes de contato do DPO]. 14. INFORMAÇÕES COLETADAS [Inserir nome da organização] processa suas informações pessoais para cumprir nossas obrigações legais, estatutárias e contratuais e para fornecer nossos produtos e serviços. Nunca coletaremos quaisquer dados pessoais desnecessários e não processaremos suas informações de nenhuma forma, exceto conforme especificado neste aviso. Os dados pessoais que coletamos são: • Nome • Data de nascimento • Endereço residencial • Email pessoal • Número de telefone residencial • Número de telefone celular • Número da Carteira de Trabalho e Previdência Social (CTPS) • Formação acadêmica • Detalhes bancários • Dados de categoria especial (ou seja, informações médicas / de saúde, etnia racial, deficiências, etc.) • [adicionar quaisquer outros tipos] 15. COLETAMOS INFORMAÇÕES DAS SEGUINTES FORMAS A [Inserir nome da organização] coleta dados pessoais através de um ou mais dos seguintes canais: • Cadastro no site da empresa • Preenchimento de formulários em eventos • Eventos promocionais • Fóruns de empregos e agências de recrutamento • Direto de candidatos e funcionários • Solicitações de vagas eletrônicas • Aplicativos postais e de e-mail • [adicionar quaisquer outros métodos]

16. COMO USAMOS SEUS DADOS PESSOAIS A [Inserir nome da organização] leva sua privacidade muito a sério e nunca divulgará, compartilhará ou venderá seus dados sem o seu consentimento; a menos que seja exigido por lei. Retemos seus dados apenas pelo tempo necessário e para os fins especificados neste aviso. Os objetivos e razões para o processamento dos seus dados pessoais são detalhados a seguir: [inserir propósito e / ou motivo como pontos] Exemplo: coletamos seus dados pessoais na execução de um contrato ou para fornecer um serviço e para garantir que os pedidos sejam concluídos e possam ser enviados para o endereço de sua preferência; Exemplo: coletamos e armazenamos seus dados pessoais como parte de nossa obrigação legal para fins contábeis e fiscais; Exemplo: temos a obrigação legal de compartilhar seus dados pessoais com [inserir nome da empresa] que é uma agência de referência de crédito e nos fornece verificações de histórico financeiro antes de você começar a trabalhar conosco; Exemplo: Ocasionalmente, enviaremos a você informações de marketing quando tivermos avaliado que sejam benéficas para você como cliente e em nossos interesses. Essas informações não são intrusivas e são processadas com base em interesses legítimos; 17. SEUS DIREITOS Você tem o direito de acessar qualquer informação pessoal que a [inserir nome da organização] processe sobre você e de solicitar informações sobre: • Quais dados pessoais mantemos sobre você; • Os objetivos do

processamento; • As categorias de dados pessoais em questão; • Os destinatários a quem os dados pessoais foram / serão divulgados; • Por quanto tempo pretendemos armazenar seus dados pessoais; • Se não coletamos os dados diretamente de você, informações sobre a fonte;

Se você acredita que mantemos quaisquer dados incompletos ou imprecisos sobre você, você tem o direito de nos pedir para corrigir e / ou completar as informações e nós nos esforçaremos para fazer isso o mais rápido possível, a menos que haja um motivo válido para não fazê-lo, nesse ponto você será notificado.

Você também tem o direito de solicitar o apagamento de seus dados pessoais ou de restringir o processamento (quando aplicável) de acordo com Lei Geral de Proteção de Dados (LGPD), bem como se opor a qualquer marketing direto de nossa parte. Quando aplicável, você tem o direito de portabilidade de dados de suas informações e o direito de ser informado sobre qualquer tomada de decisão automatizada que possamos usar.

Se recebermos uma solicitação sua para exercer qualquer um dos direitos acima, podemos solicitar que você verifique sua identidade antes de atender à solicitação, isso é para garantir que seus dados sejam protegidos e mantidos seguros.

18. COMPARTILHAMENTO E DIVULGAÇÃO DE DADOS PESSOAIS Não compartilhamos ou divulgamos nenhuma de suas informações pessoais sem o seu consentimento, exceto para os fins especificados neste aviso ou quando houver uma exigência legal.

[Inserir Nome da Organização] usa [inserir nome de Terceiros] para fornecer os serviços e funções comerciais abaixo, no entanto, todos os processadores agindo em nosso nome apenas processam seus dados de acordo com nossas instruções e cumprem integralmente este aviso de privacidade, as leis de proteção de dados e quaisquer outras medidas de confidencialidade e segurança apropriadas.

[Insira o nome da organização] [Insira os motivos para usar a empresa, o que ela processa, como o processa e forneça um link para seu aviso de privacidade]

[Insira os motivos para usar a empresa, o que ela processa, como o processa e forneça um link para seu aviso de privacidade]

19. MEDIDAS DE PROTEÇÃO [Insira o nome da organização] leva a sua privacidade a sério e toma todas as medidas e precauções razoáveis para proteger e proteger seus dados pessoais. Trabalhamos muito para proteger você e suas informações de acesso não autorizado, alteração, divulgação ou destruição e temos várias camadas de medidas de segurança em vigor, incluindo:

[inserir medidas como SSL, TLS, criptografias, pseudonimização, acesso restrito, autenticação de TI, firewalls, antivírus / malware etc.]

20. TRANSFERÊNCIA PARA FORA DO BRASIL Os dados pessoais no Brasil são protegidos Lei Geral de Proteção de Dados (LGPD), mas alguns outros países podem não ter necessariamente o mesmo alto padrão de proteção para seus dados pessoais. [Inserir nome da organização] não transfere nem armazena dados pessoais fora do Brasil. OU; [Inserir Nome da Organização] utiliza alguns produtos ou serviços (ou partes deles) que podem ser hospedados / armazenados em [inserir países fora do Brasil], o que significa que podemos transferir qualquer informação que seja enviada por você através do site fora do Brasil para os fins abaixo: [Insira quais serviços você utiliza fora do Brasil (ou seja, hospedagem de sites, servidores de e-mail, banco de dados de marketing (ou seja, MailChimp, comércio eletrônico, servidor de e-mail, etc.)] Portanto, quando você [usa nosso site / nos envia um e-mail / inscreve-se em nosso boletim informativo, etc.], as informações pessoais enviadas podem ser armazenadas em servidores hospedados em [inserir países fora do Brasil]. Quando for o caso, tomaremos medidas para garantir que esses provedores usem o nível de proteção necessário para suas informações e obedeçam a acordos e medidas estritos definidos por [inserir nome da organização] para proteger seus dados e cumprir a proteção de dados relevante leis.

OU; [Inserir nome da organização] transfere dados pessoais para fora o Brasil para os fins abaixo: - • [Insira o motivo da transferência para fora da UE e para quem] • [Insira o motivo da transferência para fora da UE e para quem] • [Insira o motivo da transferência para fora da UE e para quem] Quando transferimos informações pessoais pelos motivos acima, utilizamos as medidas e mecanismos de proteção abaixo para garantir que seus dados pessoais estejam sempre protegidos: • [Insira as medidas de proteção tomadas] • [Insira as medidas de proteção tomadas] • [Insira as medidas de proteção tomadas] 21. CONSEQUÊNCIAS DE NÃO FORNECER SEUS DADOS Você não é obrigado a fornecer suas informações pessoais para [inserir nome da organização], no entanto, como essas informações são necessárias para [fornecermos nossos serviços / entregar seus produtos / interesses legítimos], não seremos capazes de oferecer alguns / todos os nossos serviços sem suas informações. 22. LEGÍTIMO INTERESSE (quando aplicável) Conforme observado na seção 'Como usamos seus dados pessoais' deste aviso, ocasionalmente processamos suas informações pessoais sob a base legal de interesses legítimos. Quando for esse o caso, realizamos uma avaliação completa para garantir que pesamos seus interesses e qualquer risco apresentado a você contra os nossos próprios, garantindo que são proporcionais e adequados. Usamos a base jurídica dos interesses legítimos para o processamento [insira os dados / finalidade do processamento com base nos interesses legítimos] e identificamos que nossos interesses são [declarar os interesses legítimos nos quais você se baseia]. 23. TEMPO DE RETENÇÃO DOS DADOS PESSOAIS A [inserir nome da organização] apenas retém informações pessoais pelo tempo necessário e temos políticas rígidas de revisão e retenção para cumprir essas obrigações. De acordo com a legislação tributária do Brasil, somos obrigados a manter seus dados pessoais básicos (nome, endereço, detalhes de

contato) por um período mínimo de 5 anos, após o qual serão destruídos. [insira qualquer outro período de retenção ou critério usado para determinar o período conforme relevante para seu tipo de negócio ou setor]. 24. CATEGORIAS DE DADOS ESPECIAIS Devido aos produtos, serviços ou tratamentos que oferecemos, [inserir nome da organização] às vezes precisa processar informações pessoais confidenciais (conhecidas como dados de categoria especial) sobre você, para [inserir os motivos pelos quais os dados de categoria especial são necessários]. Quando coletamos essas informações, só solicitaremos e processaremos o mínimo necessário para a finalidade especificada e identificaremos uma base legal compatível para fazê-lo. [A declaração de consentimento explícito abaixo pode ser adicionada onde os dados da categoria especial são obtidos se você estiver contando com o consentimento, caso contrário, você deve indicar a base do Artigo 11 da LGPD em que se baseia]. Quando contamos com seu consentimento para processar dados de categorias especiais, obteremos seu consentimento explícito por meio de [uma assinatura / mecanismo explícito]. Você pode modificar ou retirar o consentimento a qualquer momento, e agiremos imediatamente, a menos que haja uma razão legítima ou legal para não fazê-lo. Se você consentir que coletemos e usemos seu [saúde / médico] / [inserir tipo de categoria especial] para os fins declarados acima, assine abaixo e escreva seu nome:

Nome:

Assinatura:

25. MARKETING (se aplicável) Exemplo de Concentimento: Ocasionalmente, [Insira o nome da organização] deseja entrar em contato com você para informar os [especificar produtos / serviços / promoções] que oferecemos. Se consentir que utilizemos os seus dados de contacto para este fim, tem o direito de modificar ou retirar o seu consentimento a qualquer altura, utilizando as opções de cancelamento da subscrição ou contactando [Inserir Nome da Organização] diretamente. Se você consentir que o contatemos com o marketing e as ofertas mencionados acima, marque para dizer como gostaria de ser contatado: Mensagem Email Telefone Mensagem de texto (SMS) Chamada automática Exemplo de Legítimo interesse: [Inserir nome da organização] irá ocasionalmente enviar a você [especificar produtos / serviços / promoções] por [e-mail / SMS / correio] que foram identificados como sendo benéficos para nossos clientes e em nossos interesses. Essas informações serão relevantes para você como cliente e não são intrusivas e você sempre terá a opção de cancelar / cancelar a assinatura a qualquer momento. Se você preferir não receber o marketing e as ofertas mencionados acima, marque abaixo: Desejo não Receber campanhas de Marketing APRESENTAÇÃO DE RECLAMAÇÕES [Inserir nome da organização] apenas processa suas informações pessoais em conformidade com este aviso de privacidade e de acordo com as leis de proteção de dados relevantes. Se, no entanto, desejar apresentar uma reclamação em relação ao processamento dos seus dados pessoais ou não estiver satisfeito com a forma como tratámos as suas informações, tem o direito

de apresentar uma reclamação à Agência Nacional de Proteção de Dados (ANPD). [Insira o nome da organização] [Insira o nome do responsável pela proteção de dados] [Insira o endereço da organização] [Inserir telefone e e-mail da organização]

[Inserir ANPD] [Insira o endereço da ANPD] [Insira o telefone e e-mail da ANPD]

APÊNDICE H – TEMPLATE RESPONSABILIDADES DO DPO

A FIGURA DO ENCARREGADO DE DADOS (EPD/DPO) E SUAS ATRIBUIÇÕES DE ACORDO COM A LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/2018) 1) Introdução e conceito de Encarregado de Proteção de Dados (EPD/DPO) na legislação brasileira: A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) traz a listagem dos agentes envolvidos no tratamento de dados pessoais, conceituando suas funções e atribuições no contexto da legislação. Uma dessas figuras é a do "Encarregado de Proteção de Dados", conhecido, de acordo com a legislação europeia, como Data Protection Officer, ou simplesmente "DPO". Essa denominação é mencionada na GDPR (General Data Protection Regulation) nos art. 37 a 39 do referido diploma legal. A lei brasileira, por sua vez, trata do papel do DPO primordialmente na redação do art. 41, que merece ser aqui transcrito: Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. Da leitura do dispositivo acima, pode-se concluir que a nomeação de um EPD/DPO é obrigatória, respeitada eventual norma complementar estabelecida pela Autoridade Nacional de Proteção de Dados, que tem a prerrogativa de definir hipóteses de dispensa da necessidade da indicação de um EPD/DPO conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. 2. Atividades e atribuições do DPO Analisando as determinações da Lei Geral de Proteção de Dados em conjunto com a General Data Protection Regulation (GDPR), entende-se que o EPD/DPO tem, pelo menos, as seguintes funções: 2.1 Comunicação com os titulares dos dados pessoais em geral: prestação de esclarecimentos, quando solicitados, e adoção de providências, assegurando que os direitos dos titulares sejam claros e informados; 2.2 Link/elo de comunicação com a Autoridade Nacional: recebimento de informações, solicitações e comunicações da autoridade nacional e adoção de providências; 2.3 Orientação e conscientização dos colaboradores da empresa quanto às práticas

a serem tomadas em relação à proteção de dados pessoais, garantindo e controlando o cumprimento da legislação. Para tanto, pode criar/atualizar políticas de segurança da informação e proteção de dados e realizar auditorias para verificação da conformidade da empresa; 2.4 Coordenar/auxiliar o Controlador na elaboração do AIPD (Avaliação de Impacto à Proteção de Dados Pessoais), de acordo com o art. 5º, XVIII, da LGPD; 2.5 Execução de outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares. O EPD/DPO deve, portanto, ter autonomia e liberdade no desempenho de suas funções, limitando-se a orientar o agente de tratamento dos dados pessoais. Um aspecto importante de observância no cargo é a observância ao princípio da accountability, estabelecido pelo art. 6º da LGPD. Para tanto, o EPD/DPO precisa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. A necessidade de observação desse princípio torna o agente responsável pela conformidade em suas operações de tratamento com a LGPD e, também, define que as medidas de conformidade devem ser passíveis de demonstração pelo agente. Por fim, nos termos do § 1º do art. 41 da LGPD, o acesso ao DPO deve estar claro, de forma gratuita e facilitada nos meios de comunicação (sítio eletrônico) do controlador. 3. Perfil indicado para o profissional: qualificação e (des)necessidade de certificações É evidente, da interpretação das legislações aplicáveis à proteção de dados, a importância da função desempenhada pelo EPD/DPO. O profissional a ser indicado deverá, necessariamente, ter conhecimento – ainda que geral – de toda a operação realizada pela empresa. Além dessa leitura técnica da atividade da empresa, o EPD/DPO precisa ter conhecimentos multidisciplinares e conciliar expertises de tecnologia da informação, conhecimentos jurídicos e gestão de pessoas. É, portanto, altamente recomendável que o EPD/DPO possua conhecimento amplo da Lei Geral de Proteção de Dados – e demais legislações vigentes em outros países cuja empresa se relacione – e das melhores práticas de governança nacional e internacional relacionadas à segurança da informação: A doutrina especializada sobre o tema entende que o profissional indicado deve "reunir conhecimento técnico necessário para ser suporte, conselheiro, consultor interno e realizar a formação continuada dos gestores na cultura de proteção de dados".1 A Lei Geral de Proteção de Dados não traz qualquer obrigação legal de certificação para desempenho da função do EPD/DPO. Entretanto, das práticas adotadas no mercado, verifica-se que diversas certificações são desejáveis e recomendadas para o profissional que exercerá o cargo. Dentre elas, entendemos ser pertinente destacar algumas fornecidas pela EXIN (instituição independente de certificação de profissionais em diversas áreas da segurança da informação) 2 e pela IAPP3. 4. Ferramentas necessárias para a função: EPD/DPO externo, quantidade de profissionais e (im)possibilidade de desempenho de outro cargo na instituição O controlador pode, a seu exclusivo critério, optar por indicar EPD/DPO interno (colaborador pertencente ao quadro de funcionários da própria empresa) ou, ainda, terceirizar a função ("DPO as a service"). É interessante destacar que

a primeira versão da LGPD determinava que o encarregado deveria ser “pessoa natural indicada pelo controlador”, o que limitava o desempenho do cargo a, necessariamente, uma pessoa física. Entretanto, após as alterações sofridas pela Lei, a redação se modificou para prever que o encarregado é “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”. Sendo assim, conclui-se que a função de EPD/DPO pode ser exercida por pessoa física ou jurídica. A respeito da quantidade de profissionais nomeados para a função, não há impedimento ou determinação legal regrando esse ponto. Considerando a possibilidade de exercício da função por pessoa jurídica, entende-se que o cargo pode ser atribuído a mais de um profissional. Entretanto, em razão do provável – em comparação com a prática europeia de mercado – alto custo do EPD/DPO, é viável, havendo necessidade de contratação de mais de um profissional, a constituição de uma equipe auxiliar ao próprio Encarregado nomeado. Não há qualquer impedimento legal para o acúmulo de funções pelo profissional indicado, mas é recomendável que o profissional exerça somente esse cargo, especialmente em caso de grandes organizações. Por fim, quanto às ferramentas necessárias para o desenvolvimento da função, salienta-se que a lei não determina a adoção de ferramentas específicas. Considerando todas as atuações do EPD/DPO no programa de conformidade da empresa com a LGPD e na continuação da observação e obediência à legislação em vigor, a empresa, na qualidade de Controladora dos Dados, deve analisar a viabilidade na implantação de sistemas de segurança da informação e eventuais softwares para auxílio do desempenho do profissional. Checklist de conformidade: I. Nosso EPD/DPO se reporta diretamente ao nosso mais alto nível de gerenciamento e recebe a independência necessária para executar suas tarefas. II. Nosso EPD/DPO possui recursos suficientes para poder executar suas tarefas. III. Levaremos em conta os conselhos de nosso EPD/DPO e as informações que eles fornecem sobre nossas obrigações de proteção de dados. IV. Ao executar suas tarefas, nosso EPD/DPO leva em consideração o risco associado às operações de processamento e leva em consideração a natureza, escopo, contexto e objetivos do processamento. V. Nosso EPD/DPO é facilmente acessível como um ponto de contato para nossos funcionários, indivíduos.

APÊNDICE I – TEMPLATE: POLÍTICA VIOLAÇÃO DE DADOS

Declaração [Nome de sua empresa] está comprometida com nossas obrigações sob o sistema regulatório e de acordo com a Lei Geral de Proteção de Dados (LGPD) e mantém um programa robusto e estruturado para conformidade e monitoramento. Realizamos avaliações de risco frequentes e relatórios de análise de vulnerabilidades para garantir que nossos processos e procedimentos de conformidade sejam adequados para o propósito e que ações de mitigação sejam implementadas quando necessário. No entanto, reconhecemos que podem ocorrer violações, portanto, esta política declara nossa intenção e objetivos para lidar com tais incidentes. Embora entendamos que nem todos os riscos podem ser mitigados, operamos um sistema robusto e estruturado de controles, medidas e processos para ajudar a proteger os titulares dos dados e suas informações pessoais de quaisquer riscos associados ao processamento de dados. A proteção e a segurança dos dados pessoais que processamos são de extrema importância para nós e desenvolvemos protocolos específicos de dados para quaisquer violações relacionadas a LGPD e às leis de proteção de dados. Objetivo O objetivo desta política é fornecer a intenção, objetivos e procedimentos da Empresa em relação à violação de dados envolvendo informações pessoais. Como temos obrigações nos termos da LGPD, também temos a obrigação de garantir que procedimentos, controles e medidas adequadas estejam em vigor e sejam disseminadas a todos os funcionários, garantindo que eles estejam cientes dos protocolos e linhas de relatório para violações de dados. Esta política detalha nossos processos para relatar, comunicar e investigar tais violações e incidentes. Escopo Esta política se aplica a todos os funcionários da Empresa (ou seja, funcionários permanentes, a termo fixo e temporários, quaisquer representantes terceirizados ou subcontratados, trabalhadores de agências, voluntários, estagiários e agentes contratados com a Empresa no Brasil ou no exterior). A adesão a esta política é obrigatória e o não cumprimento pode levar a ações disciplinares. Segurança de Dados e Requisitos de Violação A definição da Empresa de violação de dados pessoais é qualquer incidente de segurança, falta de controle, falha de sistema ou humana, erro ou problema que leva a, ou resulta em, destruição, perda, alteração, divulgação não autorizada de, ou acesso a dados pessoais. Juntamente com a nossa abordagem 'Privacidade by Design' para proteger os dados também temos a obrigação legal, regulamentar e comercial de garantir que as informações pessoais sejam protegidas enquanto são processadas pela Empresa. Nossas medidas técnicas e organizacionais são detalhadas em nossa Política e Procedimentos de Proteção de Dados e Políticas de Segurança da Informação. Realizamos auditorias de informações para garantir que todos os dados pessoais por nós processados sejam identificados, avaliados, classificados e

registrados de forma adequada e precisa. Realizamos avaliações de risco que avaliam o escopo e o impacto de qualquer violação de dados em potencial, tanto na atividade de processamento quanto no titular dos dados. Implementamos medidas técnicas e organizacionais adequadas, eficazes e apropriadas para garantir um nível de segurança adequado aos riscos, incluindo (mas não se limitando a): • Pseudonimização e criptografia de dados pessoais; • Acesso restrito; • Revisão, auditoria e planos de melhoria para a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento; • Plano de recuperação de desastres e continuidade de negócios (DRP) para garantir backups atualizados e seguros e a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais em tempo hábil no caso de um incidente físico ou técnico; • Procedimentos de auditoria e testes de estresse regularmente para testar, avaliar e revisar a eficácia de todas as medidas em conformidade com os regulamentos de proteção de dados; • Programas de treinamento de proteção de dados frequentes e contínuos para todos os funcionários; • Avaliações da equipe e testes regulares de conhecimento para garantir um alto nível de competência, conhecimento e compreensão dos regulamentos de proteção de dados e as medidas que temos em vigor para proteger as informações pessoais; • Rever os processos internos para garantir que os locais onde as informações pessoais são transferidas, divulgadas, partilhadas ou devam ser eliminadas, é verificada novamente e autorizada pelo Encarregado de Proteção de Dados (DPO);

Objetivos • Aderir a Lei Geral de Proteção de Dados (LGPD – L13709) e ter procedimentos e controles robustos e adequados para identificar, investigar, relatar e registrar quaisquer violações de dados; • Desenvolver e implementar medidas técnicas e organizacionais adequadas, eficazes e apropriadas para garantir um alto nível de segurança no que diz respeito às informações pessoais; • Utilizar auditorias de informação e avaliações de risco para mapear dados e reduzir o risco de violações; • Ter procedimentos de gestão de risco adequados e eficazes para avaliar quaisquer riscos apresentados pelo processamento de informações pessoais; • Garantir que quaisquer violações de dados sejam relatadas aos órgãos reguladores corretos dentro dos prazos estabelecidos em quaisquer regulamentos, códigos de prática ou manuais; • Para usar investigações de violação e registros para avaliar a causa raiz de qualquer incidente e implementar uma revisão completa para evitar a ocorrência de novos incidentes; • Usar o Formulário de Violação de Dados para todas as violações de dados, independentemente da gravidade, para que quaisquer padrões nas causas possam ser identificados e corrigidos; • Proteger consumidores, clientes e colaboradores, incluindo suas informações e identidade; • Para garantir que, quando aplicável, o Encarregado de Proteção de Dados (DPO) seja envolvido e notificado sobre todas as violações de dados e questões de risco; • Garantir que a Agência Nacional de Proteção de Dados (ANPD) seja notificada de qualquer violação de dados (quando aplicável) com efeito imediato e, no mais tardar, no prazo de 72 horas após a Sociedade ter tomado conhecimento da violação; Procedimentos para tratar incidentes A

empresa tem controles robustos para prevenir violações de dados e para gerenciá-los caso correram. Nossos procedimentos e diretrizes para identificação, investigação e notificação de incidentes são detalhados a seguir. Nossa política de de violação de dados visa mitigar o impacto de quaisquer violações de dados e garantir que as notificações corretas sejam feitas. Monitoramento e Reporte de Incidentes A Empresa nomeou um Encarregado de Proteção de Dados (DPO) que é responsável pela revisão e investigação de qualquer violação de dados envolvendo informações pessoais, independentemente da gravidade, impacto ou contenção. Todas as violações de dados são comunicadas a esta pessoa com efeito imediato, seguindo-se os procedimentos detalhados nesta política. Todas as violações de dados serão investigadas, mesmo nos casos em que as notificações não sejam necessárias, e mantemos um registro completo de todas as violações de dados para garantir que a análise de lacunas e padrões esteja disponível e seja usada. Quando uma falha de sistema ou processo deu origem a uma violação de dados, a revisão de qualquer um desses processos é registrada nos registros de Gerenciamento de Mudanças. Procedimentos para tratar incidentes Identificação do incidente Assim que um incidente de dados é identificado, ele é relatada ao Líder Direto e ao Encarregado de Proteção de Dados (DPO) para que os procedimentos de incidente possam ser iniciados e seguidos sem demora. Relatar incidentes de forma completa e com efeito imediato é essencial para o funcionamento compatível da Empresa e não se trata de atribuir culpas. Esses procedimentos são para a proteção da Empresa, seus funcionários, clientes e terceiros e são de extrema importância para o cumprimento das normas legais. Assim que um incidente for relatado, medidas devem ser tomadas para conter o incidente. Tais medidas não estão no escopo deste documento devido à vasta natureza das violações e à variedade de medidas a serem tomadas, entretanto, o objetivo de tais medidas deve ser impedir qualquer risco / violação adicional para a organização, cliente, terceiros, sistema ou dados antes da investigação e do relatório. As medidas tomadas são anotadas no formulário de incidente em todos os casos. Registro do Incidente A Empresa utiliza um Formulário de Violação de Dados para todos os incidentes, que é preenchido para qualquer violação de dados, independentemente da gravidade ou resultado. Os formulários preenchidos são registrados na pasta de incidentes (eletrônico ou em papel) e analisados em relação aos registros existentes para verificar padrões ou recorrências. Em casos de violação de dados, o Encarregado de Proteção de Dados (DPO) é responsável por realizar uma investigação completa, nomeando a equipe responsável para conter a violação, registrando o incidente no formulário de violação e fazendo as notificações legais e relevantes. O preenchimento do Formulário de Violação de Dados só deve ser feito após a contenção do incidente. Uma investigação completa é conduzida e registrada no formulário de violação, com o resultado sendo comunicado a todos os funcionários envolvidos na violação, além da alta administração. Uma cópia do formulário de incidente preenchido é arquivada para fins de auditoria e documentação. Se aplicável, a Agência Nacional de Proteção de Dados (ANPD) e o (s) titular (es) dos dados

são notificados de acordo com os requisitos da LGPD (consulte a secção 6 desta política). Os protocolos da ANPD devem ser seguidos e seu Formulário de Violação de Dados deve ser preenchido e enviado. Além disso, qualquer indivíduo cujos dados ou informações pessoais tenham sido comprometidos é notificado, se necessário, e mantido informado durante a investigação, com um relatório completo sendo fornecido de todos os resultados e ações. Avaliação de Risco de Incidente Erro Humano Quando a violação de dados for o resultado de erro humano, uma investigação sobre a causa raiz deve ser conduzida e uma entrevista formal com o (s) funcionário (s) deve ser realizada. Uma revisão do (s) procedimento (s) associado (s) à violação é conduzida e uma avaliação de risco completa concluída de acordo com os Procedimentos de Avaliação de Risco da Empresa. Quaisquer vulnerabilidade identificada que tenham causado / contribuído para a violação são revisadas e o risco avaliado para mitigar qualquer ocorrência futura da mesma causa raiz. Tal investigação podem incluir, mas não estão limitados a: • Novo treinamento em áreas específicas / todas de conformidade; • Reavaliação do conhecimento e compreensão de conformidade; • Suspensão de tarefas relacionadas à conformidade; • Advertência formal (em linha com os procedimentos disciplinares da Empresa); Erro em Sistema Quando a violação de dados é o resultado de um erro / falha em sistema, a equipe de TI deve trabalhar em conjunto com o Encarregado de Proteção de Dados (DPO) para avaliar o risco e investigar a causa raiz do incidente. Uma análise de vulnerabilidades deve ser concluída no (s) sistema (s) envolvido (s) e uma revisão completa e um relatório devem ser adicionados ao Formulário de Violação de Dados. Quaisquer vulnerabilidades identificadas que tenham causado / contribuído para o incidente devem ser revisadas e o risco avaliado para mitigar e prevenir qualquer ocorrência futura da mesma causa raiz. Todos os detalhes do incidente devem ser determinados e ações de mitigação como as seguintes devem ser tomadas para limitar o impacto do incidente: • Tentar recuperar qualquer equipamento perdido ou informações pessoais; • Desligamento de um sistema de TI; • Remover um funcionário de suas tarefas; • O uso de backups para restaurar informações perdidas, danificadas ou roubadas; • Tornar o edifício Seguro; • Se o incidente envolver qualquer código de entrada ou senha, esses códigos devem ser alterados imediatamente e os membros da equipe informados;

Avaliação de Risco O Encarregado de Proteção de Dados (DPO) deve averiguar quais informações estavam envolvidas na violação de dados e quais etapas subsequentes são necessárias para remediar a situação e mitigar quaisquer violações futuras. O investigador principal deve observar: • O tipo de informação envolvida • É sensibilidade ou conteúdo pessoal • Quais proteções existem (por exemplo, criptografia)? O que aconteceu com as informações / Onde estão agora? • Se existem consequências / implicações mais amplas para o incidente O líder responsável deve manter um registro contínuo e um relatório claro detalhando a natureza do incidente, as medidas tomadas para preservar as evidências, as notas de quaisquer entrevistas ou declarações, a avaliação do risco / investigação e

quaisquer recomendações para trabalhos / ações futuras.

Notificação de Incidente Todos os funcionários foram informados das responsabilidades da Empresa e desenvolvemos canais internos para apontamento de violação de dados para garantir que as violações de dados que caiam nos critérios de notificação sejam identificadas e relatadas sem demora.

Notificação para Agência Nacional de Proteção de Dados A Agência Nacional de Proteção de Dados (ANPD) deve ser notificada de qualquer violação que possa resultar em risco para os direitos e liberdades das pessoas. São situações que, se a violação fosse ignorada, teriam efeitos prejudiciais significativos para o indivíduo. Quando aplicável, a ANPD é notificada da violação o mais tardar 72 horas após a Empresa tomar conhecimento da mesma e é mantida notificada durante qualquer investigação de violação, sendo fornecido um relatório completo, incluindo resultados e ações atenuantes o mais rapidamente possível, e sempre dentro de qualquer período de tempo especificado. Se, por qualquer motivo, não for possível comunicar o incumprimento à ANPD no prazo de 72 horas, a notificação será feita assim que possível, acompanhada dos motivos do eventual atraso. Quando uma violação é avaliada pelo Encarregado de Proteção de Dados (DPO) e considerada improvável que resulte em um risco para os direitos e liberdades das pessoas físicas, reservamo-nos o direito de não informar a ANPD. A notificação à ANPD conterá: - • Uma descrição da natureza da violação de dados pessoais; • As categorias e o número aproximado de titulares de dados afetados; • As categorias e o número aproximado de registros de dados pessoais em questão; • O nome e os detalhes de contato do nosso Encarregado de Proteção de Dados (DPO) e / ou qualquer outro ponto de contato relevante (para obter mais informações); • Uma descrição das prováveis consequências da violação de dados pessoais; • Uma descrição das medidas tomadas ou propostas a serem tomadas para lidar com a violação de dados pessoais (incluindo medidas para mitigar seus possíveis efeitos adversos); Os procedimentos de incidentes são sempre seguidos e uma investigação realizada, independentemente das nossas obrigações de notificação e resultados, sendo os relatórios retidos e disponibilizados à ANPD, se solicitado. Quando a Empresa atua na capacidade de um processador, garantiremos que o controlador seja notificado da violação sem atrasos indevidos. Nos casos em que atuamos na capacidade de um controlador usando um processador externo, temos um acordo por escrito em vigor declarando que o processador é obrigado a nos notificar sem demora após tomar conhecimento de uma violação de

Itens Notificados Quando for provável que uma violação de dados pessoais resulte em um alto risco para os direitos e liberdades das pessoas físicas, sempre comunicaremos a violação de dados pessoais ao titular dos dados, sem atrasos indevidos, em um formato escrito, claro e legível. A notificação ao Titular dos Dados deve incluir: • A natureza da violação de dados pessoais; • O nome e os detalhes de contato do nosso Encarregado de

Proteção de Dados (DPO) e / ou qualquer outro ponto de contato relevante (para obter mais informações); • Uma descrição das prováveis consequências da violação de dados pessoais; • Uma descrição das medidas tomadas ou propostas a serem tomadas para lidar com a violação de dados pessoais (incluindo medidas para mitigar seus possíveis efeitos adversos); Nós nos reservamos o direito de não informar o titular dos dados de qualquer violação de dados pessoais quando implementamos as medidas técnicas e organizacionais adequadas que tornam os dados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los (ou seja, criptografia, mascaramento de dados, etc.) ou onde tomamos medidas subsequentes que garantem que o elevado risco para os direitos e liberdades do titular dos dados já não se materializa. Se informar o titular dos dados sobre a violação envolver um esforço desproporcional, reservamo-nos o direito de, em vez disso, fazer uma comunicação pública em que o (s) titular (es) dos dados são informados de maneira igualmente eficaz.

Guarda dos Registros de Incidentes Todos os registros e anotações feitas durante a identificação, avaliação e investigação da violação de dados são registrados e autorizados pelo Encarregado de Proteção de Dados (DPO) e são mantidos por um período de 5 anos a partir da data do incidente. Os formulários de incidentes devem ser revisados mensalmente para avaliar os padrões ou recorrências de violação e as ações tomadas para evitar a ocorrência de novos incidentes. Responsabilidades A Empresa garantirá que todos os funcionários tenham tempo, recursos e suporte para aprender, compreender e implementar todos os procedimentos deste documento, bem como compreender suas responsabilidades e como reportar as violações de dados. O Encarregado de Proteção de Dados (DPO) é responsável por conduzir auditorias de conformidade regulares, monitoramento de análise de vulnerabilidades, pelas revisões subsequentes e acompanhamento de ações.

APÊNDICE J – TEMPLATE: POLÍTICA DE GESTÃO DE DOCUMENTOS

1. OBJETIVO: O objetivo desta política é definir e documentar o procedimento, diretrizes e orientações para a gestão de documentos físicos no [NOME DA EMPRESA]. 2. APLICAÇÃO: Aplica-se a todas as áreas que possuam ou precisem implantar sistema de arquivamento físico de documentos. 3. TERMOS E DEFINIÇÕES: Arquivo físico: Conjunto de documentos produzidos e recebidos pelos colaboradores da [NOME DA EMPRESA], através de órgãos públicos, instituições de caráter público e entidades privadas ou internamente, em decorrência do exercício das atividades laborais, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

Documento físico: Um documento que apresenta dados susceptíveis de serem utilizados para comprovar algo e pode ser representado por uma carta, um diploma ou um escrito que reproduz um acontecimento, uma situação ou uma circunstância. É um documento material, tangível e possui uma representação no mundo físico, seja original ou que reproduzido por meio de vários sistemas, tais como, fotocópia ou a fotografia.

Eliminação: destruição de documentos de acordo com os prazos legais de retenção. 4. CONSIDERAÇÕES: 4.1. Os colaboradores da [NOME DA EMPRESA] exercem suas funções obedecendo às regras de conduta dispostas no Código de Conduta e as orientações dos supervisores, gestores e líderes diretos de cada equipe. 4.2. Há fluxo intenso de circulação de documentos em vias físicas nas dependências da [NOME DA EMPRESA] e, por isso, tais documentos - especialmente aqueles que possuem, em seu conteúdo, dados pessoais - devem ser arquivados de maneira adequada. 4.3. Deve haver preferência ao armazenamento de documentos em formato eletrônico e destinação e/ou eliminação adequada de vias físicas, sejam originais ou reproduzidas. 5. PROCEDIMENTOS: 5.1. Os documentos físicos que precisarem ser arquivados fisicamente nas dependências da [NOME DA EMPRESA] devem ser armazenados no Arquivo Geral, localizado em sala trancada e alarmada quando não em uso e com acesso devidamente monitorado. Devem ser asseguradas a eficiência e a qualidade dos procedimentos de geração, recebimento, tramitação e arquivamento adequado de documentos e dos processos de avaliação, destinação final (eliminação ou guarda permanente) e eventual auditoria de documentos. 5.2. O acesso ao Arquivo físico deve ser controlado e restrito, inclusive às áreas com documentos confidenciais da [NOME DA EMPRESA]. 5.3. O arquivamento de documentos físicos deve ser feito mediante registro de protocolo (recebimento, registro, classificação, distribuição e controle de retirada e devolução) do processo de arquivamento, armazenando-se o respectivo registro em formato digital no sistema interno da [NOME DA EMPRESA], com acesso restrito ao usuário responsável pelo gerenciamento do Arquivo físico. 5.4. A

eliminação e descarte de arquivos físicos deverá ocorrer em consonância com os prazos legais estipulados para a manutenção das informações pela [NOME DA EMPRESA].

6. APLICAÇÃO DAS MEDIDAS DISCIPLINARES

6.1. A aplicação das medidas disciplinares deve ocorrer de acordo com a sua natureza e diretrizes sem prejuízo das sanções administrativas, cíveis e penais, o descumprimento das normas contidas nos Princípios de Conduta e Ética e nas políticas e procedimentos internos e na legislação é passível de medidas disciplinares, conforme abaixo: i. Advertência verbal; ii. Advertência por escrito; iii. Suspensão; iv. Demissão sem justa causa; v. Demissão por justa causa. 6.2. A aplicação de qualquer das medidas disciplinares descritas acima será definida de acordo com a gravidade da infração. 6.3. Outras medidas poderão ser recomendadas, que não são consideradas medidas disciplinares, tais como: treinamento, mudança no processo, alteração de sistema ou ferramenta, estabelecimento de controles adicionais, etc. A aplicação de tais medidas deve ser acompanhada pela área XXX, a fim de assegurar a sua implementação. 7. SANÇÕES 7.1. O descumprimento das disposições legais e regulamentares aqui previstas sujeita os infratores a aplicação de medidas disciplinares previstas em normativos internos, sem prejuízo de sanções administrativas, cíveis e até criminais, dentre outras medidas cabíveis. 8. DISPOSIÇÕES GERAIS: 8.1. As diretrizes estabelecidas neste documento devem ser observadas pela Alta Administração e por todos os colaboradores da [NOME DA EMPRESA], aí incluídos diretores, empregados, contratados, prestadores de serviço, estagiários e aprendizes

APÊNDICE K – TEMPLATE: POLÍTICA DE PROTEÇÃO DADOS

26. INTRODUÇÃO

(inserir nome da empresa) precisa coletar e processar certos tipos de informações sobre os Indivíduos ou Usuários do Serviço que entram em contato com (inserir nome da empresa) para continuar nosso trabalho. Essas informações pessoais devem ser coletadas e tratadas de forma apropriada, sejam coletadas em papel, armazenadas em um banco de dados de computador ou registradas em outro material.

27. CONTROLADOR DE DADOS (inserir nome da empresa) é o Controlador de Dados, o que significa que ele determina para quais fins as informações pessoais mantidas serão usadas. Ele também é responsável por notificar a Autoridade Supervisora sobre os dados que possui e os fins gerais para os quais esses dados serão usados.

28. COMPARTILHAMENTO DE DADOS (inserir nome da empresa) pode compartilhar dados com outras agências, como a autoridades locais, órgãos de financiamento e outras agências voluntárias. O titular dos dados deverá ser informado na maioria das circunstâncias como e com quem suas informações serão compartilhadas. Existem circunstâncias em que a lei permite (inserir nome da empresa) divulgar dados (incluindo dados confidenciais) sem o consentimento do titular dos dados. São elas: a) Cumprindo um dever legal ou conforme autorizado pelo Secretário de Estado; b) Proteger interesses vitais de um indivíduo / usuário do serviço ou outra pessoa; c) O titular já tornou as informações públicas; d) Conduzir qualquer processo legal, obter aconselhamento jurídico ou defender quaisquer direitos legais; e) Monitoramento para fins de igualdade de oportunidades - ou seja, raça, deficiência ou religião; f) Prestar um serviço confidencial onde o consentimento do titular não pode ser obtido ou onde é razoável prosseguir sem consentimento.

(inserir nome da empresa) considera o tratamento legal e correto das informações pessoais muito importante para o sucesso do trabalho e para manter a confiança das pessoas com quem negociamos. (inserir nome da empresa) pretende garantir que as informações pessoais sejam tratadas de forma legal e correta. Para este fim, (insira o nome da empresa) irá aderir aos Princípios de Proteção de Dados, conforme detalhado na Lei Geral de Proteção de Dados (L13709 de set/2020). Especificamente, os Princípios exigem que as informações pessoais: a) Devem ser processadas de forma justa e legal e, em particular, não devem ser processados a menos que condições específicas sejam atendidas; b) Deve ser obtido apenas para um ou mais dos fins especificados na Lei, e não deve ser processado de qualquer forma incompatível com esse fim ou esses fins; c) Deve ser adequado, relevante e não excessivo em relação a esse (s) propósito (s); d) Deve ser preciso e, quando necessá-

rio, mantido atualizado; e) Não deve ser mantido por mais tempo do que o necessário; f) Deve ser processado de acordo com os direitos dos titulares dos dados ao abrigo da Lei; g) Devem ser mantidos em segurança pelo Controlador de Dados, que toma as medidas técnicas e outras medidas adequadas para evitar o processamento não autorizado ou ilegal ou perda acidental ou destruição de, ou danos a, informações pessoais; h) Não devem ser transferidos para um país ou território fora do Brasil, a menos que esse país ou território garanta um nível adequado de proteção dos direitos e liberdades dos titulares em relação ao tratamento de informação pessoal.

(insira o nome da empresa) irá, por meio de gerenciamento apropriado e aplicação estrita de critérios e controles: a) Observar plenamente as condições relativas à coleta e uso justo de informações; b) Cumprir suas obrigações legais para especificar os fins para os quais as informações são usadas; c) Coletar e processar informações adequadas e apenas na medida em que for necessário para atender às suas necessidades operacionais ou para cumprir quaisquer requisitos legais; d) Garantir a qualidade das informações utilizadas; e) Garantir que os direitos dos titulares possam ser plenamente exercidos de acordo com a lei. Esses incluem: • Ser informado de que o processamento está sendo realizado; • Livre acesso às informações pessoais; • Impedir o processamento em certas circunstâncias; • Corrigir, retificar, bloquear ou apagar informações que sejam consideradas informações erradas. f) Tome medidas de segurança técnicas e organizacionais adequadas para proteger as informações pessoais; g) Certifique-se de que as informações pessoais não sejam transferidas para o exterior sem salvaguardas adequadas; h) Trate as pessoas com justiça e, independentemente da idade, religião, deficiência, sexo, orientação sexual ou etnia ao lidar com pedidos de informação; i) Estabelecer procedimentos claros para responder aos pedidos de informação.

29. COLETA DE DADOS

O consentimento informado é quando o titular entende claramente por que suas informações são necessárias, com quem elas serão compartilhadas, as possíveis consequências de concordar ou recusar o uso proposto dos dados.

(insira o nome da empresa) garantirá que os dados sejam coletados dentro dos limites definidos nesta política. Isso se aplica a dados coletados pessoalmente ou por meio do preenchimento de um formulário. Ao coletar dados, (insira o nome da empresa) garantirá que o titular: a) Entenda claramente porque a informação é necessária; b) Entenda para que será usado e quais são as consequências caso o titular decida não dar consentimento para o processamento; c) Na medida do possível, conceder consentimento explícito para que os dados sejam processados; d) Receber informações suficientes sobre porque seus dados são necessários e como eles serão usados.

30. ARMAZENAMENTO DE DADOS

As informações e registros relativos aos usuários do serviço serão armazenados de forma segura e somente estarão acessíveis a pessoas autorizadas. As informações serão armazenadas apenas enquanto for necessário ou exigido por lei e serão descartadas de forma adequada. É responsabilidade da (inserir nome da empresa) garantir que todos os dados pessoais e da empresa não sejam recuperáveis de qualquer sistema de computador usado pela empresa para coleta e processamento desses dados.

31. ACESSO AOS DADOS

Todos os titulares têm o direito de acessar as informações (inserir nome da empresa) que detém sobre eles. (insira o nome da empresa) também tomará medidas razoáveis para garantir que essas informações sejam mantidas atualizadas. Em adiciona, (insira o nome da empresa) irá se assegurar que: a) Designar um Encarregado de Proteção de dados com responsabilidade específica para garantir a conformidade com LGPD; b) Todos que processam informações pessoais entendem que são contratualmente responsáveis por seguir as políticas e boas práticas de proteção de dados; c) Todos que processam informações pessoais são devidamente treinados para fazê-lo; d) Todos os que processam informações pessoais são supervisionados de forma adequada; e) Lidar prontamente com quaisquer dúvidas sobre como lidar com informações pessoais; f) Descreve claramente como trata as informações pessoais; g) Revisar e auditar regularmente as maneiras como mantém, gerencia e usa informações pessoais; h) Avaliar regularmente seus métodos e desempenho em relação ao tratamento de informações pessoais; i) Todos os funcionários estão cientes de que uma violação das regras e procedimentos identificados nesta política pode levar a ações disciplinares contra eles.

Esta política será revisada e atualizada conforme necessário para refletir as melhores práticas em gerenciamento de dados e segurança da informação, para garantir a conformidade com quaisquer alterações ou emendas feitas à LGPD (L13709).

Em caso de dúvidas ou perguntas em relação a esta política, entre em contato com o Encarregado pelo tratamento de dados pessoais da (insira o nome da empresa e os contatos do Encarregado de Proteção de Dados / DPO).

APÊNDICE L – TEMPLATE: AVALIAÇÃO DE IMPACTO DE PRIVACIDADE (DPIA)

AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS - (AIPD)

	ID	QUESTÕES	RESPOSTA	DETALHAMENTO
3.QUESTIONÁRIO	0	Selecione qual das bases legais melhor se enquadra para a finalidade da coleta e processamentos dos dados pessoais. (Consulte o DPO caso precise de suporte quanto às bases legais)		
	1	**Os dados serão armazenados somente na rede interna da "Nome da Empresa" (Sistemas, Servidor de Arquivos, Sharepoint ou OneDrive)?**		
	2	Foi definido um controle de acesso para os dados coletados?		
	3	**Foram adotados critérios de segurança para a transferência dos dados?**		
	4	Foi definido um período para retenção e processo de descarte para os dados coletados?		
	5	**Será coletado o consentimento do Titular autorizando o processamento de seus dados pela "Nome da Empresa" e por Terceiros?**		
	6	Foi estabelecido um processo para o Titular dos dados exercer seus direitos em relação aos dados coletados? (ex.: solicitar atualização dos dados, revogar o consentimento, pedir para ser esquecido, solicitar a portabilidade dos dados entre outros)?		
	7	**Caso venham a público as informações que o Projeto pretende coletar, os Titulares não serão expostos a situações vexatórias e / ou terão sua liberdade comprometida?**		
	8	Caso seja necessário o envio de mensagens por whatsapp, e-mail, ligações telefônicas ou similares, existirá um processo prévio para a coleta do consentimento dessas pessoas?		
	9	**Todos os empregados, funcionários, agentes e terceiros envolvidos no Projeto foram treinados sobre as normas de proteção de dados pessoais?**		
	10	Em caso de violação dos dados pessoais na execução do Projeto, estão disponíveis meios para impedir o agravamento da violação?		
	11	**Em caso de violação dos dados pessoais na execução do Projeto, estão disponíveis meios e modos para impedir nova violação?**		

TRABALHOS PUBLICADOS PELO AUTOR

1. Francyelcyo Farias, Rodolfo de Barros, **Lei Geral de Proteção de Dados LGPD Da Teoria a Prática**, 17th International Conference on Information Systems Technology Management, 09/2020, CONTECSI. São Paulo, Brasil, 2020. (Qualis CC 2017, B4)

2. Francyelcyo Farias, Rodolfo de Barros, **LGPD – From Theory to Practice**, CISTI'2022 - 17ª Conferência Ibérica de Sistemas e Tecnologias de Informação, realizada entre 22 e 25 de junho de 2022, na Universidad Politécnica de Madrid (UPM), Madrid, Espanha. (Qualis CC 2021, A4)