Organizadora:
Elaine Cristina Oliveira Guerra

Coordenadoras:
Elaine Guerra | Melissa Barrioni | Stella Campos | Cristiane Araújo

Manual Prático de Adequação da LGPD para Escritórios de Advocacia

OAB MINAS GERAIS | Comissão de Proteção de Dados

EXPERT EDITORA DIGITAL

Este livro tem como objetivo oferecer orientações práticas tanto para escritórios de advocacia quanto para seus clientes no processo de adaptação e implementação da Lei Geral de Proteção de Dados (LGPD). A LGPD representa um desafio significativo para todos, e considerando que os escritórios de advocacia lidam diariamente com informações pessoais e sensíveis de seus clientes, seja para fins administrativos ou judiciais, a Comissão de Proteção de Dados da OAB/MG, por meio de seu núcleo de prática, desenvolveu este manual abrangente.

O objetivo deste manual é auxiliar de forma didática em todas as etapas que um escritório de advocacia deve considerar para adaptar ou aprimorar os processos e fluxos relacionados aos dados de seus clientes. Além disso, dada a incerteza persistente que muitas empresas enfrentam, existe uma tendência a cometer erros durante as adaptações, especialmente em relação ao consentimento e à inclusão de cláusulas contratuais, ou mesmo ao tratamento excessivo de dados.

Este livro concentra-se na adaptação abrangente, abordando não apenas contratos e termos, mas todos os aspectos relacionados à LGPD. Portanto, elaboramos este manual de adequação e implementação da LGPD com carinho, atendendo às necessidades de seu escritório de advocacia e de seus clientes.

Elaine Guerra

Apoiadores

Patrocinadores

ISBN 978-65-6006-073-9

Manual Prático de
Adequação da LGPD
para Escritórios de Advocacia

Direção editorial: Luciana de Castro Bastos
Diagramação e Capa: Editora Expert
Revisão: Do Autor
A regra ortográfica usada foi prerrogativa do autor.

Dados Internacionais de Catalogação na Publicação (CIP)
GUERRA, Elaine
BARRIONI Melissa
CAMPOS Stella
ARAÚJO, Cristiane (coord.)
Titulo: Manual Prático de Adequação da LGPD para Escritório de Advocacia - Belo Horizonte - Editora Expert - 2024
Coordenadores: Elaine Guerra, Melissa Barrioni, Stella Campos e Cristiane Araújo
ISBN: 978-65-6006-073-9
Modo de acesso: https://experteditora.com.br
1.Direito Digital
2.Lei Geral proteção de dados
3.Escritório de advocacia
4. Proteção de informações pessoais
I. I. Título.
CDD: 340.0285

Pedidos dessa obra:

experteditora.com.br
contato@editoraexpert.com.br

EXPERT
EDITORA DIGITAL

Patrocínio:
Ordem Dos Advogados Do Brasil
Seção Minas Gerais - OAB/MG

Presidente:
Sérgio Rodrigues Leonardo

Vice-Presidente:
Angela Parreira De Oliveira Botelho

Secretário Geral:
Sanders Alves Augusto

Secretário Geral Adjunto:
Cassia Marize Hatem Guimarães

Tesoureiro:
Fabrício Souza Cruz Almeida

Tesoureiro Adjunto:
Marco Antonio Oliveira Freitas

Diretor Institucional:
Romulo Brasil De Avelar Campos
Wagner Antonio Policeni Parrot

Diretor De Apoio As Subseções:
Alvaro Guilherme Ribeiro Matos

Diretor De Prerrogativas:
Ercio Quaresma Firpe

Diretor De Interiorização:
Bernardo Carvalho Brant Maia
Marcio Facchini Garcia
Rodrigo Carvalho Fernandes Martins Ribeiro

Diretor De Inclusão:
William Dos Santos

Comissão de Proteção de Dados OABMG

Presidente da Comissão Proteção de Dados:
Melissa Barrioni e Oliveira
Vice-Presidente da Comissão de Proteção de Dados:
Stella Muniz Campos Elias
Diretora do Núcleo de Prática da Comissão de Proteção de Dados:
Elaine Cristina Oliveira Guerra

Livro: Manual Prático de Adequação da LGPD para Escritório de Advocacia

Organizadora:
Elaine Cristina Oliveira Guerra

Apoio da organização:
Cristiane Araújo, Melissa Barrioni e Oliveira, Stella Muniz Campos Elias

Autores:
Adiél Lima
Alan de Souza Pinto
Alessandra C. Puig Casariego
Aline Pelet Teles de Menezes
Carlos Henrique Almeida Salgado
Elaine Cristina Oliveira Guerra
Elaine Cristina Pereira dos Santos Nery
Emily Matias Assumpção
Gabriel Campos Cunha
Isabela Cristina Maia da Cruz
Izabela Nunes Pinto
Melissa Barrioni e Oliveira
Priscila Silva Ribeiro
Renato Almeida Viana
Stella Muniz Campos Elias

Revisão Ortográfica:
Edson Braz Carvalho Cruz
Jornalista graduado na UFMG. Especialista em Revisão de Textos pelo Instituto de Educação Continuada (IEC) PUC Minas.

SOBRE OS COORDENADORES

Cristiane Araújo: Coordenadora de Proteção de Dados da ESA/MG; Advogada e Professora, Mestranda em Direito pela UFMG; Coordenadora do NPJ da FAMINAS- BH; Especialista em implantação de Programa de Compliance e Proteção de Dados; Especialista em advocacia Trabalhista e Compliance pela ESA OAB/MG. Pós-graduanda em Direito; Conselheira Seccional OAB/MG.

Elaine Cristina Oliveira Guerra: Mestranda em Inovação Tecnológica e Propriedade Intelectual. Especialista em Direito, Inovação e Tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Pesquisadora da USP/SP. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados) e a Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora de capítulo de livro jurídico. Autora do "Manual Prático de Adequação da LGPD com enfoque nas Relações do Trabalho". Diretora do Núcleo de Prática de OAB/MG. Pesquisadora da USP/SP e da UFMG/MG. Mentora em projetos de LGPD. Advogada. Professora de Pós-Graduação.

Melissa Barrioni e Oliveira: Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora do Conselho Federal da OAB Nacional. Professora e Coordenadora da Pós-graduação em Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em LGPD e Proteção de Dados. Data Protection Officer – DPO. Mestranda em Educação Tecnológica pelo CEFET/UFMG. Licenciatura em Letras em curso no Instituto Anima de Educação. Pós-graduada em Docência Jurídica e Direito Digital.

Stella Muniz Campos Elias: Advogada Empresarial, Mestre em Direito, Especialista e Consultora em Proteção de Dados, DPO as a service, Especialista e Consultora em Proteção Trabalhista,

Coordenadora da Pós-graduação em Proteção de Dados da ESA OAB/MG, Professora de pós-graduação e MBAs, Palestrante, Vice-presidente da Comissão de Proteção de Dados da OAB-MG, Membro da Comissão Direito da Escola da OAB/MG, Membro Consultora da Comissão Especial de Proteção de Dados da OAB Nacional, Membro da Comissão Direito de Direitos Sociais e Trabalhistas da OAB/MG.

SOBRE OS AUTORES

Adiél Lima: Identity Management, Access Management, Data Protection, AWS Security, NIST CSF e DCPT. Risk Mapping; Vulnerability Management; Employee training. Mais de 10 certificações, sendo a maioria em segurança. http://nuvym.net.

Alan de Souza Pinto: Mestrando em Inovação Tecnológica, pela UFMG, Bolsista CAPES; Pós-graduado em Direito Digital e Proteção de Dados, pela EBRADI; Pós-graduado em Direito Civil Aplicado, pela PUC Minas; Graduado em Direito, pela PUC Minas; Membro da Comissão de Proteção de Dados da OAB/MG; Consultor em Privacidade e Proteção de Dados Pessoais; Advogado.

Alessandra C. Puig Casariego: Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG, membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em direito da economia e da empresa pela FGV. Master of Business Administration - MBA em Direito corporativo e Governança pela Escola superior da advocacia. Pós-graduação em direito bancário pela FGV. Certificação em compliance pela KPMG. Certificação em investigações corporativas pela KPGM. Curso de Extdnsso em Lei geral de proteção de dados pela PUC-RS.

Aline Pelet Teles de Menezes: Advogada inscrita na OAB/MG nº 211.427, especialista em Direito Empresarial pela PUC-MG e pós-graduanda em Direito Digital, Proteção de Dados e Compliance Trabalhista pela EMD, graduada em Direito e Relações Internacionais. Vice-presidente da Comissão de Direito Digital e Proteção de dados da

45ªSubseção da OAB, ANAD e Comissão Estadual de Proteção de Dados da OAB/MG.

Carlos Henrique Almeida Salgado: Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP; Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

Elaine Cristina Oliveira Guerra: Mestranda em Inovação Tecnológica e Propriedade Intelectual. Especialista em Direito, Inovação e Tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Pesquisadora da USP/SP. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados) e a Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora de capítulo de livro jurídico. Autora do "Manual Prático de Adequação da LGPD com enfoque nas Relações do Trabalho". Diretora do Núcleo de Prática de OAB/MG. Pesquisadora da USP/SP e da UFMG/MG. Mentora em projetos de LGPD. Advogada. Professora de Pós-Graduação.

Elaine Cristina Pereira dos Santos Nery: Advogada. Pedagoga e Professora de Educação Física. Especialista em Direito Empresarial, Trabalhista e Direito Público. Especialista em Privacidade e Proteção de dados. Especialista em Adequação a LGPD no Setor de Recursos Humanos – RH, Especialista em Adequação a LGPD na Área da Saúde. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora e Palestrante em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão

de Proteção de Dados da OAB/MG e Membro da Comissão de Proteção de Dados da UFVJM.

Emily Matias Assumpção: Advogada: Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

Gabriel Campos Cunha: Coordenador responsável pelas áreas de Direito Digital e Proteção de Dados do escritório Lacerda Diniz Sena Advogados. Atua com gestão de riscos empresariais, auditoria de conformidade legal, consultoria para adequações ao Direito da Proteção de Dados e Direito Digital.

Isabela Cristina Maia da Cruz: Advogada, Especialista em Direito Digital e Compliance. Membro da Comissão de Proteção de Dados da OAB/MG. Presidente da Comissão de Proteção de Dados Subseção Vespasiano da OAB/MG.

Izabela Nunes Pinto: Advogada. Membro colaborador (nomeado) da Comissão de Proteção de Dados da OAB/MG. Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Curso de Direito para Startups na Europa (envolvendo GDPR, LGPD e outros temas relacionados ao Direito Digital) pela Academy da Platzi. Finalista, ocupando o 3º Lugar Geral do Brasil da 1a Edição do LawCamp - 1a Competição de Implementação da LGPD no Brasil (com entrega de certificação para os 3 times vencedores). Palestrante (Adequação/ Implementação da LGPD e Direito Digital).

Melissa Barrioni e Oliveira: Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora do Conselho Federal da OAB Nacional. Professora e Coordenadora da

Pós-graduação em Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em LGPD e Proteção de Dados. Data Protection Officer – DPO. Mestranda em Educação Tecnológica pelo CEFET/UFMG. Licenciatura em Letras em curso no Instituto Anima de Educação. Pós-graduada em Docência Jurídica e Direito Digital.

Priscila Silva Ribeiro: DPO Data Protection (Encarregado de dados), Advogada, Membro da Comissão de Proteção de Dados da OAB/MG, Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPPD pela Legal *Ethics and Compliance*. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

Renato Almeida Viana: Coordenador do Comitê de LGPD do Centro de Estudos das Sociedades de Advogados de Minas Gerais – CESA/MG. Membro do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Escola Superior da Advocacia. Advogado.

Stella Muniz Campos Elias: Advogada Empresarial, Mestre em Direito, Especialista e Consultora em Proteção de Dados, DPO as a service, Especialista e Consultora em Proteção Trabalhista, Coordenadora da Pós-graduação em Proteção de Dados da ESA OAB/MG, Professora de pós-graduação e MBAs, Palestrante, Vice-presidente da Comissão de Proteção de Dados da OAB-MG, Membro da Comissão Direito da Escola da OAB/MG, Membro Consultora da Comissão Especial de Proteção de Dados da OAB Nacional, Membro da Comissão Direito de Direitos Sociais e Trabalhistas da OAB/MG.

SUMÁRIO

3. O INÍCIO - PREPARAÇÃO

4. ORGANIZAÇÃO e AÇÕES PRELIMINARES

5. IMPLEMENTAÇÃO/GOVERNANÇA

INTRODUÇÃO

Com a aprovação da Lei Geral de Proteção de Dados - LGPD, Lei n. 13.709/2018, foi inserido ao ordenamento jurídico brasileiro uma regulamentação expressa sobre o tema da privacidade e proteção de dados, cujo objetivo principal visa garantir um tratamento de dados pessoais mais transparente aos titulares de dados.

Neste sentido, todas as empresas, independente do ramo e se obtém lucro econômico, incluindo-se aqui os escritórios de advocacia, devem seguir as regras da LGPD.

Para a advocacia, o tema se torna ainda mais importante, pois lidamos diariamente com informações pessoais dos clientes, de processos, dos contratos, de colaboradores, dos prestadores de serviços, entre outros, sendo de observância obrigatória a todos os escritórios de advocacia que estes procedam à realização da adequação das rotinas internas para obedecer a LGPD.

Diante desta nova exigência, a Comissão de Proteção de Dados da OAB/MG elaborou o presente manual, para auxiliar e descrever didaticamente todas as etapas que a advocacia precisa se atentar na hora de adequar os processos e fluxos das operações de tratamento de dados dos próprios escritórios à LGPD.

Vale ressaltar que este manual se trata de documento apenas orientativo, não sendo um modelo exaustivo de programa de adequação, tampouco um modelo padrão a ser estritamente implementado, pois contamos com a união dos vários autores experientes na área para elaboração deste exemplar e isto levou em consideração a vivencia e expertise de cada um, não sendo, portanto, um modelo fechado ideal a ser seguido, mas tão somente visa ser uma ferramenta de auxílio aos que pretendem entender melhor como a implementação pode ocorrer.

BOA LEITURA!

Stella Muniz Campos Elias

1

VISÃO GERAL SOBRE À LEI GERAL DE PROTEÇÃO DE DADOS

1.1 ORIGEM, NORMAS E CONCEITOS PROVENIENTES DA LGPD

Melissa Barrioni e Oliveira[1]

Em um mundo cada vez mais dominado pela informação, presenciamos o aumento preocupante do uso inadequado de dados pessoais, envolvendo práticas como a comercialização ilícita e a utilização indevida destes para diversos fins.

Em 2013, um evento que marcou uma era ao expor a magnitude desse problema foi a revelação de casos de má conduta envolvendo gigantes da internet sediados nos Estados Unidos, incluindo empresas renomadas, como Google e Facebook, que desrespeitaram a privacidade de seus usuários. Como resposta a tais abusos, surgiram iniciativas focadas na defesa dos direitos dos indivíduos em relação à privacidade, juntamente com a criação de órgãos independentes de supervisão.

Nesse cenário, promulga-se a Lei Geral de Proteção de Dados Pessoais, ou LGPD, Lei Federal n.º 13.709, datada de 14 de agosto de 2018. Essa legislação procura regular o tratamento de dados pessoais, tanto por entidades públicas quanto privadas, alinhando-se com os princípios estabelecidos em diversas outras regulamentações internacionais sobre privacidade e o tratamento de dados em formato físico ou eletrônico.

A Lei Geral de Proteção de Dados (LGPD) surge como um marco significativo na legislação brasileira, estabelecendo diretrizes essenciais para o tratamento de dados pessoais e protegendo a privacidade dos cidadãos. A Lei é fruto de uma evolução necessária

1 Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora da Comissão Especial de Proteção de Dados do CFOAB. Professora e Coordenadora da Pós-graduação em de Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em Compliance e LGPD. Partner e Co-founder da BSS Consult. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pelo CAD (Centro de Atualização em Direito) e FUMEC/MG. Pós-Graduada em Docência com Ênfase em Educação Jurídica pela Universidade Arnaldo. Licenciatura em Letras pela Universidade São Judas.

para atender aos desafios contemporâneos relacionados à privacidade e à proteção de informações pessoais.

Para garantir de maneira efetiva a proteção de dados pessoais, é essencial que compreendamos, além do texto legal e sua origem, certos conceitos fundamentais. Estas definições incluem: "O que caracteriza um dado pessoal?", "Quais são as características de um dado sensível?", "O que engloba as operações de tratamento de dados pessoais?" e "Como se definem as figuras do titular dos dados pessoais, controlador, operador e encarregado?".

Neste primeiro capítulo, vamos explorar o surgimento, desenvolvimento e importância da LGPD, bem como os agentes envolvidos, a necessidade de uma Autoridade Nacional de Proteção de Dados, a recepção da lei pelas empresas e as oportunidades que se desenham para advogados, enquanto explicamos como este manual se torna um recurso fundamental para a compreensão e implementação da LGPD.

O SURGIMENTO DA PROTEÇÃO DE DADOS EM UM CONTEXTO MUNDIAL

Conforme a Comissão Especial encarregada da análise do Projeto da LGPD (CÂMARA FEDERAL, 2018), a influência primordial por trás da Lei remonta à experiência europeia no assunto. A jornada europeia na proteção de dados pessoais começa com a Convenção do Conselho da Europa n.º 108 de 1981, intitulada "Convenção para a Proteção dos Indivíduos em Relação ao Processamento Automatizado de Dados Pessoais". Na sequência, surge a Diretiva Europeia n.º 46 de 1995, também conhecida como Diretiva de Proteção de Dados. Em terceiro lugar, destaca-se a Diretiva n.º 58 de 2002, direcionada à salvaguarda da privacidade no contexto das comunicações eletrônicas.

O marco de 2016 presencia a revisão do sistema regulatório europeu com a aprovação do Regulamento Geral sobre a Proteção de Dados (RGPD), também denominado Regulamento n.º 679 ou "General

Data Protection Regulation (GDPR)". Este regulamento versa sobre a proteção dos direitos das pessoas físicas no que se refere ao tratamento de dados pessoais e à livre circulação desses dados. Por fim, em 25 de maio de 2018, o RGPD entra em vigor na União Europeia (UE), revogando a Diretiva n.º 46/95 e estabelecendo um padrão regulatório europeu unificado

Esse histórico conjunto de normativas europeias ressalta a consolidação da importância da privacidade nos países da União Europeia ao longo dos anos. É relevante notar, nesse contexto internacional, que o Regulamento europeu impõe restrições à transferência internacional de dados para nações que não garantam níveis adequados de proteção, comparáveis aos assegurados pela legislação europeia.

Além de reconhecer o valor dos dados pessoais para indivíduos e a sociedade, a Lei brasileira também foi desenvolvida considerando os interesses comerciais, especialmente no setor de Tecnologia da Informação e Comunicações (TIC). Em uma era em que a computação em nuvem desempenha um papel vital, um país em conformidade com a legislação europeia pode atrair operações de processamento de dados daquele continente, além de fortalecer seus laços comerciais. Esse interesse não se limita apenas à possibilidade de estabelecer centros de processamento de dados em solo nacional, mas também engloba o investimento internacional das próprias empresas de TIC. Assim, surgiu a necessidade de o Brasil adotar uma legislação que, sem renunciar a sua singularidade e soberania, harmonizasse seus padrões com o mundo e com os principais blocos econômicos, como a União Europeia.

A LGPD foi aprovada em 2018 e estava inicialmente programada para entrar em vigor em 14 de agosto de 2020. Vale ressaltar que, após inúmeras emendas e adiamentos, mesmo diante da proposta de postergação da Lei para maio de 2021 e a subsequente rejeição unânime pelo Congresso Brasileiro, a vigência da LGPD permaneceu inalterada. Por fim, após várias sugestões de modificação, em especial devido à pandemia da Covid-19, o Projeto de Lei (PL) n.º 1.179/2020

foi sancionado e transformado na Lei n.º 14.010/2020, que manteve a entrada em vigor da LGPD para setembro de 2020, com a condição de que as penalidades e sanções só começassem a ser aplicadas a partir de 1º de agosto de 2021.

A norma de proteção de dados estabelece um conjunto claro de regras e padrões para empresas que coletam e processam dados pessoais, garantindo direitos fundamentais aos titulares desses dados.

NECESSIDADE DE UMA LEI GERAL DE PROTEÇÃO DE DADOS

A era digital trouxe uma proliferação de informações pessoais, tornando crucial a proteção da privacidade. A regulamentação de Privacidade atende a essa necessidade ao estabelecer diretrizes sólidas para empresas e organizações, promovendo a confiança dos cidadãos no tratamento de seus dados pessoais.

A LGPD surgiu para suprir uma lacuna regulatória no Brasil. Ela foi criada para:

1. Proteger os direitos fundamentais à privacidade e à liberdade individual, garantindo que as informações pessoais sejam tratadas de forma adequada.

2. Promover a segurança jurídica e a transparência nas operações que envolvem dados pessoais.

3. Estabelecer regras claras e uniformes para o tratamento de dados, criando um ambiente de confiança para os cidadãos e as empresas.

APLICAÇÃO TERRITORIAL

No que se refere à abrangência territorial da Lei Geral de Proteção de Dados (LGPD), as diretrizes a respeito podem ser encontradas no seu art. 3°. Em resumo, a Lei estabelece que a localização física dos dados, o país de origem ou o país de armazenamento tornam-se irrelevantes, desde que pelo menos uma das três hipóteses:

> Art. 3º Esta Lei aplica-se 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, desde que: Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

Conforme a obra de MALDONADO et al. (2019), a primeira das hipóteses diz respeito à aplicação territorial tradicional, onde a legislação é aplicada tanto à entidade com sede no Brasil quanto às operações de tratamento realizadas em território nacional. Isso se refere a entidades de tratamento com presença física no País ou à execução de operações de tratamento em solo brasileiro, sujeitando-se, assim, à LGPD.

A terceira hipótese está relacionada à coleta de dados pessoais ocorrida no território nacional, e, em certa medida, pode ser vista como redundante em relação à primeira hipótese, uma vez que a coleta de dados é considerada uma operação de tratamento, como detalhado na seção 1.5 — Tratamento de Dados deste manual.

A segunda hipótese aborda a oferta, fornecimento de bens ou serviços, ou o tratamento de dados de indivíduos presentes em território nacional. É fundamental destacar que essas hipóteses não se acumulam. Portanto, a segunda hipótese estabelece a aplicação extraterritorial da legislação brasileira. Independentemente da localização da entidade de tratamento, ela estará sujeita à legislação

brasileira se estiver envolvida na oferta ou fornecimento de bens, ou serviços a indivíduos no território nacional ou se estiver tratando os dados desses indivíduos. Isso ocorre porque os negócios digitais têm o potencial de ser acessados de qualquer lugar no mundo (MALDONADO et al., 2019).

AGENTES DE TRATAMENTO

A lei identifica diversos agentes de tratamento, como controladores, operadores e encarregados de dados. Cada um possui responsabilidades específicas na proteção e tratamento adequado dos dados pessoais.

CONTROLADOR

Conforme disposto no artigo 5.º, inciso VI, da LGPD, o controlador é definido como uma entidade, seja ela pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relativas ao tratamento de dados pessoais.

Para elucidar, a Agência Nacional de Proteção de Dados (ANPD) (2021) oferece a seguinte definição de controlador:

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

OPERADOR

Segundo o artigo 5.º, inciso VII, da LGPD, o operador é definido como uma entidade, seja ela pessoa natural ou jurídica, de direito público ou privado, que efetua o tratamento de dados pessoais em nome do controlador.

Para uma compreensão mais detalhada sobre a identificação do operador, recomenda-se consultar o item 58 do Guia da ANPD (2021), que trata dos agentes de tratamento:

> Nesse cenário, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

ENCARREGADO

O encarregado, conforme previsto no artigo 5.º, inciso VIII, da LGPD, é a pessoa designada pelo controlador e pelo operador para atuar como um canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Conforme BLUM et al. (2020), o conceito de encarregado, em grande parte, é derivado do Regulamento Geral de Proteção de Dados (RGPD), conhecido como

"Data Protection Officer (DPO)". Diferentemente da legislação nacional, o DPO no RGPD possui uma função mais robusta na União Europeia, com uma seção inteira dedicada a essa questão. Segundo os autores, o DPO no RGPD pode ser entendido como o responsável por

monitorar a conformidade com as normas de proteção de dados e as políticas estabelecidas pelo controlador ou pelo operador, abrangendo a divisão de responsabilidades, conscientização e treinamento das partes envolvidas no tratamento de dados pessoais e a realização de auditorias correspondentes.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A criação da ANPD é um marco fundamental na área de proteção de dados. Essa autoridade é responsável pela supervisão e aplicação da lei, garantindo que as empresas cumpram suas obrigações e que os direitos dos titulares de dados sejam respeitados.

A ANPD é a autoridade que fiscaliza e aplica a lei, promovendo a conformidade e a cultura de proteção de dados no Brasil.

ADAPTAÇÃO DAS EMPRESAS ÀS NOVAS REGRAS DE PROTEÇÃO DE DADOS

Muitas empresas viram a LGPD como um desafio inicial, mas também como uma oportunidade de aprimorar suas práticas de proteção de dados, aumentando a confiança dos clientes e respeitando os padrões internacionais.

A nova regra desafiou as empresas a revisarem suas práticas de tratamento de dados. Muitas se depararam com a necessidade de ajustar suas operações para cumprir a lei.

Isso criou oportunidades para advogados e escritórios de advocacia, que passaram a oferecer serviços de consultoria jurídica especializada em proteção de dados.

PERSPECTIVAS PROFISSIONAIS PARA ADVOGADOS NO CONTEXTO DA LGPD

A nova Lei de Proteção de Dados revela novas oportunidade para advogados especializados nesta área em crescimento. Com a complexidade das regulamentações, as empresas buscam profissionais qualificados para auxiliar na adequação à LGPD, tornando essa área do direito altamente demandada.

A RELEVÂNCIA FUNDAMENTAL DO MANUAL DE PRÁTICA E IMPLEMENTAÇÃO

Este manual é um recurso indispensável para advogados que desejam compreender e implementar efetivamente a LGPD. Com a crescente demanda por expertise em proteção de dados, este guia oferece um roteiro prático e atualizado.

Ao longo deste livro, você encontrará instruções detalhadas, exemplos práticos e insights valiosos de especialistas em proteção de dados. É uma ferramenta essencial para a excelência profissional no contexto da Lei Geral de Proteção de Dados.

O manual é uma ferramenta indispensável para advogados que desejam atuar na adequação e implementação da LGPD. Com a crescente demanda por expertise em proteção de dados. Este Guia oferece um roteiro prático e atualizado, baseado em pesquisas extensas e nas melhores práticas do setor. Ele auxilia os profissionais a compreenderem a norma de privacidade, a guiarem seus clientes na jornada de conformidade e a se destacarem em um campo de atuação promissor.

Compreender o início da Regulamentação em Proteção de Dados e seu impacto é o primeiro passo em direção a uma prática jurídica bem-sucedida no mundo da proteção de dados. Concluímos, assim, o primeiro capítulo do livro, abordando o início da LGPD, sua importância e as oportunidades que se abrem para advogados.

Nos próximos capítulos, mergulharemos profundamente na metodologia e recursos necessários para uma eficaz adequação e implementação da LGPD em escritórios de advocacia.

Continue lendo este manual para obter orientações abrangentes sobre como atender aos requisitos da legislação e garantir que sua atuação como advogado seja eficaz e em conformidade com a lei.

2

ANTES DO PROJETO

2.1 QUESTIONÁRIO DE MATURIDADE

Alan de Souza Pinto[2]

A LGPD tem como objetivo proteger os dados pessoais de indivíduos e garantir a privacidade e a segurança dessas informações, impondo penalidades significativas em caso de não conformidade.

A adequação à LGPD requer uma série de ações por parte das empresas, incluindo a revisão dos seus processos e políticas de proteção de dados, a atualização de seus contratos e documentos jurídicos, o treinamento de seus colaboradores e a implementação de medidas de segurança adequadas para garantir a proteção de dados pessoais.

O questionário de maturidade é uma ferramenta útil para auxiliar as empresas a avaliar seu nível de conformidade com a LGPD e identificar áreas que precisam de melhorias. Nesse sentido, poderá ser uma lista de perguntas que abrangem todas as áreas importantes da LGPD e que permitem que a empresa avalie seu nível de conformidade em cada uma delas. Além disso, é uma ferramenta que pode ser usada para avaliar o grau de maturidade de uma organização em relação à adequação a uma norma, como a ISO 9001 ou a ISO 27001. Esse tipo de avaliação é importante porque permite que a organização identifique seus pontos fortes e fracos em relação à adequação à norma e estabeleça um plano de ação para melhorar seu grau de maturidade.

A diferença está na norma avaliada e nos níveis de maturidade propostos, que podem ser adaptados para outras normas ou contextos específicos.

As perguntas no questionário podem ser organizadas em áreas temáticas, como a gestão de dados pessoais, o consentimento do titular dos dados, as medidas de segurança, os processos de gestão de

2 Mestre em Inovação Tecnológica, pela UFMG, Bolsista CAPES; Pós-graduado em Direito Digital e Proteção de Dados, pela EBRADI; Pós-graduado em Direito Civil Aplicado, pela PUC Minas; Graduado em Direito, pela PUC Minas; Membro da Comissão de Proteção de Dados da OAB/MG; Consultor em Privacidade e Proteção de Dados Pessoais; Professor; Advogado.

incidentes e a privacidade por design. Cada área pode ter perguntas que avaliam o nível de maturidade da empresa em relação aos requisitos da LGPD. Por exemplo, na área de gestão de dados pessoais, as perguntas podem avaliar se a empresa tem um registro de todas as operações de processamento de dados, se implementou políticas de retenção de dados e se tem processos para responder a solicitações dos titulares de dados.

Ao responder às perguntas do questionário de maturidade, a empresa pode identificar as áreas em que precisa melhorar para estar em conformidade com a LGPD. Com base nessas informações, a empresa pode criar um plano de ação para implementar as mudanças necessárias e garantir que esteja em conformidade com a LGPD.

Além disso, o questionário de maturidade pode ser usado para demonstrar que a empresa está tomando medidas para se adequar à LGPD, o que pode ser útil em caso de investigações ou processos regulatórios. As respostas ao questionário poderão ser apresentadas como uma prova de conformidade da empresa com a LGPD e como uma evidência de que a empresa está tomando as medidas necessárias para proteger os dados pessoais de seus usuários.

Com isso, o questionário de maturidade é uma ferramenta importante para auxiliar as empresas a avaliarem seu nível de conformidade com a LGPD e identificar áreas que precisam de melhorias. Nesse sentido, pode ser usado como uma base para a criação de um plano de ação para implementar mudanças necessárias e garantir que a organização esteja em conformidade com a LGPD. Por fim, o questionário de maturidade também pode ser utilizado como prova de conformidade da empresa com a LGPD.

Para avaliar o nível de maturidade da empresa em relação à LGPD e identificar pontos de melhoria, desenvolvemos o questionário a seguir exposto. O questionário abrange diversos aspectos da adequação à LGPD, incluindo conhecimento, inventário de dados, consentimento, direitos dos titulares, segurança de dados, gerenciamento de incidentes e auditoria e revisão. Com base nas respostas ao questionário, as empresas podem obter uma visão geral

do seu processo de adequação à LGPD e desenvolver um plano de ação para melhorar a conformidade.

CONHECIMENTO
a) A empresa possui conhecimento suficiente sobre a LGPD e suas exigências?
b) A empresa designou um responsável pela adequação à LGPD?
c) A equipe responsável pelo processo de adequação recebeu treinamento adequado sobre a LGPD?
d) Além do conhecimento básico da LGPD, a equipe responsável pela adequação tem conhecimento específico sobre as atividades de processamento de dados da empresa?
e) A empresa forneceu aos funcionários de outras áreas da empresa informações suficientes sobre a LGPD e seu impacto nas suas atividades diárias?
f) A empresa criou um plano de treinamento contínuo para garantir que a equipe responsável esteja atualizada sobre mudanças na legislação e boas práticas?

INVENTÁRIO DE DADOS
a) A empresa identificou todos os dados pessoais que processa?
b) A empresa possui um inventário de dados preciso e atualizado?
c) Caso afirmativo, responder:
c.1) O inventário de dados inclui informações sobre a origem dos dados pessoais e sua localização?
c.2) A empresa estabeleceu um processo para verificar a precisão do inventário de dados regularmente?
c.3) O inventário de dados é acessível a todos os funcionários da empresa que precisam dele?
d) A empresa possui um processo claro para gerenciar o inventário de dados?

CONSENTIMENTO
a) A empresa possui processos para obter o consentimento dos titulares de dados?

b) A empresa possui um processo para gerenciar e documentar o consentimento dos titulares de dados?
c) A empresa coleta consentimento de forma clara e específica para cada finalidade de processamento de dados?
d) A empresa usa linguagem clara e simples para descrever as finalidades do processamento de dados aos titulares?
e) A empresa verifica regularmente se o consentimento dos titulares ainda é válido e atualizado?

DIREITOS DOS TITULARES
a) A empresa possui processos claros para atender aos direitos dos titulares de dados?
b) A empresa possui processos para responder a solicitações de titulares de dados em relação aos seus direitos?
c) A empresa possui processos para documentar ações realizadas em relação aos direitos dos titulares de dados?
d) A empresa tem um processo para lidar com solicitações de titulares de dados em relação aos seus direitos?
e) A empresa estabeleceu um prazo para responder a solicitações de titulares de dados em relação aos seus direitos?
f) A empresa implementou processos para verificar a identidade dos titulares de dados que fazem solicitações?

SEGURANÇA DE DADOS
a) A empresa possui processos claros para atender aos direitos dos titulares de dados?
b) A empresa possui processos para responder a solicitações de titulares de dados em relação aos seus direitos?
c) A empresa possui processos para documentar ações realizadas em relação aos direitos dos titulares de dados?
d) A empresa tem um processo para lidar com solicitações de titulares de dados em relação aos seus direitos?
e) A empresa estabeleceu um prazo para responder a solicitações de titulares de dados em relação aos seus direitos?

f) A empresa implementou processos para verificar a identidade dos titulares de dados que fazem solicitações?

GERENCIAMENTO DE INCIDENTES
a) A empresa possui um processo para gerenciamento de incidentes de segurança de dados?
b) A empresa possui um processo para reportar violações de segurança de dados às autoridades competentes?
c) A empresa possui um processo para notificar os titulares de dados afetados em caso de violação de segurança de dados?
d) A empresa estabeleceu um processo para lidar com violações de segurança de dados?
e) A empresa realizou um teste de simulação de violação de segurança de dados para avaliar a eficácia do seu processo de gerenciamento de incidentes?
f) A empresa tem um processo para notificar as autoridades competentes e os titulares de dados afetados em caso de violação de segurança de dados?

AUDITORIA E REVISÃO
a) A empresa realiza revisões regulares de seus processos de adequação à LGPD?
b) A empresa realiza auditorias internas regulares para avaliar a conformidade com a LGPD?
c) A empresa utiliza resultados de auditorias e revisões para melhorar seus processos de adequação à LGPD?
d) A empresa realiza revisões regulares de seus processos de adequação à LGPD para garantir que eles estejam atualizados?
e) A empresa estabeleceu um processo para avaliar o impacto de novas leis e regulamentos sobre a conformidade com a LGPD?

É importante ressaltar que a adequação à LGPD é um procedimento contínuo e que deve ser constantemente avaliado e aprimorado. Este questionário é uma ferramenta útil para avaliar o nível de maturidade da empresa em relação à LGPD e identificar pontos de melhoria. No entanto, vale lembrar que o processo de adequação requer uma abordagem interdisciplinar, envolvendo não apenas a equipe responsável pela adequação, mas toda a empresa. Nesse sentido, as empresas devem estar comprometidas com a proteção dos dados pessoais e estabelecer uma cultura de privacidade em toda a organização. Além disso, é fundamental monitorar as mudanças na legislação e manter as políticas e procedimentos atualizados para garantir a conformidade contínua com a LGPD.

2.2 PROPOSTA TÉCNICA E COMERCIAL

Alessandra C. Puig Casariego[3]

Primeiramente, é importante destacar que a apresentação de uma proposta de adequação e implementação da LGPD é capaz de agregar valor para o trabalho do advogado, pois transmite uma impressão de confiança ao alinhar expectativas entre os envolvidos, além de apresentar todas as fases do trabalho a ser contratado. Uma vez que o cliente possuirá acesso às informações acerca da solução desejada, sem dúvidas se sentirá mais seguro com o profissional que está buscando contratar.

A proposta deve ser entendida como uma carta de apresentação que formaliza um orçamento prévio. Uma proposta bem elaborada pode sim aumentar as chances de contratação.

A seguir apresentamos um passo a passo (a título de sugestão) de como elaborar uma proposta técnica/comercial de adequação e implementação da LGPD para a prestação de serviços de LGPD demonstrando a estrutura de tópicos sugerida:

- Indique o destinatário da Proposta.
- Apresente o seu escritório e os integrantes. Fale sobre a sua especialidade e área de atuação.
- Descreva de forma detalhada o serviço a ser feito, indicando inclusive as datas previstas para cada entrega. Neste ponto, é importante especificar o escopo do trabalho, se será uma

3 Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG. Membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas - FGV. Master of Business Administration - MBA em Advocacia Corporativa e Governança pela Escola Superior da Advocacia - ESA OAB. Pós-graduação em Direito Bancário pela Fundação Getúlio Vargas - FGV. Certificação em Compliance pela KPMG. Certificação em Investigações Corporativas pela KPGM. Curso de Extensão em Lei Geral de Proteção de Dados pela PUC-RS.

consultoria para algum ponto específico, para qual finalidade; se será um trabalho de implementação e adequação à LGPD.

- Informe o valor dos honorários advocatícios, que devem ser apresentados como um investimento. Exatamente, um investimento! Você deve transmitir a ideia de investimento para a melhor solução, defesa, entre outros. E, indique as formas de pagamento.
- Indique a existência de custas ou demais custos, ou ainda, o índice de correção do valor dos honorários advocatícios. Demonstre transparência!
- A proposta de honorários deve conter um prazo de validade. Não deixe de defini-lo e informá-lo na proposta.
- Inclua na proposta uma cláusula sobre privacidade e proteção de dados, dessa forma, seu possível cliente já saberá que seu escritório está seguindo todos os itens da LGPD entre outras normas.

É importante elaborar uma boa proposta de adequação e implementação da LGPD, pois será um diferencial que agregará valor ao seu trabalho e diminuirá barreiras durante a fase negocial.

2.3 CONTRATO DE PRESTAÇÃO DE SERVIÇO

Carlos Henrique Almeida Salgado[4]

O contrato de prestação de serviços é o instrumento jurídico que oficializa uma parceria entre um contratante e o contratado. É um documento que serve de garantia e segurança para todas as partes envolvidas na relação negocial e é regulado pela Lei 10.406/2002, o Código Civil Brasileiro.[5]

De acordo com artigo 594 do Código Civil,[6] o contrato de prestação de serviços é aplicável a qualquer atividade manual ou intelectual, desde que seja lícita.

A celebração do contrato é uma forma de assegurar que durante sua vigência da relação negocial, tanto contratado como contratante tenham suas obrigações e direitos assegurados pelas disposições que foram pactuadas neste instrumento jurídico.

De maneira geral, o contrato de prestação de serviços é importante para proteger o interesse das partes envolvidas.

Existem algumas informações básicas que devem constar em um contrato de prestação de serviços, tais como: identificação das partes envolvidas; descrição detalhada do serviço prestado; quais serão as obrigações contratuais de ambas as partes; o valor que será pago pela prestação dos serviços e as condições para pagamento; o prazo para cumprimento e a entrega dos serviços acordados; penalidades para o descumprimento das obrigações assumidas; possibilidade de rescisão antes do término do contrato e pagamento da multa respectiva, foro e assinatura das partes envolvidas.

---

4 Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP e Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

5 BRASIL. Lei nº 10.406, de 10 de janeiro de 2002

6 Art. 594. Toda a espécie de serviço ou trabalho lícito, material ou imaterial, pode ser contratada mediante retribuição.

Além das informações básicas descritas, a depender da natureza jurídica do contrato ou da especificidade da prestação dos serviços, o contrato de prestação de serviços deverá dispor de cláusulas específicas. Um exemplo de cláusula específica diz respeito à privacidade e à proteção dos dados pessoais que serão tratados no âmbito da relação contratual.

Nesse caso, o contrato deverá dispor sobre: I) a classificação de cada agente de tratamento na relação contratual; II) definições dos termos utilizados na LGPD; III) disposições gerais acerca da proteção de dados pessoais; IV) estrutura da segurança dos dados; V) conduta das partes diante de solicitações apresentadas pelos titulares; VI) responsabilidades relativas à privacidade e proteção de dados; VII) condutas que as partes devem adotar em caso de incidentes de segurança; VIII) procedimentos para encerramento dos tratamentos de dados e IX) Medidas de seguranças.

2.4 ACORDO DE CONFIDENCIALIDADE OU NDA

Elaine Cristina Oliveira Guerra[7]

O significado de *NDA*, ou o termo em inglês *Non Discloruse Agreement*, é em português "acordo de não divulgação ou acordo de confidencialidade". Este tem o condão de proteger, dentro do viés jurídico, as informações transitadas entre a empresa e o prestador de serviço ou entre aqueles que, de alguma forma, têm acesso aos dados pessoais ou informações sigilosas/confidenciais/segredos industriais/comerciais da organização.

Não existe na Lei Geral de Proteção de Dados (LGPD) nenhuma obrigatoriedade da utilização do *NDA*, todavia é uma prática usual de mercado que visa trazer maior conforto para as partes. O *NDAv* não é apenas para projetos relacionados à LGPD ou para grandes projetos da empresa. Ele pode e deve ser utilizado no dia a dia de todo negócio, como exemplo:

- Empresa x Empresa;
- Empresa e seus funcionários;
- Empresa e seus fornecedores;
- Empresa e seus investidores;
- Empresa e seus clientes;
- Empresa e seus franqueados;

7 Especialista em Direito, Inovação e tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados - ISFS), Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora do "Manual Prático de Adequação à LGPD com enfoque nas Relações do Trabalho". Autora de capítulos de livros jurídicos. Empresária em projetos de adequação e implementação da LGPD. Atuante com projetos de DPO as a Service. Mentora em projetos de adequação e implementação da LGPD. Palestrante em Privacidade e Proteção de dados. Diretora do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pesquisadora da USP/SP. Advogada.

- Em qualquer situação que necessite que informações sejam mantidas em sigilo.

Ainda sobre a prática de utilização do NDA, a norma ISO 27002:2022[8] trouxe um tópico específico acerca do acordo de confidencialidade e da não divulgação, a saber:

> Convém que acordos de confidencialidade ou não divulgação que refitam as necessidades da organização para a proteção das informações sejam identificados, documentados, analisados criticamente em intervalos regulares e assinados por pessoal e outras partes interessadas pertinentes.
> Para identificar os requisitos dos acordos de confidencialidade ou não divulgação, convém que sejam considerados os seguintes elementos:
> a) uma definição das informações a serem protegidas (por exemplo, informações confidenciais);
> b) a duração esperada de um acordo, incluindo casos em que a confidencialidade pode ser mantida indefinidamente ou até que as informações se tornam publicamente disponíveis;
> c) as ações necessárias quando um acordo é rescindido;
> d) as responsabilidades e ações dos signatários para evitar a divulgação de informações não autorizadas;
> e) a propriedade de informações, segredos comerciais e propriedade intelectual, e como isso se relaciona com a proteção de informações confidenciais;
> f) o uso permitido da informação confidencial e dos direitos do signatário para o uso da informação;
> g) o direito de auditar e monitorar atividades que envolvam informações confidenciais para circunstâncias altamente sensíveis;

8 ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO/IEC 27002:2022. Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da Informação.

> h) o processo de notificação e emissão de relatórios de divulgação não autorizada ou vazamento de informações confidenciais;
> i) os termos para que as informações sejam devolvidas ou destruídas no término do acordo;
> j) as ações esperadas a serem tomadas no caso de não conformidade com o acordo.

Ademais, é recomendável que o escritório de advocacia, ao ser contratado para atuar com projeto de adequação e implementação da LGPD, utilize *NDA* como uma ferramenta de *compliance* entre seu escritório e a empresa que o está contratando, visto que o escritório de advocacia terá acesso a informações privilegiadas da organização. Neste ponto, não se trata de acesso a dados de processo, mas de todas as áreas da empresa, como financeiro, faturamento, RH, marketing, compras, entre outras. Dessa forma, faz-se necessária a elaboração do *NDA* para resguardar e dar transparência do início ao fim do projeto de adequação e implementação da LGPD.

A seguir, será apresentado um passo a passo como sugestão do que deve constar no *NDA*:

- Qualificação da empresa e da outra parte;
- Objetivo/finalidade;
- O conceito de informações confidenciais e quais seriam elas,
- O que você vai proteger;
- Datas – nesse item, deve-se inserir datas de acesso à informação, validade e/ou prazo de confidencialidade;
- Quais penalidades serão aplicadas em caso de desconformidade;
- Legislação aplicável.
- Foro.

É bom ressaltar que o *NDA* protege as informações da empresa e deve informar aos signatários suas responsabilidades em proteger,

usar e divulgar informações de forma responsável e autorizada tais informações.

É importe salientar que, além do *NDA* ter um condão de resguardar a empresa na parte jurídica, faz-se necessário também aplicar toda e qualquer medida de segurança da informação (técnica) para resguardar os dados. Dessa forma, a empresa estará em *compliance* e resguardada de possíveis ataques internos ou externos.

Por fim, espera-se a percepção, ao longo deste texto que a utilização do *NDA* é fundamental para garantir a segurança de informações confidenciais e sigilosas no mundo corporativo.

3

O INÍCIO - PREPARAÇÃO

3.1 TERMO DE ABERTURA DE PROJETO (*TAP*)

Elaine Cristina Pereira dos Santos Nery[9]

Com a entrada em vigor da lei Geral de Proteção de dados (LGPD), as empresas iniciaram os projetos de adequação e implementação da LGPD.

A adequação e a implementação dos projetos de LGPD vem ocorrendo por meio de projetos desenvolvidos dentro da Organização e tem como premissa analisar toda a empresa, verificar os riscos e promover as soluções para as demandas encontradas.

O objetivo deste capítulo é trazer suporte para o desenvolvimento do projeto de adequação e implementação da LGPD escritórios de advocacia ou para o cliente. Para isso, algumas ferramentas de gestão de projetos devem ser aplicadas, como é o caso do Termo de Abertura de projeto (TAP).

O Termo de Abertura de Projeto (TAP) é um documento interno que registra /descreve formalmente o início de um projeto que será executado dentro de uma Organização. Esse documento é de extrema importância, pois será nele que a Organização descreverá de forma sucinta o que será executado em cada fase do projeto. Além disso, o TAP resguarda a empresa de eventuais discursões do que foi planejado e o que realmente é executado.

O guia O Guia PMBOK, 2017[10], traz o conceito:

> O termo de abertura do projeto é definido como o documento emitido pelo patrocinador do projeto que autoriza formalmente a sua existência e fornece ao gerente de projetos a autoridade para aplicar recursos

9 Advogada. Especialista em Direito Público. Especialista em Privacidade e Proteção de dados. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão de Proteção de Dados da OAB/MG e Membro da Comissão de Proteção de Dados da UFVJM.

10 Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, sexta edição, Pennsylvania: PMI, 2017.

> organizacionais nas atividades do projeto. O plano de gerenciamento do projeto é definido como o documento que descreve como ele será executado, monitorado e controlado.

O Termo de Abertura de Projeto (TAP) é a formalização da intencionalidade do projeto, melhor dizendo, dá vida aos objetivos, uma vez que autoriza oficialmente o início do projeto perante a instituição. Geralmente, esse TAP é elaborado pelo responsável financeiro da alta gestão, bem como pelo Gerente de projetos, pois ambos definirão qual a necessidade, os riscos, os investimentos, entre outros pontos relevantes para o projeto.

Conforme explanado, o objetivo não é descrever a metodologia, mas demostrar, de forma prática, o que deu certo e o que não pode dar errado. Dessa forma, alguns itens são de extrema importância serem descritos dentro de um TAP para resguardar o projeto como um todo, como as fases em que será desenvolvido sua execução, são elas:

- Identificação do projeto;
- Detalhamento do projeto;
- Equipe executora do projeto;
- Demanda;
- Justificativa;
- Objetivo;
- Benefícios;
- Escopo do projeto;
- Fora do escopo do projeto;
- Cronograma;
- Custo estimado;
- Riscos iniciais do projeto;
- Aprovação do projeto.

As premissas que subsidiaram a realização do projeto devem ser suficientes para garantir sua concretização. Para tanto, estabelecer

e definir os caminhos pelos quais ele será desenvolvido e quais as restrições serão consideradas devem estar previstas no TAP. Todas essas informações são inseridas para que o projeto percorra todas as fases e desenvolva o que se espera ao final do encerramento do projeto, devendo ter sido alcançado os resultados esperados, dentro do cronograma estabelecido.

O resultado desse processo autoriza formalmente a existência de um projeto, dá a direção e concede ao Gerente do Projeto a autoridade para aplicar os recursos organizacionais nas atividades do projeto.

Desse modo, espera-se alcançar maior credibilidade junto aos escritórios de advocacia e ao trabalho do advogado, além de potencializar a sua inserção e posicionamento no mercado, por meio da implementação e adequação à LGPD. Para o alcance dessa finalidade, faz-se necessário documentar todas as etapas dos processos, de modo que o resultado ideal de cada item esteja escrito, assegurando, assim, um parâmetro de qualidade para ele em sua totalidade.

3.2 PLANEJAMENTO DO PROJETO DE ADEQUAÇÃO E IMPLEMENTAÇÃO DA LGPD

Emily Matias Assumpção[11]

O projeto de adequação e implementação à LGPD é composto por fases, e, por vezes, acaba se tornando bastante complexo.

Vale dizer que, se não houver um planejamento adequado antes mesmo de se iniciar de fato o projeto, é possível que não seja entregue o que foi acordado com seu cliente, ora escritório de advocacia.

Quando se pensa em planejamento, logo se remete à gestão, visto que, sem gestão, o próprio caos se instaura no projeto.

Importante destacar que não é possível se falar em projeto de adequação e implementação à LGPD sem a participação da alta gestão e dos colaboradores. Trata-se de um trabalho conjunto, coordenado pelo DPO/Consultor, que ali exerce um papel de gestor, trazendo as diretrizes para todos os envolvidos na adequação.

Caminhando com o tema para a realidade dos escritórios de advocacia, é sabido que o número de processos é grande e os casos são complexos, logo, o tempo dos advogados é escasso. Por esse motivo, é de extrema importância planejar todo o projeto, para conseguir envolver os advogados, bem como os sócios, sem prejudicar seus trabalhos diários.

A palavra planejamento traz a ideia de programar, elaborar um plano, logo, com relação ao processo de adequação à LGPD não seria diferente. Laércio de Souza Silva, em seu artigo Soluções de tecnologia para gestão da governança em privacidade e a implementação da LGPD, diz o seguinte:

11 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

> Conforme se verifica do texto da norma, o programa de governança em privacidade não é um destino, e sim uma jornada sem fim, pois requer atualizações constantes, monitoramento contínuo, avaliações sistemáticas de impactos e riscos à privacidade, de modo que, dependendo do volume de operações, esses requerimentos, poderão ser atendidos por meio de plataformas de gestão em privacidade ou por um conjunto de soluções de tecnologias que enderece todos os temas trazidos pela norma.[12]

Desse modo, diante da complexidade das ações, bem como das necessidades acima citadas, é necessário ter um planejamento adequado do projeto de adequação à LGPD.

Importante mencionar que não existe uma metodologia de gestão e planejamento específica para a LGPD no texto da Lei, mas atualmente o mercado desenvolve e oferece metodologias ágeis, com resultados efetivos, capazes de demonstrar evidências e facilitar o processo de adequação.

A metodologia Scrum, no artigo O que é metodologia Scrum? se explica como:

> Scrum é uma metodologia de desenvolvimento ágil utilizada no desenvolvimento de Software baseada em um processo iterativo e incremental. Scrum é um framework ágil, adaptável, rápido, flexível e eficaz que é projetado para oferecer valor ao cliente durante todo o desenvolvimento do projeto.
>
> O principal objetivo do Scrum é satisfazer a necessidade do cliente através de um ambiente de transparência na comunicação, responsabilidade coletiva e progresso contínuo. O desenvolvimento parte de uma ideia geral do que precisa ser construído, elaborando uma lista de características ordenadas por

12 SILVA, Laércio de Souza et al. Proteção de Dados desafios e soluções na adequação à Lei. Ed. 2ª, Editora Forense. 2021.

> prioridade (backlog do produto) que o proprietário do produto deseja obter.[13]

Observa-se que as grandes características da metodologia *Scrum* são: a agilidade, interatividade, transparência e possibilidade de entregas que não "travem o processo".

Entre os principais objetivos do *Scrum*, tem-se a facilidade em trabalhar com projetos complexos, nesse sentido, adapta-se ao cerne do presente manual, a adequação de uma Lei (LGPD), extremamente complexa em escritórios de advocacia.

O consultor, ou DPO, que fará a adequação, quando se utiliza da metodologia *Scrum*, exerce o papel de líder de projeto, e, a partir desse ponto, direciona a alta direção e demais colaboradores sobre quais os caminhos deverão ser tomados.

O processo se inicia com a visão inicial do produto e seu planejamento, no caso a adequação e implementação da LGPD, também são definidos as prioridades e ciclos, os chamados *Sprints,* com tempo de duração.

Registra-se que, na metodologia *Scrum,* existe uma grande interação com a equipe para definir: tarefas, prioridades, finalidades, prazos e pôr fim à entrega. São realizadas reuniões diárias, que são essenciais para entender sobre o desenvolvimento do projeto.

Portanto, uma vez que seja utilizada a metodologia *Scrum* no projeto de adequação e implementação à LGPD, o consultor/DPO deverá criar o Comitê de Proteção de Dados (equipe), explicar as fases do projeto (*Product Backlog*), estruturar os prazos de entrega dos documentos e processos (*Sprint)* e sempre se valer das reuniões (*Daily Meet*), com o objetivo de sanar dúvidas, auxiliar o Comitê, manter a transparência e agilidade do processo.

Vale dizer que a metodologia *Scrum* é apenas uma das muitas metodologias ágeis e contribui significativamente para a gestão de projetos.

13 O que é metodologia Scrum? disponível em (https://www.digite.com/pt-br/agile/metodologia-scrum/) acesso em 24/02/23.

Nas palavras de Letícia de Souza Martins, em seu artigo, Scrum framework e sua usabilidade com a ferramenta de princípios ágeis, Trello.

> É necessária mudança de cultura na equipe, onde todos os membros estejam sempre focando em conhecimento sobre variados assuntos na área afim de nivelar novos conhecimentos. Scrum pode-se levar para qualquer área, sendo ela de software, vida pessoal, atividade doméstica, planejamento de festas e entre outros projetos. É possível levá-la a qualquer área e ter a mesma garantia do seu resultado com qualidade e eficiência. [14]

Outro modelo de gestão de projetos muito utilizado é o *Project Management Body of Knowledge,* também conhecido como *PMBOK*, que diferente do *Scrum*, não se trata de uma metodologia, mas de uma padronização que identifica e conceitua processos, áreas de conhecimento, ferramentas e técnicas.

O PMBOK foi desenvolvido pelo *Project Management Institute (PMI)* e tem o objetivo de determinar o início, meio e fim das atividades do projeto.

O Project Builder, em seu artigo sobre o PMBOK, conceitua-o da seguinte forma:

> Para o PMBOK, o gerenciamento de um projeto é a aplicação de habilidades, conhecimentos, ferramentas e técnicas nas atividades da iniciativa com o objetivo de satisfazer seus requisitos.
> Ele pode ser mais bem compreendido por meio dos processos que o compõem, organizados em cinco grupos:

14 MARTINS, Letícia de Souza. Scrum framework e sua usabilidade com a ferramenta de princípios ágeis, Trello. Disponível em (https://m.uniara.com.br/arquivos/file/cca/artigos/2016/leticia-souza-martins.pdf) acesso em 25/02/23.

- Iniciação;
- Planejamento;
- Execução;
- Monitoramento e controle;
- Encerramento.[15]

O PMBOK ganhou tanta relevância no gerenciamento de projetos, que foi reconhecido pelo *American National Standards Institute (ANSI)* e desde então vem sendo revisado e atualizado ao longo dos anos, estando em sua 7ª Edição.[16]

Fato é que se trata de uma gestão de processos bastante robusta e que por certo auxilia no processo de adequação e implementação da LGPD, pois garante o controle do escopo, produtividade, possibilita ao consultor/DPO o acompanhamento das tarefas do Comitê de Proteção de Dados gerenciando melhor o tempo para a entrega efetiva.

Para tanto, José Bezerra da Silva Filho, em seu artigo O Gerenciamento de Projetos tem um Novo Direcionamento com o Guia PMBOK® – 7ª Edição (2021), expõe que:

> Para garantir os resultados pretendidos da entrega do projeto, os membros da equipe do projeto devem seguir esses princípios.
> A seguir estão os 12 princípios (PMI®):
> 1) Administração: foco na administração do projeto.
> 2) Equipe: construa uma cultura de responsabilidade e respeito.
> 3) Stakeholders: envolver as partes interessadas para entender seus interesses e necessidades.
> 4) Valor: foco em garantir mais entrega de valor ao seu cliente.

15 Project Builder, PMPOK. Disponível em (https://www.projectbuilder.com.br/blog/o-que-e-pmbok/) acesso em 25/02/23.

16 FILHO, José Bezerra da Silva. O Gerenciamento de Projetos tem um Novo Direcionamento com o Guia PMBOK® – 7ª Edição. 2021. Disponível em (https://www.linkedin.com/pulse/um-primeiro-olhar-sobre-o-novo-guia-pmbok-7%C2%AA-edi%C3%A7%C3%A3o-jos%C3%A9/?originalSubdomain=pt) acesso em 25/02/23.

5) Pensamento holístico: reconheça e responda às interações dos sistemas, procurar compreender os fenômenos na sua totalidade.
6) Liderança: motivar, influenciar, treinar e aprender.
7) Adaptação: adaptar a abordagem de entrega com base no contexto.
8) Qualidade: construir qualidade em processos e resultados.
9) Complexidade: lidar com a complexidade usando conhecimento, experiência e aprendizado.
10) Oportunidades e ameaças: abordar oportunidades e ameaças.
11) Adaptabilidade e resiliência: ser adaptável - que se adapta com facilidade e é resiliente - ter capacidade de se adaptar às intempéries, às alterações ou aos infortúnios.
12) Gestão das mudanças: habilitar a mudança para alcançar o estado futuro previsto.

Portanto, o PMBOK garante uma gestão de projetos voltadas para o desenvolvimento de equipes, a execução com qualidade dos projetos, proporcionando monitoramento e controle destes.

Logo, conclui-se, no presente capítulo, que, para gerir um projeto de adequação e implementação à LGPD, não se trata de uma "receita de bolo" e possui metodologias e padronizações diferentes.

Além das citadas acima, o consultor/DPO pode se valer da metodologia que melhor atendê-lo, prezando sempre pela organização, dinamismo, comunicação, transparência para a execução de um projeto de adequação e implementação à LGPD responsável e dotado das evidências e documentos exigidos no normativo legal.

3.3 METODOLOGIA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Gabriel Campos Cunha[17]

Existem alguns modelos metodológicos para implementação de governança de privacidade e proteção de dados pessoais disponíveis no mercado (Como algumas normas da série 27000 da ISO, *COBIT Framework, DPIA - Data Protection Impact Assessmente*), mas é importante ressaltar que a aderência ou forma de aplicação de tais modelos pode variar, pois cada organização tem suas próprias particularidades e desafios.

O processo de adequação à Lei Geral de proteção de Dados - LGPD pode se dar de uma forma completa, quando todas as áreas da organização se mobilizam para realizar as atividades inerentes ou, de forma pontual, quando determinada área ou produto nasce ou é revisado, preocupando-se em estar aderente às diretrizes de privacidade e proteção de dados vigentes.

Destacaremos aqui uma metodologia que, de forma prática, tem grande aplicabilidade para as organizações na condução da sua adequação à LGPD. De forma geral e resumida, a implementação dessa metodologia se dá em 6 fases:

17 Advogado, consultor em Governança Corporativa, ESG, Compliance, Integridade, Proteção de Dados. Auditor de Sistemas De Gestão da Qualidade, Meio Ambiente, Saúde e Segurança do Trabalho. Auditor da Conformidade Legal nos temas de Proteção de Dados, Privacidade, Meio Ambiente e Saúde e Segurança do Trabalho.

Tabela 1 - Fases para adequação à LGPD e seus objetivos

Fase 1 Preparação	Fase 2 Mapeamentos	Fase 3 Análise de Lacunas e Riscos	Fase 4 Planejamento	Fase 5 Execução	Fase 6 Governança
Nivelamento interno quanto aos objetivos do projeto e informações sobre Privacidade, proteção de Dados e normas correlatas; Levantamento dos Processos setoriais; Mobilização da Liderança; Definição do grupo de trabalho	Análise detalhada dos Processos Organizacionais Apuração dos dados pessoais que fluem em cada processo, de forma organizada Estruturação de um mapa que permita identificar informações chave referentes aos dados pessoais levantados Registros de desvios, oportunidades de melhoria e boas práticas	Análise das lacunas existentes no tratamento de dados pessoais em cada processo quanto à promoção da privacidade e proteção dos dados; Identificar os riscos inerentes às lacunas identificadas Identificação de ações necessárias para preenchimento das lacunas identificadas	Elaboração de Plano de ação para endereçar o preenchimento das lacunas; Definição dos responsáveis pela execução	Desenvolver e implementar políticas, procedimentos e controles para Proteção de Dados e Privacidade – Governança de Dados Pessoais Projetar, Desenvolver e implementar políticas, procedimentos e controles para cumprir a Legislação de Privacidade e requisitos da Organização.	Consolidação da sistemática de execução da governança sobre dados pessoais; Acompanhamento da realização das ações determinadas; Avaliação de eficácia das ações; Avaliação contínua do respeito à privacidade e proteção de dados pessoais;

Fonte: Do Autor

As fases de adequação devem ser compostas por atividades e etapas que estejam de acordo com o porte da organização e o volume e complexidade do tratamento de dados pessoais na operação. Fazer esse ajuste permite que a empresa enfrente passo a passo, de acordo com suas reais necessidades e demandas, os pontos fundamentais

para sua adequação às diretrizes da LGPD e, portanto, aos direitos fundamentais da privacidade e proteção de dados pessoais. Abaixo algumas etapas importantes para as fases propostas:

Tabela 2 - Etapas importantes para cada etapa da metodologia de adequação à LGPD

Fase 1 Preparação	Fase 2 Mapeamentos	Fase 3 Análise de Lacunas e Riscos	Fase 4 Planejamento	Fase 5 Execução	Fase 6 Governança
Coletar leis e regulamentos de privacidade Estabelecer grupo de trabalho para o projeto; Estabelecer fluxos de dados e inventário de dados pessoais; Fazer nivelamento quanto ao tema junto aos líderes e membros do grupo de trabalho	Elaborar ou revisar o organograma da organização; Realizar o levantamento dos processos área a área; Realizar o levantamento de dados pessoais em fluxo nos processos organizacionais;	Análise das lacunas existentes no tratamento de dados pessoais em cada processo quanto à promoção da privacidade e proteção dos dados; Identificar os riscos inerentes às lacunas identificadas; Analisar o impacto da privacidade; Identificação de ações necessárias para preenchimento das lacunas identificadas; Analisar o impacto da privacidade;	Elaboração de Estratégias e Plano de ação para endereçar o preenchimento das lacunas, mitigação e eliminação dos riscos; Definição dos responsáveis pela execução; Estabelecer programa de Privacidade e Proteção de Dados Pessoais;	Desenvolver e implementar estratégias, planos e políticas de Proteção de Dados e Privacidade; Executar as ações planejadas no âmbito do Programa de Privacidade e Proteção de Dados Pessoais Executar o plano de treinamento de Proteção de Dados e Privacidade.	Consolidação da sistemática de execução da governança sobre dados pessoais; Acompanhamento da realização das ações determinadas; Avaliação de eficácia das ações; Avaliação contínua do respeito à privacidade e proteção de dados pessoais;

	Realizar o levantamento dos ativos organizacionais nos quais são armazenados dados pessoais e as respectivas medidas de proteção e segurança em tais ativos;	Definir e manter a matriz de atribuições e responsabilidades pela Proteção de Dados e Privacidade - Matriz RACI.;	Desenvolver e implementar um sistema de transferência internacional de dados. Planejar a continuidade do compromisso de todos os níveis hierárquicos da organização com a Proteção de Dados e Privacidade; Elaborar plano de comunicação corporativa regular para direcionamentos, questões e problemas de Proteção de Dados e Privacidade.; Planejar processos e procedimentos que garantam o envolvimento das partes interessadas em questões de Proteção de Dados e Privacidade	(SE FOR O CASO) Implementar ou melhorar os controles de Segurança de Dados Pessoais.	Registro, Manutenção, Controle, Avaliação Crítica quanto as demandas e atendimento dos titulares de dados pessoais.

Fonte: Do Autor

As etapas e atividades realizadas em cada fase têm, geralmente, entregáveis desejáveis para que a engrenagem da metodologia evolua de forma consistente. Tais entregáveis registram, ainda, o compromisso da organização no seu processo de adequação às diretrizes da LGPD e dos direitos constitucionais à privacidade e proteção de dados pessoais. Ou seja, além do seu valor intrínseco (de levar a organização a tratar direitos fundamentais de titulares de dados pessoais, suas partes interessadas, de forma adequada), os entregáveis, enquanto registros, têm a capacidade de mostrar que a organização busca e/ou está em conformidade.

Abaixo, lista-se alguns entregáveis desejáveis para cada fase da metodologia apresentada.

Tabela 3 - Entregáveis mínimos desejáveis para cada etapa do método de adequação à LGPD.

Fase 1 Preparação	Fase 2 Mapeamentos	Fase 3 Análise de Lacunas e Riscos	Fase 4 Planejamento	Fase 5 Execução	Fase 6 Governança
Manual de Leis de Privacidade Programa de Proteção de Dados & Privacidade Orçamento da estruturação da Gestão de Proteção de Dados Nomeação do Encarregado de Proteção de Dados Pessoais Contratação de sistema informatizado para gestão do projeto e governança quanto à proteção de dados pessoais e privacidade (caso tenha sido definida)	Organograma da organização elaborado ou revisado Mapa de processos área a área; Inventário de Dados Pessoais Mapa do ciclo de vida dos dados pessoais em fluxo nos processos organizacionais; Relatório dos ativos organizacionais nos quais são armazenados dados pessoais e as respectivas medidas de proteção e segurança em tais ativos;	Identificação das bases legais para tratamento dos dados pessoais Relatório de Análises de Proteção de Dados e Privacidade Apontamento de Lacunas por processos; Identificação de riscos por processo	Estratégia de Proteção de Dados e Privacidade Programa de Proteção de Dados e Privacidade (Planos de Implementação de Ações de Proteção de Dados e Privacidade) Plano atualizado de conscientização, comunicação e treinamento em privacidade Plano de tratamento de solicitações, reclamações e retificação Plano de Gerenciamento de Riscos de Terceiros Plano de Resposta à Violação de Privacidade de Dados	Elaboração e Implementação da Política de Proteção de Dados e Privacidade; Função de Proteção de Dados e Privacidade incluída nas descrições de cargos; Elaboração e implementação Sistema de Classificação de Dados Pessoais; Elaboração e implementação de Procedimento de aprovação do	Registro do Monitoramento contínuo seus processos e sistemas de tratamento de dados pessoais; Sistema informatizado de Proteção de Dados e Privacidade (se for o caso); Relatório de Proteção de Dados & Privacidade; Relatórios de Auditoria de Dados Pessoais; Reuniões periódicas do comitê;

			Processamento dos Dados Pessoais; Desenvolvimento e implementação de um Sistema de transferência internacional de Dados (se for o caso); Execução das atividades de treinamento corporativo de Proteção de Dados e Privacidade; Implementação de Controles de Segurança de Dados Pessoais; Elaboração e implementação de Avisos de Privacidade de Dados; Execução de Plano de Resposta à Violação de Privacidade de Dados; Elaboração e implementação da Política de retenção de Dados Pessoais; Elaboração e implementação de termos de consentimento; Elaboração implementação de Cláusulas e aditivos contratuais (fornecedores, clientes e colaboradores); Adequação das plataformas digitais da organização.		

Fonte: Do Autor

Cabe ressaltar que todo o processo é relevante para o aprendizado organizacional. O grupo de trabalho, ou comitê responsável pelo projeto, assim como o Encarregado de Proteção de Dados Pessoais, deve ter o cuidado de documentar toda a trajetória das atividades, pois são ativos importantes da inteligência da organização.

A 6ª fase, de Governança, também é uma fase de aprendizado, o que é fundamental para melhoria contínua. Desde a revisão de processos para apurar sua adequação à LGPD até a elaboração/adoção de procedimentos ou ferramentas novas, podem (devem) ser adotadas nesta fase, como forma de aprimoramento da gestão de dados e privacidade.

3.4 FORMALIZAÇÃO DA COMISSÃO OU COMITÊ DE PROTEÇÃO DE DADOS

Isabela Cristina Maia da Cruz[18]

O Comitê Gestor de Proteção de Dados Pessoais - CGPDP tem por finalidade auxiliar no cumprimento da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

Ao iniciar um programa de adequação e implementação da Lei Geral de Proteção de Dados deve-se ter em mente a importância da criação e constituição de um Comitê/comissão de proteção de dados.

O comitê será responsável pela criação do regimento interno da organização, que nada mais é do que um documento no qual serão abarcados um composto de regras para o bom funcionamento cotidiano daquela entidade.

A criação do CGPDP se dará por meio da formação de uma equipe multidisciplinar, composta por colaboradores da organização, que acumularão as suas atividades cotidianas àquelas do Comitê. O CGPDP ficará vinculado ao Diretor Presidente, que desempenha o papel de controlador de dados, nos termos da LGPD (Lei n. 13.709/2018).

Após sua formação, o Comitê ficará responsável pela avaliação dos mecanismos de tratamento e proteção dos dados existentes, bem como pela proposição de ações voltadas ao seu aperfeiçoamento.

Atualmente, não existe na LGPD nenhum artigo específico obrigando as empresas a constituírem uma comissão/comitê de proteção de dados, todavia, a LGPD trouxe de forma clara e objetiva algumas recomendações em seu artigo 50 para que os Controladores e Operadores de dados pessoais possam adotar nas Organizações em seu dia a dia:

18 Advogada, Especialista em Direito Digital e Compliance. Membro da Comissão de Proteção de Dados da OAB/MG. Presidente da Comissão de Proteção de Dados Subseção Vespasiano da OAB/MG.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.[19]

As recomendações de boas práticas trazidas no mencionado artigo fazem com que as empresas amadureçam em termos de conformidade (Compliance), ou seja, que elas individualmente, ou por meio de associações, formulem regras de boas práticas e governança que se apliquem ao ramo da atividade.

Leme e Blank (2020 p.218) 3 aduz que "as regras devem ser implementadas e integradas no processo de tratamento de dados e governança da empresa".

Trazendo para a prática, antes de criar o comitê/comissão, as empresas devem atentar-se para o seu tamanho e suas condições financeiras, analisar quais são as áreas existentes e quais são os pontos focais de cada área. Após esta primeira análise, faz-se necessário treinar todos os pontos focais em termos de privacidade e proteção de dados. Além do mais, é importante que o comitê/comissão entenda o seu real papel e o quanto poderá contribuir para uma mudança de cultura em sua totalidade.

Trazer profissionais que conheçam do processo da empresa para a comissão/comitê é fundamental. Todavia, a empresa deve se resguardar registrar/documentar a constituição desse comitê/

19 BRASIL., LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, acesso em 16/02/2023

comissão. Além do mais, é importante que todos os membros que vão compor o comitê/comissão assinem o termo de confidencialidade (NDA), tendo em vista que os membros terão acesso a informações privilegiadas e muitas vezes confidenciais da empresa.

Em termos de documentação, é extremamente importante a elaboração de ata de todas as reuniões deliberadas pelo comitê/comissão, para que, assim, nenhum processo venha a se perder.

Não menos importante, faz-se necessário treinar o comitê/comissão, não só no início da constituição, mas durante todo o processo de adequação e implementação da LGPD. A empresa não deve parar por aqui, ela deve, sempre, capacitar suas equipes, para que essas possam disseminar a cultura de privacidade e proteção de dados por toda a organização.

3.5 REGIMENTO INTERNO DO COMITÊ DE PROTEÇÃO DE DADOS / COMITÊ GESTOR DA LGPD

Izabela Nunes Pinto[20]

O principal objetivo do regimento será esclarecer com detalhes quais são as normas que ditam as dinâmicas e as relações de trabalho, notadamente no que diz respeito aos direitos e deveres dos colaboradores.

Após a criação do Comitê, o regimento interno deverá ser disponibilizado a todos os colaboradores daquela entidade, seja via digital ou física.

A acessibilidade do documento é fundamental para que os gestores tenham uma gerência maior da dinâmica do funcionamento da empresa, contribuindo, desse modo, para maior agilidade na tomada de decisões, sem prejuízo da previsibilidade e da segurança da administração da pessoa jurídica.

Importa mencionar que, a elaboração do regimento interno não é obrigatória para a criação de uma pessoa jurídica. No entanto, sua constituição poderá trazer benefícios imensuráveis, além de agregar valor para a empresa, sendo crucial para a consolidação da estrutura interna da organização, já que esta ficará mais organizada e, via de consequência, tornar-se-á mais confiável à vista de clientes e investidores.

Ao se elaborar o regimento interno, deve-se atentar às peculiaridades da organização, além de ser de suma importância que este esteja em consonância com a legislação trabalhista (CLT - Decreto-Lei nº 5.452, de 1º de maio de 1943), e com toda a legislação vigente, de modo que as vontades do empregador não podem se sobrepor aos

20 Advogada. Membro nomeado da Comissão de Proteção de Dados da OAB/MG. Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Curso de Direito para Startups na Europa (envolvendo GDPR, LGPD e outros temas relacionados ao Direito Digital) pela Academy da Platzi. Finalista, ocupando o 3º Lugar Geral do Brasil da 1a Edição do LawCamp - 1a Competição de Implementação da LGPD no Brasil. Palestrante (Adequação/Implementação da LGPD e Direito Digital).9

direitos e garantias trabalhistas, caso contrário suas cláusulas poderão ser consideradas nulas ou, até mesmo, suscitar processos judiciais, o que ocasionará ampla instabilidade à organização.

Além disso, o corpo do regimento interno deverá conter algumas determinações acerca das condutas e diretrizes praticados pela organização (ex.: valores, visão e missão) e que deverão ser observados e praticados por todos os colaboradores, permitindo, desse modo, maior transparência, engajamento e eficácia nas relações internas. E mais, deverá estabelecer, ainda, a hierarquia entre os diferentes cargos ocupados na empresa, melhorando o fluxo de trabalho em equipe.

Para elaboração do regimento interno, é essencial que as ações do CGPDP sejam amparadas por um grupo de trabalho técnico, devendo este demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

O programa (regimento interno) a ser desenvolvido pelo CGPDP deverá se orientar pelo que preconiza o disposto na seção II da LGPD, art. 50, § 2º, inciso I, que estabelece a necessidade de "implementar programa de governança em privacidade", visando à aplicação dos princípios da Segurança e Prevenção elencados no art. 6º da Lei, devendo, portanto:

- Ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- Ser adaptado à estrutura, à escala e ao volume das operações da entidade, bem como à sensibilidade dos dados tratados;
- Estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

- Estar integrado à estrutura geral de governança, estabelecendo e aplicando mecanismos de supervisão internos e externos;
- Contar com planos de resposta a incidentes e remediação; e
- Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Ademais, importante se atentar para algumas atribuições incumbidas ao Comitê de Proteção de Dados (CGPDP) para criação do regimento interno, tais como:

- Avaliar ou propor políticas e procedimentos de tratamento de dados pessoais;
- Revisar a Política de Proteção de Dados e a Política de Privacidade da entidade a cada 02 (dois) anos (tempo estipulado a título exemplificativo)
- Reunir-se na periodicidade prevista no Regimento;
- Tratar casos omissos ou de exceção em políticas ou procedimentos.

Nesse mesmo sentido, também são algumas funções e responsabilidades dos agentes ligados ao Comitê:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da Autoridade Nacional e adotar providências, com o devido compartilhamento das informações com o Comitê;
- Orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pela entidade, na função de controladora, ou estabelecidas em normas complementares.

Diante dos apontamentos feitos acima, resta claro que a criação de uma 'Comissão" e, por consequência, do regimento interno, tem por finalidade formular diretrizes, propor ações e monitorar medidas destinadas à implementação de boas práticas relacionadas à proteção de dados pessoais, de modo a assegurar um processo de adequação à LGPD de forma padronizada, permanente e sistêmica nas atividades, ações e projetos das organizações.

A constituição de um regimento interno, pode evitar incontáveis problemas para a organização, no entanto, é necessário destacar que sua elaboração deverá ser realizada com o máximo de critério e responsabilidade dos envolvidos, vez que uma má redação do documento poderá gerar falta de entendimento dos colaboradores e acarretar mais problemas do que soluções.

Assim, diante de todo o exposto, conclui-se que, apesar de não ser um documento de cunho obrigatório, o regimento interno é de suma importância na constituição e regulamentação de entidades, sendo um diferencial no momento da contratação da empresa por um cliente ou, ainda, na decisão de um investidor.

3.6 FORMALIZAÇÃO DO ENCARREGADO DE PROTEÇÃO DE DADOS

Renato Almeida Viana[21]

A Agência Nacional de Proteção de Dados ("ANPD") publicou, no dia 26/04/2022, a versão atualizada do "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado"[22], com o objetivo de trazer maior segurança aos titulares de dados, agentes de tratamento e encarregados, sanando algumas das principais dúvidas que têm sido apresentadas à ANPD quanto aos papéis dos agentes de tratamento (controlador e operador) e do encarregado.

Nesse contexto, é importante abordar os conceitos desses principais atores trazidos pela LGPD.

O Guia esclarece que a principal diferença entre o controlador e o operador é o poder de decisão, sendo que este só pode agir no limite das finalidades determinadas por aquele. Em outras palavras, o operador é quem realiza o tratamento de dados pessoais em nome do controlador.

O art. 39 da LGPD estabelece que "o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria".

Dispõe o art. 5º, inciso VI, da LGPD, que o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. O inciso VII do mesmo artigo conceitua operador como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados

21 Coordenador do Comitê de LGPD do Centro de Estudos das Sociedades de Advogados de Minas Gerais – CESA/MG. Membro do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Escola Superior da Advocacia. Advogado.

22 Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF. Abril 2022 Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 05/01/2023.

pessoais em nome do controlador (Brasil, 2018)[23]. Nesse sentido, para Rony Vainzof[24]:

> "O conceito de controlador contempla absolutamente todas as decisões sobre as atividades que refletem o ciclo de vida dos dados pessoais. Desde o projeto, passando pela coleta ou recepção, todas as formas de processamento, até o descarte.
> (...)
> Portanto, as decisões sobre quais espécies de dados serão tratados, para quais propósitos, com quem serão compartilhados, por quanto tempo eles serão mantidos, quais são os requisitos de segurança necessários, por exemplo, são de competência do controlador."

São algumas obrigações do operador: (i) seguir as instruções do controlador, (ii) firmar contratos que estabeleçam, entre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com o suboperador.

Tanto o controlador quanto o operador são considerados agentes de tratamento, de acordo com o art. 5º, inciso IX, da LGPD.[25]

Os escritórios de advocacia, na maioria das vezes, desempenham esses dois papéis: o de controlador, quando está tratando dados de seus

23 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 5º, inciso VII. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jan. 2023.

24 LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2022. Viviane Nóbrega Maldonado, Renato Opice Blum Editor: Revista dos Tribunais LEI 13.709, DE 14 DE AGOSTO DE 2018 CAPÍTULO I. DISPOSIÇÕES PRELIMINARES Art. 5º. Página RL-1.2 https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.2

25 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 5º, inciso IX. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jan. 2023.

colaboradores, associados e parceiros; e de operador, quando executa o tratamento de dados de acordo com as orientações de seus clientes.[26]

A LGPD ainda traz no seu art. 5º, inciso VII[27], a figura do encarregado, que apesar de não ser considerado pelo referido diploma como um agente de tratamento, é responsável por atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> VIII - encarregado: 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);

A ANPD esclarece que o encarregado é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD, destacando que, no exercício de suas atribuições, o encarregado pode desempenhar um importante papel de fomentar e disseminar a cultura da proteção de dados pessoais na organização.

Diferentemente de outras legislações de proteção de dados estrangeiras, a LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado, sendo que o art. 41 da Lei dispõe que:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

26 TAFAILE, Cinthia. LGPD e os escritórios de advocacia: muito além de um novo nicho de mercado. Nextlaw academy. Data de publicação: 04/02/2021. Disponível em: https://www.nextlawacademy.com.br/blog/lgpd-e-os-escritorios-de-advocacia-muito-alem-de-um-novo-nicho-de-mercado#:~:text=Ou%20seja%2C%20a%20LGPD%20atinge,%2C%20associados%2C%20fornecedores%2C%20etc. Acesso em: 05 Jan de 2023.

27 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 5º, inciso VII. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jan. 2023.

Assim, como regra geral, deve-se considerar que toda organização deverá indicar uma pessoa para assumir esse papel[28]. Contudo, em cumprimento ao estabelecido no § 3º do art. 41, a ANPD publicou a Resolução CD/ANPD nº 2, de 27 janeiro de 2022[29], que aprova o Regulamento de Aplicação da LGPD para "Agentes de Tratamento de Pequeno Porte", que traz hipótese de dispensa da necessidade de indicação do encarregado para esses agentes:

> Art. 11. Os agentes de tratamento de pequeno porte **não são obrigados** a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.

A Resolução CD/ANPD nº 2/2022 define em seu art. 2º, inciso I, agentes de tratamento de pequeno porte como sendo:

> I - Agentes de tratamento de pequeno porte: **microempresas, empresas de pequeno porte**, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

O art. 2º, inciso II, da referida Resolução, ainda determina que microempresas e empresas de pequeno porte são definidas como:

---

28 Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF. Abril 2022Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf .Acesso em: 05 jan. de 2023.

29 Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Publicado em 28/01/2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022 376562019. Acesso em: 05 jan. de 2023.

> II - microempresas e empresas de pequeno porte: **sociedade empresária, sociedade simples, sociedade limitada unipessoal**, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006.

Nesse contexto, é pertinente avaliar a necessidade de nomeação de encarregado para escritórios de advocacia, em observância ao disposto no art. 11 da Resolução CD/ANPD nº 02/2022, que dispensa a obrigatoriedade da nomeação para agentes de tratamento de pequeno porte.

Inicialmente, importante destacar que a Lei nº 8.906/1994[30], que dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB), estabelece em seu art. 15 que:

> Art. 15. Os advogados podem reunir-se em sociedade simples de prestação de serviços de advocacia ou constituir sociedade unipessoal de advocacia, na forma disciplinada nesta Lei e no regulamento geral.
> § 1º A sociedade de advogados e a sociedade unipessoal de advocacia adquirem personalidade jurídica com o registro aprovado dos seus atos constitutivos no Conselho Seccional da OAB em cuja base territorial tiver sede.

30 BRASIL. Lei nº 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 06 jan. de 2023.

O art. 982[31] do Código Civil Brasileiro define como empresária toda sociedade que tem por objeto o exercício de atividade própria de empresário sujeito a registro (art. 967 do Código Civil), e simples as demais. Nesse sentido, escritórios de advocacia são sociedades simples, ou seja, são sociedades que exploram atividade econômica, objetivam lucro, mas não exploram atividades empresariais[32].

Assim, pela interpretação dos artigos 2º e 11 da Resolução CD/ANPD nº 02/2022, pode-se entender que um escritório de advocacia constituído como sociedade simples, não estaria, a princípio, obrigado a nomear um encarregado, por ser tratar de agente de pequeno porte de tratamento de dados. Contudo, o art. 11º da Resolução da ANPD estabelece a obrigação de disponibilização de um canal de comunicação com o titular de dados para atender ao disposto no art. 41, § 2º, I, da LGPD e orienta que a indicação do encarregado será considerada política de boas práticas e governança:

> § 1º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.
> § 2º A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD.

Portanto, apesar de a indicação do encarregado não ser compulsória para os escritórios de advocacia que preencham os requisitos determinados pela Resolução CD/ANPD nº 02/2022, a própria norma reforçou expressamente a importância do encarregado para

31 BRASIL. Lei nº 10.406, de 10 de janeiro de 2022. Institui o Código Civil. Art. 982. Salvo as exceções expressas, considera-se empresária a sociedade que tem por objeto o exercício de atividade própria de empresário sujeito a registro (art. 967); e, simples, as demais. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 05 de jan. 2023.

32 BRASIL. Superior Tribunal de Justiça, Recurso Especial nº 1.227.240-SP (2010/0230258-0), Rel. Ministro Luis Felipe Salomão, Data de Julgamento 26/05/2015.

qualquer empresa. Isso porque o art. 52, § 1º, IX da LGPD, considerará as peculiaridades do caso concreto para aplicação de sanções após o procedimento administrativo, sendo a adoção de políticas de boas práticas e governança considerada parâmetro para aplicação de penalidades.

Não obstante, a não exigência de nomeação de encarregado para agentes de pequeno porte detalhada no art. 11 da Resolução CD/ANPD nº 02/2022 não é absoluta. O art. 3º da Resolução dispõe que não poderão se beneficiar do tratamento jurídico diferenciado os agentes de tratamento de pequeno porte que:

> I - realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 8º;
> II - aufiram receita bruta superior ao limite estabelecido no art. 3º, II, da Lei Complementar nº 123, de 2006 ou, no caso de startups, no art. 4º, § 1º, I, da Lei Complementar nº 182, de 2021; ou
> III - pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso.

De acordo com o referido artigo da Resolução CD/ANPD nº 02/2022, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, entre os a seguir indicados:

> I - critérios gerais:
> a) tratamento de dados pessoais em larga escala; ou
> b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
> II - critérios específicos:
> a) uso de tecnologias emergentes ou inovadoras;
> b) vigilância ou controle de zonas acessíveis ao público;

> c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
> d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.
> § 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.
> § 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Não há vedação na lei quanto ao encarregado ser um membro do próprio escritório, um funcionário ou o próprio sócio. A ANPD, no Guia Orientativo disponibilizado em abril de 2022, determina apenas que é importante que o encarregado tenha liberdade na realização de suas atribuições.

Vale assinalar ainda que, como o art. 41 da LGPD não determina se o encarregado deve ser pessoa física ou jurídica ou se este deve ou não fazer parte da empresa do controlador, é certo que este poderá ser terceirizado. Porém, conforme pondera Roinzof[33]

33 LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2021. Autor: Viviane Nóbrega Maldonado, Renato Opice Blum. Editor: Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018. CAPÍTULO I. DISPOSIÇÕES PRELIMINARES. Art. 5º. Página RL-1.2 https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v3/page/RL-1.2.

> "...é de extrema relevância que o agente de tratamento, no caso dessa decisão, avalie se o encarregado terceirizado conseguirá exercer todas as suas funções, principalmente de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e dar andamento nas solicitações dos titulares nas comunicações da ANPD."

Também não há vedação de que o encarregado seja um comitê ou grupo de pessoas nomeadas pela empresa, desde que seja designado, também nesse caso, um contato principal para as questões internas, para atender aos titulares dos dados e à ANPD.

A Regulação da CD/ANPD nº 02/2022 ainda preceitua que:

> "A LGPD não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados. Ao contrário, considerando as boas práticas, é importante que o encarregado tenha recursos adequados para realizar suas atividades, o que pode incluir recursos humanos. Outros recursos que devem ser considerados são tempo (prazo apropriados), finanças e infraestrutura.

A ANPD recomenda que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviços ou um ato administrativo.

No que diz respeito às suas qualificações profissionais, estas devem ser definidas mediante juízo de valor realizado pelo controlador que o indica, considerando conhecimento de proteção de dados e segurança de informação em nível que atenda às necessidades das operações de tratamento de dados pessoais da organização[34].

34 Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF. Abril 2022. Disponível em:https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf .Acesso em: 05 jan. de 2023.

A LGPD, em seu art. 41, § 2º[35], define as atividades do encarregado como sendo:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> (...)
> § 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.

Por agir como um ponto de contato com os titulares de dados e a ANPD, é importante que os detalhes de contato do encarregado de dados estejam facilmente acessíveis, nos termos do § 1º do art. 41 da LGPD[36]:

> § 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.

O § 3º do aludido artigo ainda estabelece que a autoridade nacional poderá estabelecer normas complementares sobre a

35 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 41º,§1º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jan. 2023.

36 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 41º, §1º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jan. 2023.

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.

Ressalte-se que não há necessidade, tendo em vista a ausência de previsão legal ou regulamentar, de comunicação ou de registro da identidade e das informações de contato do encarregado perante a ANPD.

Rony Vainzof[37] discute a importância de o encarregado ter independência opinativa para desempenhar o seu papel de orientar o controlador acerca das práticas de tratamento de dados pessoais e intermediar as relações. Ainda nesse sentido leciona Luis Fernando Chaves[38]:

> "há de ser livre no desempenho de suas funções, sem que receba instruções ou seja destituído em razão do (adequado) exercício de suas incumbências, ainda que suas recomendações, embora legais, sejam desfavoráveis aos negócios da empresa por ele assistida."

Na mesma linha, Rony Vainzof[39] arrazoa que, além da independência opinativa do encarregado, este ainda deve estar em constante busca de aprimorar seu conhecimento para melhor proteção dos dados pessoais tratados pela empresa:

37 LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2022. Viviane Nóbrega Maldonado, Renato Opice Blum. Editor: Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018. CAPÍTULO I. DISPOSIÇÕES PRELIMINARES. Art. 5º.. Página RL-1.2https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.2

38 CHAVES, Luis Fernando Prado. Responsável pelo tratamento, subcontratante e DPO. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). Comentários ao GDPR – Regulamento Geral de Proteção de Dados da União Europeia São Paulo: Ed. RT, 2018. p. 134-135.

39 LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2021. Autor: Viviane Nóbrega. Maldonado, Renato Opice Blum. Editor: Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018 CAPÍTULO I. DISPOSIÇÕES PRELIMINARES Art. 5º. Página RL-1.2 https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v3/page/RL-1.2

> "É importante que o Encarregado tenha atenção à sua formação contínua, para estar sempre atualizado, aprimorando seus conhecimentos de forma a contribuir para uma melhor proteção no tratamento de dados pessoais da sua empresa, diante da rápida evolução tecnológica e dos riscos inerentes de cada projeto que envolva dados pessoais."

Importante mencionar que a LGPD não exige expressamente a necessidade de o encarregado ter conhecimento especializado da legislação para ser nomeado, contudo a Legislação Europeia de proteção de dados pessoais, "General Data *Protection Regulation" ("GDPR")*[40] estabelece em seu art. 37 essa imposição:

> Art. 37. O responsável pela proteção de dados deve ser designado com base nas qualidades profissionais e, em particular, no conhecimento especializado da legislação e práticas de proteção de dados e na capacidade de desempenhar as funções referidas no artigo 39.

Em um processo de adequação da LGPD em um escritório de advocacia, a nomeação de um encarregado deverá observar os critérios dispostos no artigo 41 da Lei. Conforme discorrido acima, o encarregado poderá ser pessoa física ou jurídica, e apesar de a LGPD em seu art. 41 trazer a regra geral de nomeação do encarregado pelo controlador, a Resolução nº 02, de 27 de janeiro de 2022 da ANDP, em seu art. 11, prevê a hipótese de dispensa dessa condição para agentes de tratamento de pequeno porte.

Vale ressaltar que, apesar de não ser obrigatória a nomeação do Encarregado para os agentes de pequeno porte, conforme a Resolução da ANPD, sobretudo, para as sociedades simples, a nomeação do

40 GENERAL DATA PROTECTION REGULATION. GDPR. Regulation (EU) 2016/679. 25 de Maio de 2018. Disponível em: https://gdpr-info.eu/. Acesso em: 09 jan. de 2023.

encarregado é recomendável a um escritório de advocacia. Isso porque, em tese, tal ato exterioriza um cuidado maior no cumprimento da legislação de proteção de dados pessoais perante seus clientes e parceiros e pode eventualmente resguardar o escritório de sofrer penalidades mais severas em caso de aplicação de sanções por descumprimento da Lei (art. 52, § 1º, IX), uma vez que a nomeação do encarregado é considerada como política de boas práticas e governança, conforme disposto no art. 11, § 2º, da Resolução CD/ANPD, nº 02 de 27 de janeiro de 2022.

Por fim, frisa-se que, conforme recomendado pela ANPD, o encarregado deve ser indicado por um ato formal, como um termo de nomeação ou contrato de prestação de serviços, o que também deverá ser observado na implementação da LGPD nos escritórios de advocacia.

Abaixo, segue tabela para orientação geral na formalização do Encarregado de Proteção de Dados.

Formalização do Encarregado	
Conceitos Importantes	
Controlador, art. 5º, VI, da LGPD	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Operador, art. 5º, VII, LGPD.	Pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
Principal diferença entre operador e controlador	O operador é quem realiza o tratamento de dados pessoais em nome do controlador. Tanto o controlador quanto o operador são considerados agentes de tratamento, de acordo com o art. 5º, inciso IX, da LGPD
Quem é o encarregado?	
Encarregado, art. 5º, VIII, LGPD	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).

Principais Funções do Encarregado, art. 41, §2º LGPD	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.
Informações de contato, art. 41, § 1º, LGPD	A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
Quando indicar um encarregado?	
Regra Geral, art. 41 da LGPD	A LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado. Assim, deve-se assumir, como regra geral, que toda organização deverá indicar uma pessoa para desempenhar esse papel.
Exceção, art. 11 Resolução CD/ ANPD nº 2 de 27 de janeiro de 2022	O Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte traz hipótese de dispensa da necessidade de indicação do encarregado.
Quem pode ser o encarregado?	
A LGPD também não distingue se o encarregado deve ser pessoa física ou jurídica, e se deve ser um funcionário da organização ou um agente externo.	
Principais pontos a serem observados para nomeação de um Encarregado	
• O encarregado deve apresentar independência opinativa para orientar o controlador acerca das práticas de tratamento de dados pessoais e intermediar relações; • Deve buscar sempre aprimorar seu conhecimento na proteção de dados pessoais; • Deve possuir conhecimento especializado da Legislação e prática de proteção de dados, apesar de não ser uma necessidade imposta pela LGPD; • Evitar o acúmulo de funções para que o encarregado seja capaz de realizar suas atribuições com eficiência.	
Formalização da nomeação do Encarregado	

O Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado publicado pela ANPD em abril de 2022 recomenda que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviços ou termo de nomeação.

Formalização do Encarregado pelos Escritórios de Advocacia

- Poderá ser agente interno ou externo do escritório;
- Formalização da nomeação via Contrato de Prestação de Serviços ou Termo de Nomeação;
- Divulgação do contato e identidade do encarregado no sítio eletrônico do escritório.

3.7 FORMALIZAÇÃO DOS PAPÉIS – MATRIZ DE RACI

Priscila Silva Ribeiro[41]

Para os advogados e escritórios de advocacia que possuem em sua rotina o controle e cumprimento de prazos, atendimento aos clientes, captação e recepção de novas demandas, gestão, assim como atividades administrativas envolvidas na dinâmica do "advogar", adaptar o escritório de advocacia aos ditames da Lei Geral de Proteção de Dados, utilizando-se de ferramentas de gestão eficientes se mostra vantajoso e aconselhável.

O trabalho de adequação de um escritório de advocacia, principalmente os de grande porte, os quais lidam com grandes quantidades de dados dos clientes, pode ser algo complexo. Neste sentido, a Matriz de RACI, também conhecida como tabela RACI ou matriz de responsabilidades, pode ser um grande aliado quanto se trata de otimizar a questão, ao passo que define as responsabilidades na execução de um projeto, de forma clara e visual.

No ensejo, imperioso ressaltar que o intento deste capítulo não é ensinar a metodologia de um projeto, mas trazer boas práticas do dia a dia dos escritórios de advocacia, a teor do que dispõe o artigo 50 da LGPD:

> **Art. 50.** Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações

41 DPO Data Protection (Encarregado de dados), Advogada, Membro da Comissão de Proteção de Dados da OAB/MG, Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPCPD pela Legal Ethics and Compliance. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

> específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Conforme já exposto em tópico específico, a Lei Geral de Proteção de Dados elenca 3 figuras centrais e suas respectivas responsabilidades, sendo elas o Controlador, o Operador e o Encarregado de Dados.

De forma prática, a Matriz de Raci elencará as atribuições de cada um dos agentes de tratamento previstos em lei, assim como do encarregado de Dados, em cada etapa do projeto. O instrumento delimitará de forma específica cada atividade a ser executada, assim como o fluxo esperado.

Não existe na legislação obrigatoriedade quanto à utilização da matriz de RACI nos projetos de adequação à Lei Geral de Proteção de Dados. Porém, na prática, observou-se a sua eficácia quanto à otimização do fluxo de trabalho, sendo, portanto, uma das boas práticas a ser adotadas.

A definição das atividades é realizada por meio das letras existentes no acrônimo RACI, nos termos a seguir expostos:

R	A	C	I
Responsável	Aprovador	Consultado	Informado
Quem será o responsável pela execução de cada atividade.	O responsável pela aprovação de determinada atividade. Também será a pessoa cobrada caso aconteça algum problema.	É um especialista no assunto, o qual será consultado no desenvolvimento das atividades, a fim de melhorar o resultado.	informados sobre o que acontece no escritório, ainda que não atuem diretamente no projeto.

Fonte: do Autor, 2023.

É importante delimitar as funções de cada um dos envolvidos, principalmente quando exista multiplicidade de pessoas designadas

para executar determinada tarefa, a fim de se evitar confusões ou mesmo lacunas e não cumprimento de determinada atividade.

Abaixo, segue um modelo básico de matriz de RACI, o qual servir como ponto de partida para inspiração e início de qualquer projeto de adequação e implementação da LGPD.

DESCRIÇÃO DA ATIVIDADE INDICADOR	NOME DO EXECUTOR	DATA DE INÍCIO	DATA DE ENTREGA	STATUS

Fonte: do Autor, 2023.

A Matriz de Raci, além de facilitar a organização e atuação dos membros envolvidos no projeto de adequação a LGPD, contribui para a eficácia do projeto, assim como para a ciência de todos os integrantes do escritório, mesmo os não envolvidos diretamente em sua execução, sobre as tarefas em andamento e os responsáveis pelo seu desempenho.

3.8 TREINAMENTO DE CONSCIENTIZAÇÃO DO LGPD

Alan de Souza Pinto[42]

O treinamento de conscientização do LGPD tem como objetivo principal informar e educar os colaboradores de uma empresa sobre a Lei Geral de Proteção de Dados e como ela afeta as atividades cotidianas da organização.

A LGPD é aplicável a todas as empresas que processam dados pessoais, incluindo informações como nome, endereço, número de telefone, e-mail, entre outras. O treinamento de conscientização é essencial para garantir que as empresas estejam em conformidade com a lei, para que, assim, evitem possíveis sanções.

Desse modo, a conscientização dos profissionais é um dos pilares fundamentais para a implementação da LGPD nas organizações. O treinamento deve abordar não apenas as regras da lei, mas também os impactos da LGPD nos negócios e a importância da proteção dos dados pessoais dos clientes e usuários (SOUZA E MELO, 2020).

Por esse motivo, a conscientização dos colaboradores deve ser contínua e abrangente, envolvendo todos os setores da organização, desde o RH até o departamento de TI (OLIVEIRA, 2020). É importante que os treinamentos sejam adaptados à realidade da empresa e incluam exemplos práticos de situações que podem ocorrer no dia a dia dos profissionais. Ademais, vale ressaltar que a conscientização aos colaboradores deve ser acompanhada de medidas de segurança da informação, como a implementação de políticas de privacidade e a adoção de tecnologias de proteção de dados, como criptografia e firewall (BUCCI, 2020).

Nesse sentido, pode ser realizado por meio de várias modalidades, como presencial, virtual, e-learning, videoaula, entre

42 Mestre em Inovação Tecnológica, pela UFMG, Bolsista CAPES; Pós-graduado em Direito Digital e Proteção de Dados, pela EBRADI; Pós-graduado em Direito Civil Aplicado, pela PUC Minas; Graduado em Direito, pela PUC Minas; Membro da Comissão de Proteção de Dados da OAB/MG; Consultor em Privacidade e Proteção de Dados Pessoais; Professor; Advogado.

outras. O conteúdo do treinamento deve abranger todos os aspectos da lei, incluindo, mas não se limitando:

- Definição de dados pessoais: os colaboradores precisam entender o que são dados pessoais e as diferentes categorias existentes, como dados sensíveis e não sensíveis;
- Bases legais para o tratamento de dados: é importante que os colaboradores conheçam as bases legais para o tratamento de dados pessoais, como o consentimento, o legítimo interesse, entre outras;
- Direitos dos titulares de dados: os colaboradores precisam estar cientes dos direitos dos titulares de dados, como o direito de acesso, retificação, exclusão e portabilidade dos dados;
- Proteção de dados: é importante que os colaboradores compreendam as medidas de segurança necessárias para proteger os dados pessoais, como a criptografia de dados, o uso de senhas fortes, o armazenamento em local seguro, entre outras;
- Responsabilidades e sanções: é necessário que os colaboradores entendam suas responsabilidades em relação à proteção de dados pessoais e as possíveis sanções em caso de não cumprimento da lei.

Além desses aspectos, o treinamento deve incluir exemplos práticos de como garantir a proteção dos dados pessoais no dia a dia da empresa, como a utilização de políticas de privacidade, a revisão e atualização de contratos com fornecedores, entre outras práticas recomendadas.

Por fim, o treinamento de conscientização da LGPD é uma iniciativa importante para garantir que as empresas estejam em conformidade com a Lei Geral de Proteção de Dados e para proteger os dados pessoais de seus clientes e usuários. A educação dos

colaboradores é uma das principais estratégias para alcançar esse objetivo e garantir a privacidade e segurança dos dados pessoais.

3.9 LEVANTAMENTO DE ATIVOS COM DADOS PESSOAIS

Adiél Lima[43]

Compreender e analisar os ativos de uma Organização faz parte da gestão de processos de uma empresa. Por isso, é importante compreender o que são ativos e quais medidas as empresas devem adotar para protegê-los. Assim, ativos são pessoas ou equipamentos de uma empresa. No contexto deste livro, são os equipamentos (ex.: computadores centrais - servidores) da empresa.

Agora, que você já sabe o que são ativos, é importante que a empresa saiba quais são os seus equipamentos que processam e armazenam dados pessoais para que seja possível implementar o nível de proteção adequado. Isso pode ser feito por meio de um inventário.

O inventário possibilita mapear os ativos de uma organização, definir o seu nível de importância para o negócio, saber quais dados eles processam, armazenam e compartilham, atribuir responsáveis e protegê-los da melhor maneira possível.

Sem este inventário é muito difícil planejar e implementar uma solução de proteção para os dados pessoais, uma vez que não se sabe o que e muito menos como proteger.

Para realizar o levantamento de ativos é necessário:

- Catalogá-los e gerenciar este catálogo – pode ser utilizada uma planilha de excel, por exemplo;
- A sugestão é para que seja utilizado um software para Gestão de Ativos, pois ele lida melhor com a mudança constante de informações a respeito dos ativos;
- A seção 1 da metodologia de Segurança da Informação CIS Controls v8 – Inventário e Controle de Ativos contêm maiores

43 Identity Management, Access Management, Data Protection, AWS Security, NIST CSF e DCPT. Risk Mapping; Vulnerability Management; Employee training. Mais de 10 certificações, sendo a maioria em segurança. http://nuvym.net

detalhes a respeito de como implementar e gerenciar este processo em sua empresa.

Por fim, baseado na seção 4 da metodologia NIST SP 800-115 – Testes de Segurança (pentest), ativos desconhecidos podem ser um risco a empresa, uma vez que não há controle sobre eles e não se sabe quais ações eles estão executando na rede, que podem ser maliciosas, um hacker tentando invadir, por exemplo.

3.10 MAPEAMENTO E INVENTÁRIO DE DADOS

Alessandra C. Puig Casariego[44]

Com o advento da Lei Geral de Proteção de Dados, o primeiro passo da jornada para estar em conformidade com a LGPD é o mapeamento de dados pessoais, também conhecido como *data mapping* ou inventário de dados.

O mapeamento de dados consiste na análise do caminho que o dado pessoal percorre desde o momento em que é coletado pelo escritório até o seu descarte, ou seja, o mapeamento permite entender como os dados pessoais são coletados e como se movem dentro do escritório.

O objetivo principal desse processo é exatamente identificar a origem dos dados, quais são os canais utilizados para coleta, quais dados são tratados, por onde eles perpassam, com quem são compartilhados (agentes de tratamento) e onde e em qual formato estão armazenados.

Ademais, o mapeamento de dados permite analisar quais as categorias de dados tratados pelo escritório, para qual finalidade eles são coletados, qual a hipótese legal justifica o tratamento desses dados e qual é o grau de risco envolvido na coleta de cada informação.

Depois de uma breve explanação sobre o que é mapeamento de dados, vamos entender como se deve fazer o mapeamento de dados na prática?

Para realizar o mapeamento de dados, você poderá utilizar uma planilha de Excel, bem como contratar uma empresa especializada

44 Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG. Membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas - FGV. Master of Business Administration - MBA em Advocacia Corporativa e Governança pela Escola Superior da Advocacia - ESA OAB. Pós-graduação em Direito Bancário pela Fundação Getúlio Vargas - FGV. Certificação em Compliance pela KPMG. Certificação em Investigações Corporativas pela KPGM. Curso de Extensão em Lei Geral de Proteção de Dados pela PUC-RS.

com software específico para adequação e implementação da LGPD (existem várias no mercado).

Algumas informações são cruciais para a realização do mapeamento/inventário dos dados pessoais, tais como:

- Responsável pelo preenchimento;
- Macroprocesso (Quais são os processos executados e a descrição dos processos);
- Quais são os dados pessoais tratados/duração e descarte;
- Existência de dados de Crianças e adolescentes;
- Compartilhamento de dados internos;
- Compartilhamento de dados externos (Controladores/co-controladores /Operadores/suboperadores);
- Detalhes sobre o titular dos dados pessoais/Natureza dos Dados Pessoais Tratados (indicar se há dados pessoais sensíveis).
- Armazenamento dos Dados Pessoais;
- Segurança da Informação (SI);
- Transferência Internacional de Dados Pessoais;
- Decisão automatizada;
- Registros/gravações de vídeo, imagem e voz;
- Anonimização e Pseudonimização;
- Portabilidade dos dados pessoais;
- Base legal;
- Gaps;
- Recomendações.

Os exemplos mencionados acima servirão de base para que o escritório/empresa realize o devido mapeamento/inventário de dados pessoais. Somente a partir desse mapeamento/inventário é que a empresa poderá aplicar tanto medidas técnicas como organizacionais.

Conforme já mencionado, o mapeamento/inventário é crucial para a tomada de decisão da empresa/escritório, bem como para elaboração de alguns documentos exigidos pela Autoridade Nacional

de proteção de dados (ANPD), como é o caso do Relatório de Impacto a Proteção de Dados (RIPD), plano de resposta aos titulares, entre outros.

3.11 MAPEAMENTO DO SITE E DEMAIS APLICATIVOS

Carlos Henrique Almeida Salgado[45]

A Lei Geral de Proteção de Dados (LGPD) foi criada com o objetivo de proteger a privacidade, o interesse e a liberdade dos titulares dos dados e, consequentemente, atribuir uma série de obrigações para as empresas, sejam elas públicas ou privadas, para o adequado tratamento dos dados pessoais. [46]

O mapeamento do tratamento dos dados pessoais é dessas uma das obrigações impostas pela LGPD, que determina que os controladores e operadores façam o registro de todas as atividades de tratamento realizadas, mantendo-o sempre atualizado, de forma que seja possível realizar uma trilha de auditoria nos dados pessoais tratados pela Instituição, conforme previsto pelo artigo 37 da LGPD[47]:

> *Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.*

O documento deve refletir o caminho percorrido pelo dado pessoal dentro do site ou do aplicativo que está sendo mapeado, desde sua origem até seu descarte, incluindo os processos e procedimentos

45 Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP e Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

46 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 mar.2023.

47 BRASIL. Lei nº 10.406, de 10 de janeiro de 2002

pelos quais o dado transita e os mecanismos de segurança adotados durante o tratamento.

Na realização de um mapeamento do site ou de um aplicativo, seja ele manual ou via sistema, de forma resumida, devem ser verificados: I) responsável pelo preenchimento: nome e sobrenome, departamento, e-mail e telefone; II) site/plataforma: descrição do endereço do site, se o site já está atualizado e com as Nomas de Privacidade e Segurança da Informação, se quem cuida do site é a própria empresa que está sendo mapeada ou outra empresa terceirizada, caso seja este último caso, se existe algum contrato de prestação de serviços que formalize esta relação; III) políticas e procedimentos específicas para o site relativos à privacidade e a proteção dos dados pessoais: se existe política de privacidade, política de cookies, informações sobre os meios de contatos (DPO) no site da empresa, a possibilidade do titular requerer seus direitos no site; e por fim; IV) quais são os dados e a forma com que são realizadas as coletas de informações do site/plataforma: quais são os dados pessoais coletados, se o site coleta informações financeiras do titular dos dados e em caso positivo, quais são essas informações, se esses dados são compartilhados com alguma empresa terceira e quais são essas empresas, se o site armazena senhas dos usuários, onde são armazenados os dados coletados, qual a forma de descarte desses dados após atingida sua finalidade, quais medidas técnicas estão sendo aplicadas para resguardar os direitos dos titulares; V) geolocalização**:** se a empresa utiliza da geolocalização em seu site ou em seus aplicativos, se sim, quais são as medidas técnicas e administrativa aplicadas; VI) cookies: quais são os *cookies* coletados no site, qual a finalidade da coletados de cada cookies no site e por quanto tempo os cookies são utilizados/guardados; VII**)** incidentes e violações de dados pessoais: se já existiu algum tipo de incidente ou violação de dados pessoais no site da empresa, se (sim) - em qual momento, dia, mês e ano e quais medidas foram adotadas (GUERRA, Elaine).

O mapeamento auxiliará a empresa na identificação de tipos de dados pessoais tratados no site/plataforma ou no aplicativo, na atribuição de bases legais de cada tratamento, no atendimento

das solicitações de titulares de dados pessoais, e a tornará apta a demonstrar de forma objetiva o cumprimento dos princípios da Lei (transparência e responsabilização) e, principalmente, a comprovar seu processo de conformidade com a LGPD, quando requerido pelos entes fiscalizadores, parceiros de negócios e até mesmo pelo poder judiciário verificarem sua plataforma.

3.12 MAPEAMENTO DE DADOS PESSOAIS TI

Adiel Ribeiro[48]

O Mapeamento de dados pessoais, executado pelo setor de tecnologia, pelo setor de segurança da informação, ou ambos, é similar ao processo de Levantamento de Ativos. Ele é importante para que se saiba como e por que esses dados são coletados, processados, armazenados, compartilhados ou excluídos nos respectivos ativos da empresa.

Somente a partir desta visão holística do fluxo de dados pessoais tratados pelos ativos da empresa é possível definir o nível adequando de proteção, pois ela permite visualizar o caminho percorrido desde a coleta até a sua exclusão.

O nível adequado de proteção sugere que a informação seja protegida conforme seu nível de criticidade para o negócio e é ideal que seja a um custo-benefício aceitável.

Como exemplo prático, pense em empresas que tratam dados pessoais sensíveis, de orientação sexual ou médicos. Estes dados devem ser fortemente protegidos, pois podem causar danos irreversíveis ao titular, caso vazem.

Por isso é importante saber em quais ativos eles são processados, armazenados, quem os acessa, se são e como eles são compartilhados e até mesmo se são devidamente excluídos, impossibilitando acesso não autorizado.

Baseado nessa visão holística, é possível identificar qual dado pessoal está sendo tratado nos ativos da empresa, como e quando ele é coletado, qual a finalidade, quais pessoas, sistemas e terceiros poderão ter acesso a ele, onde e como ele será armazenado, se ele pode ser compartilhado, e quais são os meios de transmissão.

Ademais, no processo de mapeamento de dados, quatro perguntas são importantes:

48 Gestão de Vulnerabilidades e Segurança em nuvem AWS.
http://nuvym.net

1. Quais dados pessoais estou tratando em meus ativos?
2. Como?
3. Por quê?
4. Quais as medidas de proteção estão implementadas?

A partir disso é possível planejar, implementar e aumentar o nível de proteção de dados pessoais nos ativos da empresa.

É importante enfatizar que o Mapeamento do fluxo de Dados Pessoais é complementar ao Inventário de Ativos.

A seção 5.9 - Inventário de Informações e Outros Ativos Associados da ISO 27002:2022 – padrão de mercado em Segurança da Informação, pode ajudar tanto no Inventário de Ativos quanto no Mapeamento do Fluxo de Dados.

A seção 3.3 - Relacionamento do Ciclo Vida do Tratamento dos Dados Pessoais com ativos organizacionais do guia de boas práticas Lei Geral de Proteção de Dados (LGPD) – publicado pela ANPD, apresenta detalhadamente como executar o processo do Mapeamento de Fluxo de Dados e os Ativos Envolvidos.

3.13 MANUAL DE PRIVACIDADE – LEIS, NORMAS, DECRETOS, REGULAMENTOS, PORTARIAS (PRAZO DE GUARDA)

Elaine Cristina Oliveira Guerra[49]

O Manual de Privacidade (Leis, Normas, Decretos, Regulamentos, Portarias entre outros) tem por finalidade identificar e descrever quais documentações são utilizadas em cada setor da Organização, bem como qual sua finalidade, prazo de guarda, a legislação que trata do assunto (documentos), a base legal aplicada na LGPD para utilização deste documento.

Este manual auxiliará a empresa no cumprimento do artigo 15 e 16 da Lei Geral de Proteção de Dados, que trata do término do tratamento dos dados pessoais.

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - Fim do período de tratamento;
> III - Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

49 Especialista em Direito, Inovação e tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados - ISFS), Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora do "Manual Prático de Adequação à LGPD com enfoque nas Relações do Trabalho". Autora de capítulos de livros jurídicos. Empresária em projetos de adequação e implementação da LGPD. Atuante com projetos de DPO as a Service. Mentora em projetos de adequação e implementação da LGPD. Palestrante em Privacidade e Proteção de dados. Diretora do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pesquisadora da USP/SP. Advogada.

> IV - Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.
> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - Cumprimento de obrigação legal ou regulatória pelo controlador;
> II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Findo este lapso temporal, faz-se premente a necessidade do descarte adequado desses documentos, com exceção de outra norma que obrigue a sua guarda.

Ademais, é bom enfatizar que a LGPD prega pelo ciclo de vida dos dados pessoais, e esse, precisa ser respeitado. Assim, a partir do momento em que a empresa não exerce o descarte adequado na legislação comandante, há claro desrespeito aos princípios contidos na LGPD.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> II - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais

> e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da 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.

É importante destacar que o Encarregado de Proteção de Dados (*DPO*), juntamente com o comitê de privacidade e proteção de dados, tem a obrigação de SEMPRE atualizar a legislação pertinente aos dados tratados pela Organização, bem como documentar todo e qualquer descarte realizado no setor.

Abaixo, segue um modelo que poderá auxiliar escritórios de advocacia no manuseio e descarte dos dados pessoais.

ÁREA:				
Documento	Finalidade	Prazo de Guarda	Legislação	Base Legal/LGPD

Fonte: Do autor, 2023

3.14 ANÁLISE DE RISCO (JURÍDICO) DE TODOS OS PROCESSOS MAPEADOS PELA EMPRESA (MATRIZ DE RISCO)

Elaine Cristina Pereira dos Santos Nery[50]

A Lei Geral de Proteção de dados estabelece uma série de disposições a serem implementadas quanto ao processo de conformidade a Lei dentro das Organizações.

O Controlador, ao iniciar a adequação e implementação da Lei dentro de sua Organização, estabelece objetivos e premissas a serem alcançados. Para tanto, o ideal é que a adequação seja feita com base em um modelo de gestão de riscos.

Pensando na gestão e definição dos riscos existentes em cada processo, as empresas buscaram metodologias já aplicadas no mercado, como é o caso da utilização das normas ISOs, as quais estabelecem requisitos para obtenção de um Sistema de Gestão da Qualidade (SGQ) de uma organização, não significando, necessariamente, conformidade de produto às suas respectivas especificações.

A ABNT NBR ISO31000[51], por exemplo, define que todas as atividades de uma organização envolvem risco, como tais, precisamos mitigá-las para evitar qualquer tipo de vazamento de dados nos processos. A Norma ISO 73:2009 fornece vocabulário para desenvolvimento de entendimentos comuns sobre termos e conceitos, já a ISO 31000:2009 [52], que trata da gestão de riscos, aponta princípios e diretrizes:

50 Advogada. Especialista em Direito Público. Especialista em Privacidade e Proteção de dados. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão de Proteção de Dados do Estado (OAB/MG), Membro da Comissão de Proteção de Dados da Universidade Federal dos Vales do Jequitinhonha e Mucuri- UFVJM.

51 ABNT ISO GUIA ISO 31000:2009 **Gestão de riscos — Princípios e diretrizes** *Risk management – Principles and guidelines*ABNT NBR ISO 31000:2009.

52 ABNT ISO GUIA ISO 73:2009 Gestão de riscos – Vocabulários - 12 páginas.

> "Organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco". Todas as atividades de uma organização envolvem risco.
> As organizações gerenciam o risco, identificando-o, analisando-o e, em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco. Ao longo de todo este processo, elas comunicam e consultam as partes interessadas e monitoram e analisam criticamente o risco e os controles que o modificam, a fim de assegurar que nenhum tratamento de risco adicional seja requerido".

A gestão dos riscos é uma obrigação que recai tanto sobre o controlador quanto sobre o operador. Nesse contexto, é de suma importância manter um entendimento claro de todas as ações dentro da organização que envolve o processamento de dados pessoais. Isso pode ser alcançado por meio do estabelecimento do "registro das operações de tratamento de dados pessoais", conforme previsto no artigo 37 da LGPD.

A legislação Brasileira exige que em determinados planos, o controlador prepare o relatório de avaliação de impacto de proteção de dados - RIPDI. Isso se aplica, por exemplo, ao tratamento de dados com base na justificativa de Legítimo Interesse (conforme descrito no artigo 10, parágrafo 3) ou quando envolve o uso de informações sensíveis (conforme previsto no artigo 38).

O relatório requer a inclusão de detalhes de procedimentos relativos ao processamento de informações pessoais que possam afetar as liberdades civis e os direitos fundamentais, bem como estratégias de segurança e abordagens para reduzir tais riscos, conforme estipulado no artigo 5º, parágrafo XVII. Além disso, mesmo quando o tratamento de dados, não se fundamenta no interesse legítimo ou não envolve

informações sensíveis, o Controlador tem a opção de empregar relatórios de impacto na proteção de dados como um instrumento auxiliar para avaliar o risco associado à execução de procedimentos específicos.

A instituição de uma avaliação e administração de riscos eficazes na empresa está em harmonia com o princípio que determina a incorporação de práticas de responsabilidade pró-ativa (*accountability*) por parte dos responsáveis pelo tratamento de dados.

Portanto, ao utilizar metodologias como certificações, relatórios de impacto e matrizes de risco, fica evidente que uma Organização, cuja base de sua gestão é o gerenciamento de riscos, promove uma melhoria na governança, a qual está presente em todos os processos, desde o princípio.

Segundo a ISO 31000:2009[53], o gerenciamento de riscos deve acontecer em cada tomada de decisão, e deve ser considerada por gestores como sendo essencial para a realização dos objetivos da organização, constituindo atributo que normalmente aparece refletido nas declarações de política da organização, em especial as relativas à gestão de riscos.

Outrossim, a ISO 3100:2009 descreve que convém a Organização identificar as fontes de risco, as áreas de impactos, os eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais.

Segundo o PMBOX[54], o gerenciamento dos riscos do projeto inclui os processos de condução do planejamento, da identificação, da análise, do planejamento das respostas, da implementação das respostas e do monitoramento dos riscos em um projeto.

Trazendo para a prática no projeto de adequação e implementação da LGPD, é fundamental que, após a realização do mapeamento e/ou durante, seja feita uma análise dos riscos de cada processo, para assim,

53 ABNT ISO GUIA ISO 31000:2009 **Gestão de riscos — Princípios e diretrizes** *Risk management – Principles and guidelines*ABNT NBR ISO 31000:2009.

54 PMI. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)**, Project Management Institute, 6ªed – Newtown Square, PA: Project Management Institute, 2017.

poder adotar medidas técnicas e administrativas a fim de aceitar e/ou mitigar os riscos.

Abaixo, segue um modelo de tabela eficaz para realizar o mapeamento de risco – todavia, é apenas um modelo, pois a matriz de risco deve ser criada de acordo com os processos da empresa.

TIPO	DESCRIÇÃO	QUANTIDADE
Crítico	Deve ser mitigado imediatamente.	
Grave	Deve ser mitigado.	
Moderado	Deve ser priorizado.	
Pequeno	Pode aguardar um período razoável.	
Desprezível	Pode aguardar um período maior.	

Fonte: Elaborado pelo próprio autor, 2023.

3.15 ANÁLISE DE RISCO

Adiel Ribeiro[55]

O objetivo da análise de risco é verificar a probabilidade de um incidente (invasão, vazamento de dados, parada de sistemas entre outros) ocorrer versus o impacto que isso pode causar na empresa.

Ela é executada baseada no Levantamento de Ativos e no Mapeamento de Dados Pessoais, apresentados anteriormente, entre outros, por exemplo, Gestão de Vulnerabilidades, que pode ser vista em detalhes na metodologia de Segurança da Informação CIS Controls v8 – item 07 – Continuous Vulnerability Management.

A partir da Análise de Risco, é possível visualizar qual a função do respectivo ativo na rede, sua criticidade, quais dados ele trata e quais controles compensatórios estão em ação para mitigar a probabilidade de um incidente, baseado no impacto que isso pode causar ao negócio.

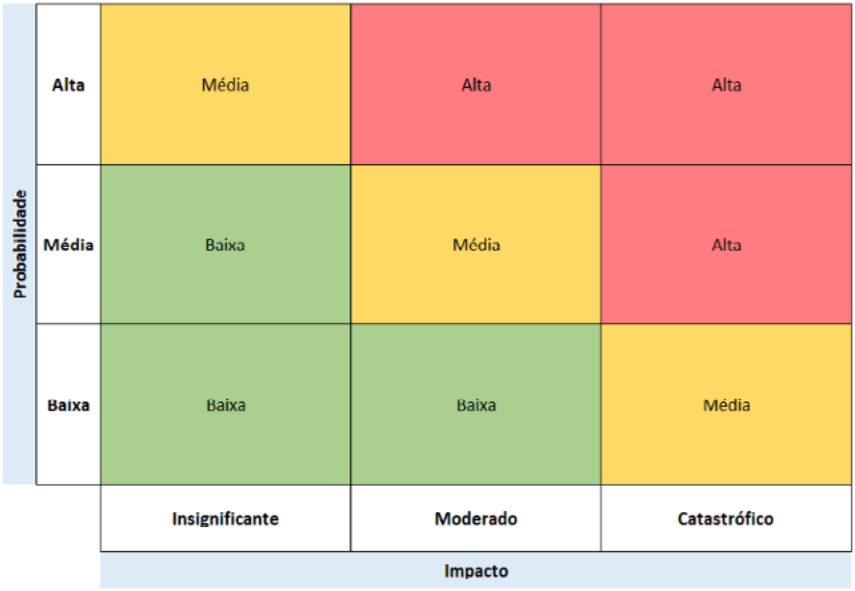
A Análise de Riscos se baseia fundamentalmente em se é viável tratar o respectivo risco ou se o tratamento dele é mais trabalhoso e mais caro do que o impacto negativo que ele pode causar.

Fatores que podem contribuir para possíveis ativos que apresentem riscos ao negócio são o caso de aplicações legadas, que não podem ser atualizadas e são necessárias ao funcionamento das empresas.

(Neste caso é sugerido que estes riscos sejam formalizados e aceitos). Abaixo, um desenho de Matriz de Risco:

55 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net

Figura 1: Matriz de risco



Baseado na análise de risco, é possível determinar que riscos as empresas correm, como, quando e por que eles serão mitigados e se eles serão aceitos.

Um exemplo:

Qual dos itens abaixo apresenta maior impacto para um escritório de advocacia?

1 - O site ficar fora do ar

2 - Documentos de clientes vazarem

O item 2 apresenta maior impacto.

Para elaborar a Análise de Risco, é necessário identificar qual a probabilidade deste evento ocorrer e determinar se é um risco alto, médio ou baixo, ou conforme a classificação determinada pela empresa.

O mesmo ocorre para o item 1, o site ficar fora do ar pode ser ruim, que cause pouco impacto, a depender do negócio da empresa, isso pode representar um risco baixo na análise.

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46). "Guia de boas práticas Lei Geral de Proteção de Dados (LGPD)"

A Análise de Riscos leva em conta também as medidas de proteção implementadas para reduzir a probabilidade e o impacto de um possível incidente.

Nas figuras abaixo é possível comparar e visualizar a diminuição do risco por meio da implementação de medidas de proteção.

Figura 2: Nível de risco p/ tratamento de Dados Pessoais

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]
R01	Acesso não autorizado.	10	15	150

Figura 3: Nível de risco residual p/ tratamento de Dados Pessoais

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S)[3] APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico. 2. Desenvolvimento seguro. 3. Segurança em Redes.	Reduzir	5	10	50	Sim

Cada empresa deve desenvolver sua própria metodologia de análise e classificação de riscos, conforme o seu negócio.

Os itens 2.5.2.6 Identificar e avaliar os riscos e 2.5.2.7 Identificar medidas para tratar os riscos do GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) podem auxiliar nessa tarefa.

O NIST Risk Management Framework – RMF é um guia completo para elaborar uma Análise de Riscos, disponível em: https://csrc.nist.gov/projects/risk-management.

3.16 PLANO DE AÇÃO E ORÇAMENTO

Emily Matias Assumpção[56]

O plano de ação é uma das etapas do processo de adequação à LGPD em que se é possível ver a parte prática da Lei de forma efetiva.

Tal observação se constata quando analisamos de forma pormenorizada cada fase do processo e seu objetivo. O mapeamento de dados é aquela famosa "faxina", ou seja, busca entender quais dados tramitam na empresa, qual finalidade, por quanto tempo, se há descarte, transferência, entre outros. Já na fase de *Gap Analysis* (levantamento de riscos), os dados mapeados são analisados e consequentemente são levantados os riscos, considerando seu grau de impacto e probabilidade.

No plano de ação, são indicadas melhorias para cada risco levantado, mas trazendo a adequação à LGPD para a realidade da maioria das empresas e escritórios de advocacia em nosso País não é viável, nem mesmo é possível realizar todas as melhorias indicadas no plano de ação de uma só vez, isso porque nem sempre as empresas têm recursos humanos e financeiros para executar as tarefas do plano de ação.

Desse modo, o plano de ação é um documento onde constam todas as melhorias e soluções apontadas, com prazos para estruturação, periodicidade, o nome do responsável pela melhoria, o setor envolvido, tempo de revisões, entre outras questões que você, como consultor, pode achar necessário incluir.

Muito se fala que o processo de adequação à LGPD não é uma "receita de bolo", e de fato isso é um argumento que procede, mas existem algumas metodologias que auxiliam nas fases do processo, como é o exemplo da metodologia 5W2H no plano de ação.

56 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

Nas palavras de Guilherme Rabelo, em seu artigo, ele explica o conceito de 5W2H e como ela pode aumentar produtividade.

> O 5W2H é uma ferramenta de produtividade que consiste em um conjunto de sete diretrizes que contribuem para a organização das tarefas, com o foco na melhoria contínua.
> Assim, a metodologia usa perguntas que visam ajudar os profissionais a desenvolverem o planejamento de projetos, estratégias ou atividades, com praticidade e clareza. Seguindo essa lógica, todos os envolvidos conseguem entender melhor o que se espera deles.[57]

Nesse sentido, o 5W indica às cinco diretrizes que começam, em inglês, com a letra W, sendo elas: *What* (O que), *Why* (Por que), *Where* (Onde), *Who* (Quem), *When* (Quando). O 2H indica às duas perguntas iniciadas com a letra H, em inglês: *How* (Como) e *How much* (Quanto custa).

Como já dito acima, para desenvolver o plano de ação é necessário ter disponibilidade de recursos, sejam eles humanos e financeiros, por esse motivo as perguntas supracitadas fazem toda diferença no plano de ação.

No momento em que o escritório define o que é preciso fazer no plano de ação, o porquê (adequação do escritório à LGPD), se a adequação será feita nas dependências do escritório ou na modalidade de *home office*, por exemplo, quem serão as pessoas envolvidas (cargos, funções, setores que vão desempenhar), em quanto tempo serão desenvolvidos (por esse motivo é importante estabelecer um prazo limite para o desenvolvimento das tarefas) e quanto vai custar o projeto, seu cliente consegue ter a noção completa do plano de ação e como ele deverá ser feito.

57 RABELO, Guilherme, O que é 5W2H e como ela pode aumentar produtividade? Disponível em (https://www.siteware.com.br/metodologias/o-que-e-5w2h/) acesso em 19/03/23.

De igual modo, nem todos os escritórios de advocacia possuem profissionais da Tecnologia da Informação e da Segurança internos, por esse motivo é de extrema importância incluir a contratação dos referidos profissionais no orçamento da empresa.

Logo, o plano de ação é um documento que norteia sobre as próximas etapas, a periodicidade, processos e cargos envolvidos, bem como prazo para a implementação na empresa. Segue abaixo um exemplo do que deve conter no plano de ação:

O quê? (qual a melhoria apontada)	Por quê? (motivo)	Quem? (responsável)	Onde? (local)	Quando? (cronograma, prazos)	Como? (processo)	Quanto? (custo)

Portanto, reitera-se que o plano de ação pode mudar de acordo com o porte do escritório, bem como o nível de complexidade das demandas, sendo a metodologia 5W2H um ponto de partida para otimizar e trazer celeridade na fase do plano de ação.

3.17 RELATÓRIO DE MATURIDADE LGPD

Gabriel Campos Cunha[58]

O relatório (diagnóstico) de maturidade das organizações em relação à adequação à Lei Geral de Proteção de Dados (LGPD) serve para demonstrar e ajudar as empresas a compreenderem a sua situação atual em relação ao cumprimento da lei de proteção de dados.

Este relatório pode/deve avaliar diversos aspectos, alinhados com o ramo de atividade da organização, abordando, por exemplo, o mapeamento de processos, controle da coleta, armazenamento, compartilhamento de dados pessoais nos processos da organização, questões de segurança, incidência e respeito às bases legais, contratos com fluxos de dados pessoais, procedimentos, práticas adotadas ou não pela organização para promover a segurança da informação e a privacidade, entre outros.

Este relatório deve identificar lacunas em relação ao cumprimento da LGPD e propor medidas para corrigi-las. Além disso, pode-se atribuir à tais lacunas os riscos associados à privacidade e proteção de dados e, junto a isso, seu grau de potencialidade a causar danos.

Vale dizer que este relatório pode ser utilizado para demonstrar a conformidade da organização com a LGPD, ou mesmo o início de um projeto de adequação, o que pode ser útil em casos de auditorias ou processos judiciais.

Abaixo, sugere-se a organização temática para organização do relatório com seguintes itens (minimamente)

1. Introdução
2. Questões legais e regulatórias

58 Advogado, consultor em Governança Corporativa, ESG, Compliance, Integridade, Proteção de Dados. Auditor de Sistemas De Gestão da Qualidade, Meio Ambiente, Saúde e Segurança do Trabalho. Auditor da Conformidade Legal nos temas de Proteção de Dados, Privacidade, Meio Ambiente e Saúde e Segurança do Trabalho.

3. Contextualização ramo de atividade e recomendações prévias
4. Políticas, procedimentos e práticas já realizados pela empresa inerentes à LGPD
5. Descrição dos setores, processos, e ciclo de vida dos dados pessoais
6. Informações sobre segurança da informação: políticas de segurança da informação, organização da segurança da informação, segurança em recursos humanos, gestão de ativos, controle de acesso, criptografia, segurança física e do ambiente, segurança nas operações, segurança nas comunicações, aquisição, desenvolvimento e manutenção de sistemas, relacionamento na cadeia de suprimentos, gestão de incidentes de segurança da informação, aspectos da segurança da informação na gestão da continuidade do negócio).
7. Lacunas e riscos
8. Planos de ações

Quanto as Lacunas e Riscos, recomenda-se que seja apresentado para a organização em perspectiva uma estrutura conectando os processos organizacionais às lacunas encontradas e aos riscos inerentes, estabelecendo-se as ações recomendadas para eliminação ou mitigação deste risco.

Abaixo, trago-lhes uma tabela como exemplificação:

Análise de Impacto do Tratamento de Dados Pessoais						
Nº da Análise	Setor	Processo	Lacuna	Risco	Grau de Risco	Ações Recomendadas
1º	RH	Recrutamento e Seleção	Ausência de termo de consentimento para tratamento de dados sensíveis de candidatos PCD	O tratamento de dados pessoais é realizado sem a devida base legal podendo gerar riscos de sanção administrativa, condenações judiciais e indenizações.	Alto	1º Elaborar e implementar mecanismo de coleta de consentimento para o tratamento de dados pessoais sensíveis no processo de recrutamento e seleção de PCDs; 2º Realizar a eliminação dos dados sensíveis coletados de PCD, sem a devida base legal ou articular a consecução de consentimento para esses dados

Fonte: Do Autor

3.18 ATA DE REUNIÃO

Isabela Cristina Maia da Cruz[59]

A ata é um instrumento utilizado pela empresa para que possa fazer um registro expositivo de fatos e decisões tomadas nas reuniões, assembleias, sessões. É um documento de grande importância, pois é responsável por registrar todas as informações e decisões tomadas, servindo como meio de consulta sempre que necessário.

Além do mais, ela poderá ser utilizada para comprovar determinadas ação que foram realizadas pela empresa, bem como para evitar atitudes de má-fé de algum colaborador, cliente, parceiro e terceiros que porventura integram a Organização.

A LGPD não traz uma obrigatoriedade de ter uma ata para todas as reuniões, mas é utilizado como melhores práticas dentro das Organizações.

Ademais, é bom enfatizar que a ata possui alguns mecanismos para evitar fraudes, como não deixar espaços em branco para que informações sejam preenchidas, não escrever números em algarismos arábicos ou romanos, em caso de erros, não se pode rasurar, entre outras informações.

A título de exemplificação, são necessários os seguintes itens para a ata:

- Data, local, hora do início e término;
- Pauta da reunião;
- Membros presente, bem como a justificativa da ausência;
- Cargo dos membros presentes;
- Impressibilidade dos membros saberem das necessidades tomada, e discursões que foram feitas;

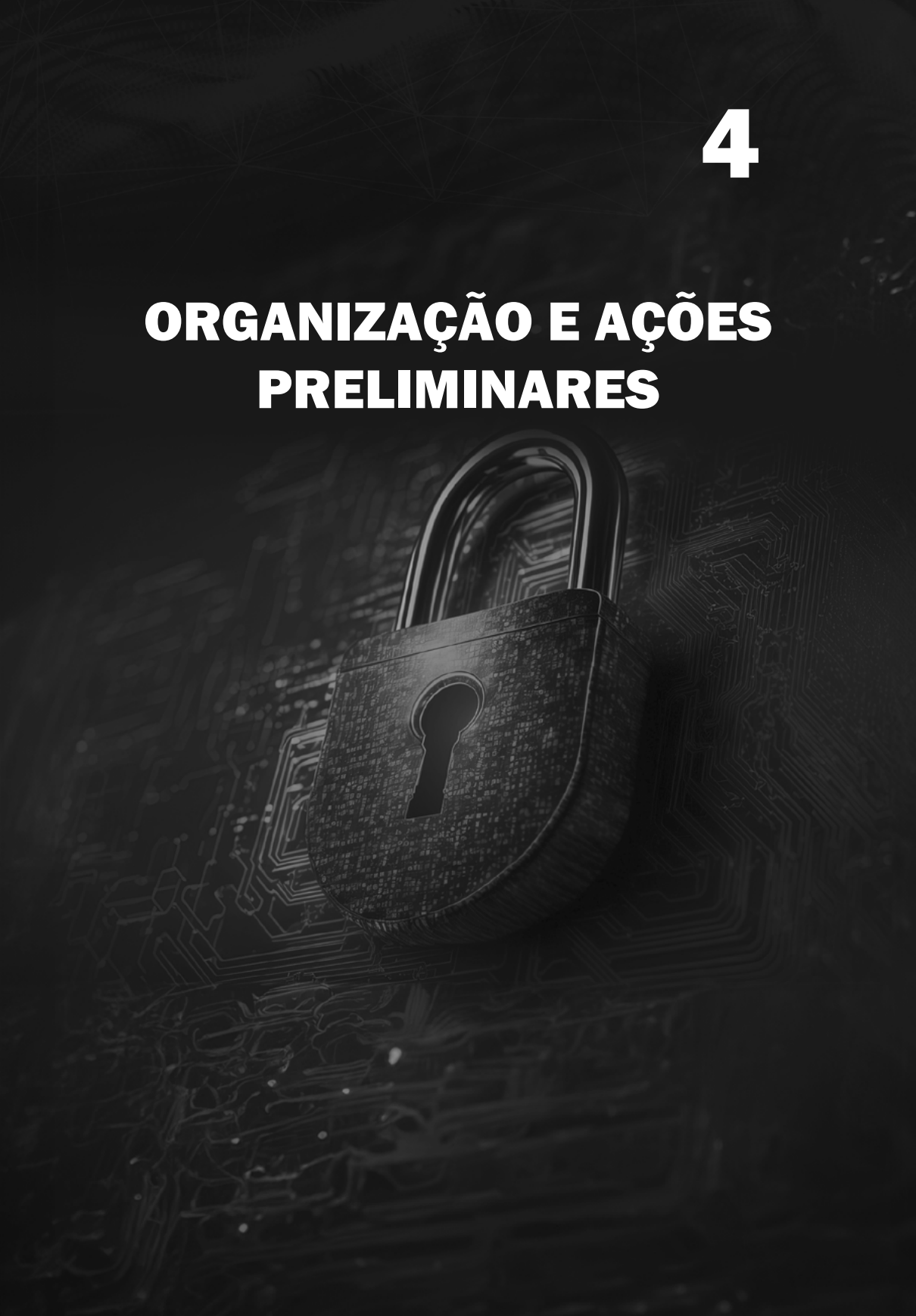
59 Advogada, especialista em Direito Digital e compliance, Presidente da comissão proteção de dados, subseção Vespasiano, membro da Comissão Lei Geral de Proteção de Dados-OAB/MG.

- O propósito da reunião, a importância, com a necessidade de constar por quem a necessidade fora tomada;
- Assinatura dos responsáveis legais.

Com os itens exemplificados acima, a empresa terá evidências de todos os processos que foram realizadas, tanto interno (Colaboradores), como externa (clientes), a fim de resguardar a empresa em todas as esferas (cível, administrativo e judicial).

4

ORGANIZAÇÃO E AÇÕES PRELIMINARES



4.1 APRESENTAÇÃO DO PLANO DE AÇÃO (JURÍDICO) PARA ALTA GESTÃO

Izabela Nunes Pinto[60]

A Lei Geral de Proteção de Dados Pessoais 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, sendo que as normas gerais contidas na aludida Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Para elaborar o plano de adequação à LGPD, é necessário o engajamento das principais áreas da empresa/instituição, cujas lideranças devem compor a equipe de planejamento, implementação e monitoramento das atividades a serem desenvolvidas.

Nesse sentido, é importante que a organização defina uma pessoa para liderar o Projeto de Adequação à Proteção de Dados. Na Lei, essa é a figura do DPO (encarregado de proteção de dados), bem como uma equipe para auxiliar o DPO no desenvolvimento do Projeto e no *Compliance*.

O Plano de Ação é o instrumento orientador de adequação da alta gestão, seja por pessoa natural ou por pessoa jurídica de direito público ou privado, à Lei Geral de Proteção de Dados Pessoais. Ou seja, é um documento que contém as diretrizes para uma boa governança e alinhamento às práticas da legislação.

Nesse sentido, importante mencionar alguns dos objetivos, gerais e específicos, do plano de ação.

60 Advogada. Membro nomeado da Comissão de Proteção de Dados da OAB/MG. Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Curso de Direito para Startups na Europa (envolvendo GDPR, LGPD e outros temas relacionados ao Direito Digital) pela Academy da Platzi. Finalista, ocupando o 3º Lugar Geral do Brasil da 1a Edição do LawCamp - 1a Competição de Implementação da LGPD no Brasil. Palestrante (Adequação/Implementação da LGPD e Direito Digital).9

Objetivos Gerais:

- Implementar a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) na empresa;
- Implementar as diretrizes estratégicas e operacionais da LGPD nos processos da Instituição;
- Conscientizar os colaboradores para garantir a proteção da privacidade de dados pessoais tratados na empresa;
- Favorecer o atendimento aos direitos dos titulares de dados.

Objetivos Específicos:

- Conferir transparência sobre o uso dos dados pessoais pela empresa;
- Instituir e implementar política de privacidade de dados pessoais;
- Oferecer maior clareza à gestão sobre os ciclos de vida dos dados pessoais;
- Disseminar conhecimentos necessários acerca do tema, conscientizando a todos os colaboradores sobre a importância do cuidado ao realizar o tratamento de dados pessoais pela empresa;
- Definir mecanismos de governança para monitoramento do tratamento de dados pessoais

Considerando os objetivos supramencionados, para a apresentação do plano de ação necessário a adoção de algumas práticas. Vejamos:

Identificar a oportunidade de melhoria: O intuito é conhecer a finalidade e os princípios da LGPD.

Realizar a análise do fenômeno: Devem ser identificados quais dados pessoais são coletados e tratados pela organização.

Proporcionar a análise do processo - Mapear, analisar e identificar as lacunas:

- mapear a categoria de todos dados pessoais coletados (empregados, terceiros, clientes, entre outros);
- mapear o fluxo dos dados pessoais (como são coletados, por quem, finalidade do tratamento, local de armazenamento, com quem são compartilhados, quais os meios técnicos e administrativos de segurança dessas informações entre outros);
- averiguar a localização dos servidores e quem tem acesso a eles;
- mapear as empresas terceiras que prestam serviço para a organização;
- analisar os contratos vigentes
- verificar se há políticas, normas, procedimentos relacionados à segurança da informação, armazenamento e descartes de dados, gestão de risco, o que se deve fazer em caso de incidentes como vazamento de dados pessoais;
- Relacionar quaisquer outras informações relevantes e específicas para a organização desenvolver um Projeto de Governança Digital.

O Plano de Ação deve estar devidamente documentado e estruturado, ou seja, com as ações a tomar, os responsáveis e prazos bem definidos.

Para adequação da empresa à LGPD deverá ser encaminhado aos setores responsáveis pelo tratamento de dados alguns formulários para alimentação do sistema, com o objetivo de dar uniformidade e celeridade às informações necessárias para a avaliação da Comissão Multidisciplinar e consequente adoção de providências.

Para cumprimento desta fase, os membros designados para compor a equipe multidisciplinar, que será responsável pela elaboração do plano de ação, devem participar de capacitações, realizar pesquisas e reuniões de modo a melhor planejar e decidir as ações a serem implementadas.

As ações que forem elencadas para execução serão produto de levantamento realizado por cada setor da empresa, por meio de planilha ou formulário, de modo a determinar quais ações devem ser prioritárias. Após a realização do levantamento, as ações deverão ser validadas pela Comissão para servir de insumo ao Plano de Adequação.

O propósito da apresentação do Plano de Ação é entender não somente o problema, mas, principalmente, suas causas, e não as consequências.

4.2 PLANO DE AÇÃO TI/SI

Adiel Ribeiro[61]

O objetivo do plano de ação de TI/SI pode ser baseado na ISO 27001 – que inclui a implementação de um SGSI (Sistema Gerenciador de Segurança da Informação), que deve estar alinhado aos objetivos de negócio, ou seja, como a Segurança da Informação pode apoiar a estratégia de negócio da empresa. A maneira como a SI pode apoiar a empresa é auxiliando-a a identificar e mitigar os riscos, de forma que, entre outros, os sistemas estejam sempre disponíveis e que, como exemplo, não haja acesso não autorizado.

Pense em um banco: Clientes não devem acessar contas de outros clientes.

Este é um dos objetivos do plano de ação para instituições financeiras, que devem aderir, entre outros, normas regulatórias tais como:

- PCIDSS;
- CIRCULAR SUSEP Nº 638, DE 27 DE JULHO DE 2021

Ademais, é bom mencionar que as medidas de mitigação de riscos são técnicas e organizacionais, aplicadas por meio de pessoas, processos e tecnologia. Em se tratando dessas medidas, a Norma ISO traz algumas recomendações, como exemplo:

- pessoas (6.3 - Conscientização, educação e treinamento em segurança da informação);
- processos (6.4 - Processo disciplinar);
- tecnologia (5.23 - Segurança da informação para uso de serviços em nuvem).

61 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net

Após uma breve explanação, cabe mencionar que a Alta Gestão deve auxiliar, avaliar e aprovar a implementação de Segurança da Informação de acordo com os gaps apontados nos capítulos anteriores e trazidos no plano de ação. Somente assim a empresa poderá garantir que está no caminho certo em termos de segurança da informação e proteção de dados pessoais.

4.3 ANÁLISE DO PROCESSO DE ADMISSÃO/CONTRATAÇÃO

Priscila Silva Ribeiro[62]

O processo de seleção de empregados envolve significativo tratamento de dados pessoais, assim como de dados pessoais sensíveis dos candidatos. Assim, imperiosa a observação dos escritórios de advocacia sobre os ditames da Lei quando se inicia o processo de contratação.

Ou seja, os cuidados ao tratar os dados dos candidatos a uma vaga de trabalho devem ser intensificados, melhorados e aprimorados, de modo a atender aos ditames da nova lei.

Ressalta-se que todos os dados fornecidos pelos candidatos com o objetivo de preencher uma vaga de trabalho, seja por meio de currículos impressos ou mesmo por meios digitais, em sites próprios dos escritórios ou terceirizados em outras plataformas, passam a ser de responsabilidade de quem os coleta. Assim, devem ser observadas as disposições contidas na LGPD desde a fase pré-contratual.

Ademais, no caso de necessidade de preenchimento de formulários e fichas de seleção pelos candidatos, faz-se indispensável a observação quanto aos dados exigidos e a sua finalidade de modo a proceder com as devidas alterações em caso de excesso.

Mesmo em momento anterior à vigência da Lei em análise, a coleta de alguns dados e informações de candidatos e empregados já se fazia temerária. Porém, após a sua vigência, o cuidado e a revisão de procedimento passam a ser obrigatórios.

Os contratantes devem rever a finalidade ao solicitar informações dos candidatos, tais como orientação sexual e opção religiosa, as quais se mostram excessivas ao fim pretendido, nas maiorias dos casos.

62 *Data Protection*. Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPCPD pela Legal Ethics and Compliance. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

A revisão se faz imprescindível a fim de ser respeitado os ditames contidos no artigo 6º do diploma legal. O qual determina a observância da coleta de dados sempre nos limites da finalidade, adequação e necessidade, senão vejamos:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (BRASIL, 2019).
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. (BRASIL, 2019)[63]

Assim, sempre deve ser realizado por parte dos contratantes a ponderação quanto à finalidade específica que respalda a coleta do dado; se o dado atende à finalidade objetivada, assim como se não foram cometidos excessos no procedimento.

Ultrapassado o momento de seleção do candidato, estabelecida a relação contratual, a coleta, recepção, armazenamento e retenção de dados pessoais dos empregados se faz imprescindível e é inerente ao vínculo empregatício constituído, de modo a cumprir as obrigações principais e acessórias ao contrato de trabalho. Cita-se, a título de exemplo, a contribuição para o INSS e o depósito em conta vinculada do FGTS.

63 BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Dispõe sobre a Proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências.

Quanto aos empregados que compõem o quadro do escritório, é importante que se faça a análise dos dados anteriormente coletados, a fim de conferir se houve a coleta em conformidade aos limites legais.

Do mesmo modo é necessário elaborar termos aditivos para os empregados, a fim de que o tratamento ocorra integramente em conformidade ao disposto em Lei.

Outro ponto de extrema importância a ser observado diz respeito à finalidade específica. O dado pessoal fornecido pelo empregado para atender a uma finalidade não pode ser utilizado de outra forma, se expressa a autorização do titular.

Apenas de modo a ilustrar uma situação frequente ocorrida no âmbito laboral sobre o tema, encontra-se o do empregado que fornece seu endereço a fim de obter o vale-transporte. O mesmo colaborador, no entanto, pode recusar a utilização do dado para outra finalidade, como receber um brinde em sua casa em virtude do seu aniversário. No exemplo mencionado, seria necessária uma autorização específica do empregado, a fim de que o dado em questão fosse utilizado com finalidade diversa da existente originalmente e para atividade totalmente prescindível ao vínculo empregatício.

Outro tema bastante controvertido quando se aborda a Lei Geral de Proteção e as relações laborais diz respeito à necessidade de coleta do consentimento do empregado para o tratamento de dados. Considerando a especificidade das relações laborais e as obrigações inerentes ao vínculo empregatício, o consentimento apenas será utilizado quando não houver prejuízo à sua regular constituição.

Porém, mesmo quando utilizado o consentimento, deve se observar estritamente o preceituado no artigo 5º, XII, da LGPD, vejamos:

> **Art. 5º** Para os fins desta Lei, considera-se:
> **(...)**
> **XII -** consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com

> o tratamento de seus dados pessoais para uma finalidade determinada; (BRASIL, 2019).[64]

Assim, a fim de que os escritórios estejam completamente respaldados, caso optem por obter o consentimento do empregado para o tratamento de algum dado pessoal, importante observar também os ditames contidos no artigo 8º, caput e §1º, da LGPD, *in verbis:*

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.[65]

Para o caso de dados tornados manifestamente públicos pelo titular de dados, conforme preceitua o artigo 7º, §4º da Lei, é dispensada a obtenção do consentimento. Todavia, mesmo nesta situação, o §3º do mesmo artigo de Lei enuncia que a finalidade, boa-fé e interesse público devem ser observados, assim como o seu §6º.

Sobre o consentimento, caso este seja a única base legal para o tratamento de algum dado específico, é essencial que o empregador tenha ciência sobre a possibilidade de sua revogação a qualquer momento pelo empregado, como determinado pelo §5º do artigo 8º da Lei, o que deve ser respeitado.

No aspecto laboral, outro importante ponto a ser considerado diz respeito à coleta de biometria para fins de registro da jornada de trabalho. Todavia, sendo esta modalidade comum e praticada, o

64 BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Dispõe sobre a Proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências.

65 BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Dispõe sobre a Proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências.

tratamento estaria abarcado pelo cumprimento de obrigação legal pelo controlador, conforme preceituado no artigo 11, II, a, da LGPD, não existindo motivos para rever atitudes neste aspecto.

De uma análise atenta da Lei, verifica-se que a informação sobre filiação sindical, prevista no artigo 5ª, II, é considerada dado pessoal sensível, e, dessa forma, os empregadores devem ter bastante cuidado com esta informação.

Ainda, no decorrer do pacto laboral, é imprescindível que o empregador observe aos demais incisos do artigo 6º da Lei Geral de Proteção de Dados, tais como segurança da informação, qualidade dos dados, transparência, mesmo nas relações de trabalho, devendo estar apto a cumpri-las, senão vejamos:

> Artigo 6º
> (...)
> V - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da 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. (BRASIL, 2019)[66]

Adverte-se, ainda, que a extinção do pacto laboral não encerra a obrigação de quem emprega no tocante ao armazenamento dos dados pessoais até então coletados.

Em certas circunstâncias, o escritório pode ser demandado a comprovar *a posteriori* o cumprimento de obrigação, de forma judicial ou administrativa, o que impõe o armazenamento de documentos pelos prazos legais cabíveis, como medida de cautela. Entretanto, após o seu transcurso, é importante que seja realizado o seu devido e regular descarte, conforme preceituado em Lei.

Ponto de extrema controvérsia e cautela por parte dos empregadores diz respeito à solicitação da certidão de antecedentes criminais dos candidatos. Mesmo em casos em que a apresentação do documento seja obrigatória, em virtude de imposição legal, ou pela natureza da função, faz-se imprescindível que o contratante tenha um processo de seleção padronizado, ainda que este seja realizado por empresas terceirizadas.

A imperativa quanto a seguir o mesmo procedimento para todos os candidatos concorrentes a uma mesma vaga, objetiva que seja a vedada qualquer tipo de discriminação ou violação a isonomia.

Ainda, deve ser ressaltado o teor do artigo 1ª, da Lei 9.029/95, que prevê a proibição de práticas discriminatórias nas relações de trabalho, transcreve-se:

66 BRASIL. Lei nº 13.853, de 8 de julho de 2019. Dispõe sobre a Proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências.

> Art. 1º É proibida a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, reabilitação profissional, idade, entre outros, ressalvadas, nesse caso, as hipóteses de proteção à criança e ao adolescente previstas no inciso XXXIII do art. 7º da Constituição Federal. (Brasil, 1995)[67]

A exigência de certidão de antecedentes criminais foi objeto de decisão vinculante do Tribunal Superior do Trabalho (TST), no julgamento do Recurso Repetitivo RR 243000-58.2013.513.0023, com a fixação da tese jurídica prevalecente nº01.

No julgamento da tese acima mencionada, foi definido que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais, em virtude da existência de lei, natureza do ofício ou elevado grau de fidúcia, tema 01, vejamos:

> I) não é legítima e caracteriza lesão moral a exigência de Certidão de Antecedentes Criminais de candidato a emprego quando traduzir tratamento discriminatório ou não se justificar em razão de previsão de lei, da natureza do ofício ou do grau especial de fidúcia exigido. Vencidos parcialmente os Exmos. Ministros João Oreste Dalazen, Emmanoel Pereira e Guilherme Augusto Caputo Bastos; II) a exigência de Certidão de Antecedentes Criminais de candidato a emprego é legítima e não caracteriza lesão moral quando amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos ou deficientes (em creches, asilos ou intuições

67 BRASIL. Lei nº 9029 de 1995. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências.

> afins), motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas, entorpecentes e armas, trabalhadores que atuam com informações sigilosas. Vencidos parcialmente os Exmos. Ministros Augusto César de Carvalho, relator, Aloysio Corrêa da Veiga, Walmir Oliveira da Costa e Cláudio Mascarenhas Brandão, que não exemplificavam; III) a exigência de Certidão de Antecedentes Criminais, quando ausente alguma das justificativas de que trata o item II, supra, caracteriza dano moral in re ipsa, passível de indenização, independentemente de o candidato ao emprego ter ou não sido admitido. Vencidos, parcialmente, os Exmos. Ministros João Oreste Dalazen, Emmanoel Pereira e Guilherme Augusto Caputo Bastos e, totalmente, os Exmos. Ministros Aloysio Corrêa da Veiga, Renato de Lacerda Paiva e Ives Gandra Martins Filho.

Dessa forma, os cuidados quanto à solicitação deste documento devem ser os mesmos praticados antes mesmo da vigência da LGPD. Todavia, tratando-se de relações laborais, as dúvidas podem ser sanadas com respaldo Lei Trabalhista, nas disposições constitucionais, assim como na jurisprudência do próprio Tribunal Superior do Trabalho.

4.4 ANÁLISE DOS CÓDIGOS INTERNOS OU MANUAL DO COLABORADOR

Alessandra C. Puig Casariego[68]

A LGPD (Lei Geral de Proteção de Dados) visa proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei dispõe sobre o tratamento de dados realizado por pessoa física ou jurídica de direito público ou privado e contempla um extenso conjunto de operações efetuadas em meios físicos ou digitais.

Nesse contexto, tendo como objetivo proteger os dados pessoais dos cidadãos, incluindo aqueles que são coletados e processados pelas empresas, é essencial que as empresas se atentem às diversas questões relativas ao tratamento desses dados.

Um ponto muito importante se refere à necessidade da empresa se certificar de que os dados pessoais dos funcionários e colaboradores estão sendo tratados em consonância com as diretrizes da LGPD. Isso inclui garantir que as informações coletadas sejam estritamente necessárias para a execução das atividades laborais, que sejam armazenadas de forma segura e que o acesso a elas seja limitado apenas a pessoas autorizadas, sem prejuízo da necessária definição quanto ao ciclo de vida desses dados.

A empresa deve também fornecer treinamentos e orientações periódicas e contínuas aos funcionários e colaboradores para garantir que eles estejam cientes das políticas de privacidade da empresa e

68 Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG. Membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas - FGV. Master of Business Administration - MBA em Advocacia Corporativa e Governança pela Escola Superior da Advocacia - ESA OAB. Pós-graduação em Direito Bancário pela Fundação Getúlio Vargas - FGV. Certificação em Compliance pela KPMG. Certificação em Investigações Corporativas pela KPGM. Curso de Extensão em Lei Geral de Proteção de Dados pela PUC-RS.

saibam como lidar com informações sensíveis, bem como tomar medidas para garantir a segurança e proteção dos dados.

Adicionalmente, faz-se necessário disponibilizar políticas e normativos internos sobre o tema. Ainda, estabelecer as diretrizes da segurança e proteção dos dados no Código de Ética da empresa reflete uma boa prática para garantir um resultado eficaz para a conscientização dos funcionários e colaboradores.

O Código Interno ou Manual do Colaborador deve conter, minimamente, a seguinte estrutura de tópicos:

1. Abrangência
2. Objetivos
3. Revisão e Atualização do Código Interno ou Manual do Colaborador
4. Papéis e Responsabilidade
5. Definições e Diretrizes
6. Questões relativas ao Tratamento de Dados Pessoais
7. Direitos dos Titulares de Dados Pessoais
8. Segurança e Sigilo de Dados
9. Sanções e Penalidades

Recomenda-se, ainda, que os colaboradores e destinatários desse documento assinem um "Termo de ciência e compromisso", relativo ao conteúdo nele disponibilizado, o que deve ser exigido a cada atualização.

Portanto, estabelecer diretrizes e orientações sobre segurança e proteção dos dados por meio de códigos internos, políticas, código de ética ou manual do colaborador é um passo importante para que a empresa esteja em conformidade com a LGPD e possa proteger de forma efetiva os dados pessoais que realiza o tratamento.

4.5 ANÁLISE DE CONTRATO DE TERCEIROS (PARCEIROS E FORNECEDORES)

Carlos Henrique Almeida Salgado[69]

A Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório sobre o tratamento de dados pessoais, tendo como um de seus princípios basilares pilares a segurança e a prevenção, previstos nos incisos VII e VIII, do art. 6º da Lei. Sendo, portanto, fundamental a todos os agentes de tratamento, adotar medidas técnicas e administrativas suficientes para proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, compartilhamento indevido de dados, bem como criar instrumentos e mecanismos para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.[70]

Essas medidas podem ser instrumentalizadas de diversas formas internamente, por meio de políticas e procedimentos internos que estabelecerão regras e padrões para certificar a segurança dos dados pessoais tratados pela empresa.

No entanto, não basta que o controlador ou o operador apliquem apenas mecanismos protetores internos, é necessário que a segurança e prevenção sejam instrumentalizadas em relações comerciais com terceiros, principalmente com aqueles cuja contratação envolver o tratamento de dados pessoais

A verificação do histórico de integridade dos terceiros que se relacionam com a empresa é um dos principais elementos para

69 Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP e Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

70 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 mar.2023.

se demonstrar a efetividade de um programa de conformidade. A execução sistemática e adequada dessa verificação permite evitar e mitigar riscos para o negócio no relacionamento com terceiros.[71]

Nas relações comerciais, é muito importante realizar a gestão de terceiros e adequar os processos internos com as determinações estabelecidas na LGPD. As empresas devem atuar em conformidade com a lei em todas as fases de do negócio, desde a negociação até a finalização da prestação dos serviços, mas, principalmente, no momento da formalização do contrato, por isso é imprescindível que os contratos com terceiros, fornecedores, prestadores de serviços e parceiros de negócios sejam analisados pelas formas, de forma que sejam verificados os dados que serão tratados no âmbito daquela relação e inseridas as cláusulas necessárias e adequadas para cada tipo de relação comercial.

A gestão de terceiros pode ser realizada desde a fase pré-contratual, por meio da aplicação do "Questionário de Maturidade", conforme já abordado no capítulo X. A partir da fase contratual, a empresa na figura de controlador dos dados, deverá realizar a análise do instrumento contratual, de forma a proteger os dados pessoais tratados por meio de instrumentos jurídicos próprios, firmando com seus fornecedores e parceiros de negócios aditivos contratuais aos contratos de prestação de serviços ou inserindo cláusulas especificas no próprio instrumento analisado, de forma a deixar expressas as condições e os limites para a realização de cada atividade de tratamento realizada pelas partes.

O art. 46 da LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, sendo, portanto, obrigação legal da empresa, seja como controladora ou operadora dos dados pessoais, realizar essa análise de forma minuciosa e fundamentada do instrumento que regerá aquele negócio, inserindo, nos contratos celebrados com terceiros prestadores de serviços, cláusulas que

71 FRANCO, Isabel. Guia prático de compliance / organização. – 1. ed. – Rio de Janeiro: Forense, 2020.

regulem a privacidade dos dados pessoais envolvidos na relação contratual e demais informações necessárias para garantir a proteção dos dados pessoais dos titulares. [72]

Além das disposições gerais acerca da proteção de dados pessoais, deverão ser previstos expressamente o fluxo de tratamento dos dados pessoais e as orientações claras acerca da forma que deve ocorrer o tratamento desses dados. O contrato deve conter o inventário de todo o tratamento de dados realizados entre as partes, a estrutura da segurança dos dados utilizada, tanto pelo controlador quanto pelo operador, a conduta das partes diante de solicitações apresentadas pelos titulares; o período de retenção e guarda dos dados compartilhados e o procedimento adequado para descarte após finalizada a relação contratual.

Os contratos devem dispor sobre medidas de segurança que deverão ser adotadas, bem como prazos para descarte dos documentos que contenham dados pessoais após o atingida a finalidade correlata ao tratamento daquele dado pessoal. O compartilhamento dos dados pessoais entre as partes também deve ser tratado com cautela neste instrumento.

O art. 42 da LGPD dispõe que o agente de tratamento, que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, estabelecendo a responsabilização solidária entre o controlador e o operador em situações de exposição e incidentes de segurança. [73]

Dessa forma, os contratos entre as empresas deverão ter cláusulas especificando as condições e obrigações de cada agente de tratamento quanto aos dados compartilhados, delimitando, no que for possível, a responsabilidade de cada parte, relativas à privacidade e

72 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 mar.2023.

73 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 mar.2023.

proteção de dados e principalmente, as condutas que cada uma das partes deve adotar em caso de incidentes de segurança que envolvam dados pessoais. Isso permitirá a identificação do responsável em caso de um incidente de segurança, para que sejam aplicadas as cláusulas de responsabilidade previstas nos contratos celebrados.

É importante que esteja prevista no documento a possibilidade de implantar trilhas de auditoria sistêmicas que permitam a identificação de autoria do integrante da equipe de terceirizada contratada quanto aos acessos às bases de dados ou que revelem desvios de finalidade do tratamento de dados pessoais, bem como a integridade dos registros eletrônicos correlatos. Isso é fundamental para comprovar, em caso de ocorrência de incidente envolvendo o tratamento de dados pessoais, ter se tratado de culpa do terceiro (na figura de operador), e não da empresa (como controladora de dados).

Em suma, as disposições referentes que precisam conter nos contratos fornecedores são as seguintes: I) Definições e conceitos da LGPD (art. 5º); II) Referência aos princípios da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6); III) Base legal (art. 7º, I a X); IV) Possibilidade ou não de compartilhamento pelo operador (art. 7º, §5º); V) Referência sobre gestão de consentimentos (art. 8º e 9º); VI) Indicação de canal de comunicação aos titulares. Direitos dos titulares e livre acesso aos dados tratados (art. 9º); VII) Indicação de canal de comunicação aos titulares. Direitos dos titulares e livre acesso aos dados tratados (art. 9º); VIII) Cláusula geral que contemple a forma de coleta, tratamento e proteção de dados pessoais (art. 9º, II); IX) Definição de término de tratamento e formas de eliminação dos dados (art. 15º e 16º); X) Cláusula que informe e/ou assegure os direitos dos titulares de dados pessoais (art. 18º); XI) Indicação de canal de comunicação aos titulares de dados pessoais (art. 41º, § 1º); XII) Transferência internacional de dados (art. 33º, IX); XIII) Previsão sobre atividades de tratamento definidas pelo controlador que serão realizadas pelo operador (art. 39º); XIV) Definição expressa

de qual empresa exercerá as funções de controlador e de operador (art. 39º); XV) Previsão de elaboração de relatório de impacto (art. 38º); XVI) Indicação do encarregado de dados do controlador (art. 41º); XVII) Requisitos de segurança, boas práticas e governança no relacionamento entre partes envolvidas (art. 46º); XVIII) Comunicação de incidentes de segurança ao controlador (art. 48º); XIX) Previsão do monitoramento fiscalização das atividades do controlador que serão realizadas pelo operador (art. 46º); XX) Previsão de procedimentos claros e específicos de regras de boas práticas, incluindo atendimento aos direitos dos titulares (art. 50º e 51º); e principalmente, XXI) Delimitação de responsabilidade controlador/operador e direito de regresso (art. 42).[74]

Analisando adequadamente os contratos formalizados com terceiros e inserindo cláusulas específicas relacionada aos dados pessoais tratados em cada relação contratual, os controladores e operadores estarão resguardados em face de questionamentos de titulares, entes parceiros e agentes fiscalizadores, quanto aos padrões exigidos pela LGPD na análise de riscos relativos à privacidade à proteção dos dados pessoais dos titulares compartilhados com seus parceiros de negócios.

74 BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em 02 mar.2023.

4.6 ANÁLISE DE CONTRATO DE CLIENTES (PF/PJ)

Elaine Cristina Oliveira Guerra[75]

O propósito da análise de contratos de clientes, sejam eles pessoas físicas ou jurídicas, em relação à privacidade e à proteção de dados, vai além de simplesmente proteger a empresa em questões judiciais. Envolve também a verificação do cumprimento dos requisitos estabelecidos pela Lei Geral de Proteção de Dados.

É responsabilidade da empresa fornecer transparência ao cliente quanto à forma como ela lida com os dados pessoais. Isso implica o dever de a empresa demonstrar o ciclo de vida dos dados/informações: como a empresa coleta, trata, compartilha, localização (se no Brasil ou no exterior), as medidas de segurança para proteger esses dados.

No que diz respeito à prática e ao projeto, deve-se fazer uma minuciosa revisão de cada cláusula do contrato, identificando lacunas e questões a serem abordadas com o cliente, conforme apresentado na tabela sugerida abaixo.

75 Especialista em Direito, Inovação e tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados - ISFS), Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora do "Manual Prático de Adequação à LGPD com enfoque nas Relações do Trabalho". Autora de capítulos de livros jurídicos. Empresária em projetos de adequação e implementação da LGPD. Atuante com projetos de DPO as a Service. Mentora em projetos de adequação e implementação da LGPD. Palestrante em Privacidade e Proteção de dados. Diretora do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pesquisadora da USP/SP. Advogada.

INSTRUMENTOS ANALISADOS: (Descrever o tipo de contrato/termo que você está revisando para o cliente)			
QUEM – Cliente/Fornecedor/Colaborador entre outros	FINALIDADE	GAPS	RECOMENDAÇÕES/ INCLUSÃO DE CLÁUSULAS (LGPD)

É importante ressaltar que a conformidade com a LGPD não se limita apenas às cláusulas contratuais, mas também envolve a implementação de medidas técnicas de segurança.

4.7 LGPD NA PROPOSTA TÉCNICA E COMERCIAL

Elaine Cristina Pereira dos Santos Nery[76]

As Organizações elaboram e recebem diariamente propostas técnicas e comerciais.

A princípio, este é um dos meios de entrada de dados pessoais de possíveis clientes da Organização.

Dessa forma, é extremamente importante que se tenham cláusulas claras e objetivas sobre o ciclo de vida dos dados pessoais, ou seja, como é realizada a coleta, como são processados, de que forma esses dados são classificados, como são utilizados, por quem são acessados, se há realização de compartilhamento, como são arquivados/armazenamento e qual a forma de eliminação.

Essas são algumas perguntas que devem ser respondidas antes da elaboração de quaisquer propostas técnicas e comerciais.

A LGPD não veio para inviabilizar quaisquer negócios, ela veio para dar transparência para o titular dos dados pessoais. Por isso, é extremamente importante iniciar os seus serviços com as cláusulas sobre privacidade e proteção dos dados.

A proposta comercial, ao ser elaborada, deve enfatizar a necessidade do tratamento dos dados pessoais coletados como forma de viabilizar a negociação do preço de serviço e atender à legislação aplicável, caso contrário, o propósito do contrato de prestação de serviço resta prejudicado.

Além disso, é importante destacar que os dados pessoais do titular serão armazenados em local seguro e apropriado. A estes se poderá ter acesso à cópia, mediante termo de requerimento, bem como a exercer

76 Advogada. Especialista em Direito Público. Especialista em Privacidade e Proteção de dados. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão de Proteção de Dados do Estado (OAB/MG), Membro da Comissão de Proteção de Dados da Universidade Federal dos Vales do Jequitinhonha e Mucuri- UFVJM.

seus direitos previstos no artigo 18 da Lei nº 13.709/2018 (LGPD), resguardando-os no tocante ao sigilo e à segurança das informações.

A título prático, segue um pequeno texto parada do cliente.

> A empresa XXXX coleta e processa seus dados pessoais nesta proposta comercial com base no artigo xxx, inciso xxx da LGPD. Seus dados pessoais serão coletados especificamente para XXXXX e serão armazenados de forma segura e adequada pelo período de XXXX, garantindo o sigilo e a segurança das informações.
>
> Nossa empresa não realiza transferências internacionais de dados, ou, nossa empresa realiza transferência internacional de dados para o seguinte país XXXXX.
>
> Como titular de dados pessoais, você tem o direito de acessar suas informações, mediante solicitação por meio de um termo específico, conforme previsto no artigo 18 da Lei nº 13.709/2018 (LGPD). Para isso, basta entrar em contato conosco por meio do nosso canal de privacidade em XXXXXX. (Texto do autor do capítulo).

4.8 CARTA LGPD – CONTROLADORES – OPERADORES - CLIENTE

Emily Matias Assumpção[77]

A Lei Geral de Proteção De Dados – LGPD, em seu art. 6º, discorre sobre os princípios relativos às atividades de tratamento:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos

77 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

> agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da 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.
> Desse modo, obedecendo ao supracitado artigo, é importante que as empresas que realizem o tratamento de dados pessoais, haja de acordo com a finalidade, transparências e demais princípios da LGPD.

Para tanto, é recomendado que se envie aos controladores, operadores e clientes, uma carta ou informativo com o objetivo de dar transparência sobre o processo de adequação à LGPD, bem como garantindo que os princípios e demais imposições do normativo legal serão respeitados e obedecidos.

O referido informativo, além de trazer segurança jurídica, demonstra boa-fé no processo de adequação à LGPD e se trata de uma boa prática.

Para melhorar o entendimento, segue abaixo *template* elaborado para ser enviado em forma de carta/informativo para controladores, operadores e clientes:

Informativo do Escritório XYZ

Prezados clientes e prestadores de serviços (controladores e operadores)

O Escritório XYZ, inscrito no CNPJ nº XXXXXXXXXXXXXX, declara estar no processo de conformidade com a Lei Geral de Proteção de Dados (Lei nº13.709/2018), declara ainda que realiza o tratamento dos dados pessoais dentro dos limites legais, com a adequada segurança destes dados pessoais, indicando a finalidade destes e se compromete no que lhe compete a realizar das melhores formas e práticas, a garantia da privacidade no tratamento dos dados pessoais.

É de responsabilidade dos controladores e operadores realizarem o tratamento dos dados pessoais, de acordo com as diretrizes impostas LGPD.

Asseguramos aos titulares (clientes) que não envidaremos esforços para cumprir e assegurar todos os direitos dispostos na Lei.

Nosso setor de proteção de dados, em conjunto com o Encarregado de Dados, estabeleceu um canal de comunicação aberto por meio do e-mail: escritorioxyz@lgpd.com.br ou escritórioxyz@dpo.com.br.

4.9 AVALIAÇÃO DE ATENDIMENTO À LGPD POR FORNECEDORES

Gabriel Campos Cunha[78]

Sob a luz da LGPD, as organizações precisam estar atentas à sua cadeia de fornecimento visando à mitigação de riscos quanto à violação do direito à privacidade e proteção de dados pessoais.

Nas relações contratuais, em diferentes níveis de complexidade, volume e centralidade quanto ao objeto contratual, dados pessoais sempre fluirão entre as partes. Nesse contexto, os agentes de tratamento (contratante e contratada) assumirão papéis, seja como controladores, seja como operadores.

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade desse tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais[79]. Geralmente essa posição é ocupada pelos contratantes.

Já o operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada[80]. Neste caso, a posição contratual é geralmente ocupada por operadores.

Algumas das responsabilidades pelo tratamento de dados pessoais estão dispostas nos art. 42 a 45 da LGPD, os quais destacamos:

78 Advogado, consultor em Governança Corporativa, ESG, Compliance, Integridade, Proteção de Dados. Auditor de Sistemas De Gestão da Qualidade, Meio Ambiente, Saúde e Segurança do Trabalho. Auditor da Conformidade Legal nos temas de Proteção de Dados, Privacidade, Meio Ambiente e Saúde e Segurança do Trabalho.

79 Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, consultado dia 09/04/2023 em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

80 Op. cit.

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - Que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.
Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
I - O modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;

> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.
> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Portanto, avaliar os fornecedores quanto ao atendimento à LGPD antes de firmar um contrato, com o objetivo de garantir que este cumpra as obrigações legais e regulatórias necessárias para o negócio, é uma importante ferramenta para a mitigação de riscos inerentes ao tratamento de dados pessoais.

É recomendável que, de acordo com a complexidade, volume, sensibilidade e finalidade do tratamento dos dados pessoais no cumprimento do objeto contratual, haja uma gradação de risco do contrato quanto a potenciais impactos a direitos inerentes à privacidade e proteção desses dados. Proporcionalmente, no que se refere aos riscos atribuídos ao contrato de fornecimento, as avaliações de fornecedores devem ser mais ou menos aprofundadas, justificando-se, em alguns casos, processo de auditoria nos terceiros contratados.

Para a avaliação de fornecedores devem ser observados desde a política de privacidade, medidas de segurança adotadas até a reputação do contratado quanto ao tema.

A avaliação de fornecedores, portanto, é um processo essencial para garantir que a empresa esteja em conformidade com a LGPD e proteja os dados pessoais dos seus clientes e usuários e evite riscos legais quanto aos descumprimentos de direitos dos titulares.

5

IMPLEMENTAÇÃO/ GOVERNANÇA

5.1 IMPLEMENTAÇÃO DE CONTROLES DE SEGURANÇA

Adiel Ribeiro[81]

O objetivo da implementação dos controles é auxiliar para que os processos da empresa sejam seguidos e auditáveis. A título de exemplo, se existe um processo que determina que informações X sejam acessíveis apenas pelo grupo X, então deve haver controles que restrinjam este acesso para este grupo apenas.

Os controles, podem ser, entre outros, por meio de:

- Usuário e senha;
- Firewall;
- Criptografia;
- Segmentação de redes;

Explicando de forma prática: Os controles devem prevenir e caso haja um acesso não autorizado eles devem ser capazes de detectar e possibilitar a tomada de decisão pelo time de Segurança da empresa, conforme sugerido pela ISO 27002:2022 – item 5.26 - Resposta a incidentes de segurança da informação.

Tais controles também devem garantir a integridade e a disponibilidade da informação.

Além da norma ISO já citada acima, ainda existe a metodologia de Segurança da Informação NIST SP 800-53, que fornece uma lista completa e bem detalhada a respeito da implementação de controles de Segurança para a proteção de sistemas e dados.

Por fim, faz-se necessária a implementação de controles para garantir a segurança dos processos definidos pela empresa, de acordo com o seu negócio e os requisitos de Segurança da Informação e Proteção de Dados Pessoais, que envolvem entre outros:

81 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net

- Regulamentação do setor;
- Contratos;
- Leis;
- Acordos.

5.2 REVISÃO DE CONTRATOS E A IMPORTÂNCIA DA ELABORAÇÃO DE ADITIVOS PARA SE ADEQUAR À LGPD

Aline Pelet Teles de Menezes

Com o advento da LGPD é primordial que as empresas se preocupem com a adequação de toda a documentação que transita internamente e externamente. Os contratos são documentos essenciais nesse processo, pois há coleta de inúmeros dados das partes, não só na qualificação, mas, a depender do tipo do contrato, são coletados dados de terceiros, dados de saúde, dados de crianças e adolescentes, entre outros.

O controlador, ao analisar as cláusulas contratuais e os padrões utilizados na rotina da empresa, deve incluir cláusulas de proteção de dados, demonstrando sua preocupação com os dados que circulam em toda a cadeia organizacional e comercial. Com relação aos contratos vigentes, é imprescindível que haja um mapeamento dos contratos existentes para identificar as diversas área que podem envolver a coleta e tratamento de dados. E, a partir desse mapeamento, devem ser elaborados aditivos com cláusulas de adequação à LGPD, podendo dividir, de maneira geral, os contratos de acordo com as partes qualificadas, sendo as principais: fornecedores, clientes e colaboradores.

Os contratos que envolvem fornecedores e clientes precisam de atenção especial, ainda na fase pré-contratual, pois é recomendável que se faça uma *due-diligence* para verificar se a parte está atenta às mudanças trazidas pela Lei 13.709/18. Deve-se verificar se há política de privacidade, se o cliente ou forncedor possui a preocupação com a coleta de dados internamente, se possui um programa efetivo quanto à proteção de dados pessoais. Verificadas essas questões, ou ainda, quando o fornecedor ou cliente já é um parceiro antigo do controlador, deve-se elaborar um aditivo que contemple cláusulas de consentimento, confidencialidade, responsabilidade e principalmente, como as partes tratam o incidente de segurança.

Além disso, quando o contrato abrange dados pessoais específicos, como por exemplo, um contrato de plano de saúde, é importante que o documento contenha cláusula informando a finalidade de coleta e tratamento dos dados, bem como, as sanções que as partes podem sofrer no caso de vazamento desses dados.

Os contratos de colaboradores também devem conter cláusulas gerais de responsabilidade, consentimento e as sanções para cada parte, na eventualidade de um incidente de segurança. O controlador também deve observar aqueles dados que precisa coletar em razão de cumprimento de obrigação legal, para alimentação dos sistemas de órgãos públicos como e-social e e-cac, documentos contábeis e financeiros, informações que são relacionadas em cálculos de impostos e tributos.

É essencial que o controlador informe inclusive o prazo de armazenamento de dados de funcionários, sobretudo, após o encerramento do vínculo empregatício.

5.3 CONSENTIMENTO

Priscila Silva Ribeiro[82]
Renato Almeida Viana[83]

Como se sabe, a Lei 13.853/2019, Lei Geral de Proteção de Dados Pessoais, LGPD (BRASIL, 2019), tem como fundamento a proteção de direitos e garantias fundamentais. Nesse contexto, para que o dado pessoal possa ser adequadamente tratado, deverá haver o enquadramento em uma das 10 bases legais previstas no art. 7º da LGPD.

O consentimento do titular do dado pessoal é uma das bases legais previstas em Lei, elencada no inciso I, do artigo acima referenciado, a qual se encontra definida no art. 5º, XII, do mesmo diploma legal.

Esta base legal consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" e deve ser obtida de forma prévia ao tratamento do dado.

Dessa forma, constata-se que para o consentimento do titular do dado possa ser considerado válido é preciso que as seguintes características estejam presentes:

- livre,
- informado,
- inequívoco e,
- para finalidade determinada.

82 Data Protection. Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPCPD pela Legal Ethics and Compliance. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

83 Coordenador do Comitê de LGPD do Centro de Estudos das Sociedades de Advogados de Minas Gerais – CESA/MG. Membro do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Escola Superior da Advocacia. Advogado.

Existe uma falsa ideia de que o consentimento do titular do dado pessoal seria a melhor base legal para lastrear o tratamento de dados do titular. Porém, seja pelo fato de que não há hierarquia entre as bases legais, seja porque o seu titular poderá revogar o consentimento a qualquer momento, não é recomendável obtê-lo caso haja outra base legal mais adequada à natureza do tratamento.

Portanto, o consentimento genérico e sem observância dos requisitos acima será nulo nos termos do art. 8º, § 4º da LGPD. Exatamente por essa razão, o Termo de Consentimento não deve ser elaborado de forma padronizada e genérica, mas, sim, individualizada, com consideração a todas as particularidades do caso, informação clara sobre quais dados pessoais serão tratados, para qual finalidade específica, por quanto tempo, entre outras.

Por fim, importante registrar que, mesmo com a obtenção do consentimento do titular, deverão ser observados os princípios previstos na LGPD, em especial, o da transparência, da necessidade, da finalidade e da adequação.

Para o caso de dados tornados manifestamente públicos pelo titular de dados, o consentimento deixa de ser obrigatório. Todavia, mesmo nesta hipótese, o dado não deve ser utilizado de maneira irrestrita. Ou seja, os direitos do titular de dados trazidos pela LGPD devem ser resguardados pelo controlador e operador de dados.

No que tange aos dados pessoais considerados sensíveis, é possível a realização do seu tratamento, em hipóteses para além do consentimento, sendo limitadas à disposição contida no artigo 11, inciso II, da LGPD (BRASIL, 2019):

> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Sobre o tema consentimento, apenas é permitido coletar dados pessoais de crianças e adolescentes quando expressamente autorizado por ao menos um dos pais ou responsável legal, conforme dispõe o artigo 14, § 1º, da LGPD (Brasil, 2019).

Apenas é permitido o tratamento de dados pessoais de crianças e adolescentes sem o devido consentimento com a finalidade contatar os pais ou o responsável legal, conforme expressamente previsto no artigo 14, § 3º, da LGPD (Brasil, 2019). Nesses casos, os dados só podem ser utilizados uma única vez e não podem ser armazenados e transferidos para terceiros sem o consentimento obrigatório.

A seguir, apresentamos um modelo básico de termo de consentimento para escritório que, como tal, deverá ser devidamente adequado à sua real necessidade.

Após uma visão holística sobre a utilização da base legal do consentimento, são sugeridos alguns tópicos que devem constar

no termo de consentimento para os clientes, colaboradores e seus dependentes:

- Quais são os dados pessoais tratados
- Qual a finalidade do Tratamento dos Dados
- Se existe o compartilhamento de Dados
- A responsabilidade pela Segurança dos Dados
- Término do Tratamento dos Dados
- Direito de Revogação do Consentimento
- Tempo de Permanência dos Dados Recolhidos

O consentimento conferido pelo titular de dados pode ser revogado a qualquer momento, mediante manifestação expressa, conforme disposição do artigo 8º, § 5º, da LGPD (BRASIL, 2019).

O consentimento é umas das bases legais mais relevantes elencadas na LGPD. Do mesmo modo a que confere o direito quanto ao tratamento de dados pessoais exclusivamente a vontade do titular. Logo, é importante que as organizações se atentem para este fato e estejam preparadas para o caso de sua revogação.

Para a utilização da base legal em análise, recomenda-se às organizações que se aprofundem na interpretação da Lei, e decidam, a partir de uma interpretação analítica, se ela é a mais adequada em cada caso e se a organização está preparada caso ocorra a revogação.

5.4 IMPLEMENTAÇÃO DE POLÍTICAS - TI

Adiel Ribeiro[84]

A implementação de políticas pode ser entendida como implementação de processos pela empresa, ela auxilia na implementação dos controles de todas as áreas da organização, bem como pode ser utilizada para regulamentar o funcionamento da empresa e o comportamento esperado dos colaboradores no dia a dia, diante das diversas situações inerentes ao negócio.

Existem diversas políticas voltadas para a segurança da empresa e a proteção de Dados Pessoais, algumas delas são:

- Segurança da Informação;
- Dispositivos Móveis,
- Segurança física/lógica,
- Procedimento de Exclusão de Dados Pessoais;
- Política de backup,
- Trabalho remoto,
- Mesa limpa e tela limpa.

A ISO 27701 contém, entre outros itens, o detalhamento de várias políticas que auxiliam na Proteção e Privacidade de Dados Pessoais.

Por fim, cada empresa deve avaliar as políticas necessárias conforme o seu ramo de atuação, levando em conta os contratos, legislação e obrigações diversas.

84 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net

5.5 CARTILHA DE RECURSOS HUMANOS E CLIENTE

Alan de Souza Pinto[85]

A Lei Geral de Proteção de Dados (LGPD) tem como objetivo proteger a privacidade dos titulares de dados pessoais e aumentar a transparência e responsabilidade das empresas em relação ao tratamento de dados. Nesse sentido, é importante que as empresas estejam em conformidade com a lei, e que seus colaboradores estejam preparados para lidar com os desafios impostos pela LGPD. Com isso, a equipe de recursos humanos, em especial, deve estar atenta às suas obrigações e à importância de garantir a proteção dos dados pessoais dos candidatos e funcionários.

A equipe de recursos humanos tem um papel fundamental na implementação da LGPD nas empresas. Ela é responsável por coletar, armazenar e processar diversos tipos de dados pessoais, como informações de candidatos a vagas de emprego, dados de funcionários e informações sobre a folha de pagamento. Por isso, é importante que a equipe de RH esteja familiarizada com as exigências da LGPD e esteja em conformidade com a lei.

Desse modo, a LGPD estabelece diversas obrigações para as empresas em relação ao tratamento de dados pessoais. A equipe de RH deve garantir que a empresa obtenha o consentimento explícito dos candidatos e funcionários para coletar e processar seus dados pessoais. Além disso, deve implementar medidas técnicas e organizacionais para garantir a privacidade dos dados pessoais e evitar vazamentos. A nomeação de um Encarregado de Proteção de Dados (DPO) é obrigatória, bem como a notificação à Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidentes de segurança.

85 Mestre em Inovação Tecnológica, pela UFMG, Bolsista CAPES; Pós-graduado em Direito Digital e Proteção de Dados, pela EBRADI; Pós-graduado em Direito Civil Aplicado, pela PUC Minas; Graduado em Direito, pela PUC Minas; Membro da Comissão de Proteção de Dados da OAB/MG; Consultor em Privacidade e Proteção de Dados Pessoais; Professor; Advogado.

Paralelamente a isso, a LGPD também reconhece diversos direitos aos titulares de dados pessoais, como o direito de acesso, correção, exclusão, oposição e portabilidade dos seus dados. Por isso, a equipe de RH deve estar preparada para lidar com essas solicitações e orientar os titulares de dados sobre como exercer seus direitos.

Nesse sentido, estar em conformidade com a LGPD é essencial para garantir a proteção dos dados pessoais dos candidatos e funcionários, além de ser uma obrigação legal que deve ser seguida por todas as empresas que coletam e processam dados pessoais. A equipe de RH tem um papel fundamental nesse processo, e deve estar preparada para atender às exigências da lei. Vale lembrar que a implementação da LGPD pode trazer benefícios para as empresas, como a melhoria da sua reputação e a construção de uma relação de confiança com seus clientes e funcionários. É importante, portanto, que a equipe de RH esteja ciente de suas obrigações e do papel que desempenha na proteção dos dados pessoais.

QUAIS SÃO OS RISCOS DO RH NÃO SE ADEQUAR À LGPD?

A não conformidade com a LGPD pode acarretar diversos riscos para o setor de Recursos Humanos (RH), nos termos do art. 52, da LGPD, tais como:

Multas e sanções:	A LGPD prevê multas para as empresas que não cumprirem suas obrigações de proteção de dados, podendo chegar a até 2% do faturamento da empresa. Além disso, a ANPD pode impor outras sanções, como a proibição do tratamento de dados pessoais.
Reputação e imagem da empresa:	A não conformidade com a LGPD pode prejudicar a imagem da empresa, afetando sua reputação no mercado e a confiança de seus clientes e funcionários. Isso pode levar à perda de negócios, de talentos e de investidores.
Responsabilidade civil e criminal:	A LGPD também prevê a responsabilidade civil e criminal em casos de violação de dados pessoais. Caso a empresa seja responsabilizada, ela pode ter que pagar indenizações às vítimas da violação.
Perda de informações importantes:	O não cumprimento da LGPD pode levar à perda de informações importantes sobre funcionários e candidatos, como dados de contato, informações financeiras e médicas, histórico de empregos e outros dados sensíveis.
Processos trabalhistas:	O não cumprimento da LGPD pode aumentar o risco de processos trabalhistas por parte dos funcionários e candidatos que tiveram seus dados violados ou não foram adequadamente informados sobre o tratamento de seus dados.

Assim, é essencial que o setor de RH se adapte à LGPD para evitar riscos jurídicos, de imagem e de perda de informações importantes. Ademais, pertinente ressaltar que a conformidade com a LGPD é uma obrigação legal e moral das empresas, que devem garantir a privacidade e a segurança dos dados pessoais de seus funcionários e candidatos.

COMO A LGPD IMPACTA O SETOR DE RH?

A Lei Geral de Proteção de Dados (LGPD) tem um grande impacto no setor de Recursos Humanos (RH), já que as empresas que lidam com informações pessoais de funcionários e candidatos devem estar em conformidade com a legislação para proteger a privacidade e os direitos dos indivíduos. Abaixo estão alguns exemplos de como a LGPD impacta o setor de RH:

Coleta e armazenamento de dados pessoais:	O RH deve garantir que os dados pessoais coletados, seja dos funcionários, seja dos candidatos, possam ser armazenados de forma segura e que as informações sejam utilizadas apenas para as finalidades específicas para as quais foram coletadas.
Compartilhamento de dados pessoais:	O RH deve garantir que as informações sejam compartilhadas apenas com os terceiros que realmente precisam acessá-las e que esses terceiros também estejam em conformidade com a LGPD.
Direito de acesso dos titulares dos dados:	Os funcionários e candidatos têm o direito de acessar seus dados pessoais e solicitar a correção, exclusão ou bloqueio de informações incorretas ou desnecessárias. O RH deve garantir que os titulares dos dados possam exercer esses direitos de forma fácil e eficaz.
Tratamento de dados sensíveis:	A LGPD estabelece regras mais rigorosas para o tratamento de dados sensíveis, como informações de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso. O RH deve garantir que o tratamento desses dados seja feito de acordo com a legislação e apenas para as finalidades específicas para as quais foram coletados.

Responsabilidade pela conformidade:	A LGPD estabelece que as empresas são responsáveis por garantir a conformidade com a legislação e pela proteção dos dados pessoais dos funcionários e candidatos. O RH deve garantir que as políticas e procedimentos estejam em conformidade com a LGPD e que os funcionários estejam cientes de suas obrigações em relação à proteção dos dados pessoais.

COMO ADEQUAR O SETOR DE RH ÀS EXIGÊNCIAS DA LGPD?

Para adequar o setor de RH às exigências da LGPD, as empresas podem seguir as seguintes etapas:

Conscientização e treinamento:	É importante que os funcionários do RH compreendam a importância da LGPD e como ela afeta o seu trabalho. Portanto, a empresa pode fornecer treinamento e conscientização aos funcionários sobre a legislação, suas implicações e responsabilidades.
Identificação de dados pessoais:	A empresa precisa identificar todos os tipos de dados pessoais que são coletados e processados pelo setor de RH. É preciso criar um inventário de dados pessoais que inclua informações sobre a finalidade da coleta, a base legal para o processamento e a duração do armazenamento.
Revisão de políticas e procedimentos:	A empresa precisa revisar as políticas e procedimentos do RH para garantir que estejam em conformidade com a LGPD. As políticas e procedimentos devem incluir diretrizes claras sobre a coleta, armazenamento e processamento de dados pessoais e como esses dados podem ser compartilhados.

Garantia da segurança dos dados:	A empresa precisa garantir a segurança dos dados pessoais coletados e armazenados pelo RH. As informações devem ser protegidas contra acesso não autorizado, alteração, divulgação ou destruição.
Atendimento às solicitações dos titulares dos dados:	A empresa deve garantir que os titulares dos dados possam exercer seus direitos sobre a LGPD, como o direito de acesso, correção e exclusão de dados pessoais. O RH deve estabelecer procedimentos para lidar com essas solicitações.
Avaliação de riscos:	A empresa deve realizar avaliações de riscos periodicamente para identificar e mitigar possíveis riscos à privacidade dos dados pessoais coletados pelo RH.

Com isso, a adequação do setor de RH às exigências da LGPD envolve um processo de conscientização, revisão de políticas e procedimentos, adequação do consentimento, segurança dos dados, atendimento às solicitações dos titulares dos dados e avaliação de riscos.

LGPD E RH NO CONTEXTO DO HOME OFFICE

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) continua a ser aplicável, mesmo em situações de trabalho remoto, e as empresas devem estar em conformidade com a lei para proteger a privacidade dos funcionários e candidatos.

Algumas das medidas que o setor de RH pode adotar para adequar-se à LGPD no *home office* incluem:

Adoção de medidas de segurança para dispositivos remotos:	O RH deve adotar medidas para proteger os dispositivos utilizados pelos funcionários no trabalho remoto, como a instalação de antivírus, *firewalls* e criptografia de dados. Além disso, a empresa deve orientar os funcionários sobre a importância de proteger suas informações pessoais e manter as senhas seguras.
Utilização de ferramentas de videoconferência seguras:	O RH deve utilizar ferramentas de videoconferência seguras para garantir que as reuniões virtuais sejam protegidas contra acesso não autorizado e que as informações compartilhadas durante as reuniões sejam criptografadas.
Acesso remoto controlado:	O RH deve garantir que o acesso remoto aos sistemas da empresa seja controlado e que apenas os funcionários autorizados possam acessar dados pessoais e informações confidenciais.
Orientação sobre as políticas de privacidade:	O RH deve orientar os funcionários sobre as políticas de privacidade da empresa e as medidas de segurança adotadas para proteger seus dados pessoais durante o trabalho remoto.
Utilização de contratos e termos de responsabilidade:	O RH pode utilizar contratos e termos de responsabilidade para estabelecer as obrigações dos funcionários em relação à proteção de dados pessoais durante o trabalho remoto, como a obrigação de manter as informações confidenciais seguras e de notificar a empresa em caso de violação de segurança.

Desse modo, o setor de RH deve adotar medidas adicionais para garantir a proteção de dados pessoais no contexto do *home office*, incluindo a adoção de medidas de segurança para dispositivos remotos, a utilização de ferramentas de videoconferência seguras, o acesso

remoto controlado, a orientação sobre as políticas de privacidade e a utilização de contratos e termos de responsabilidade.

CUIDADOS DO CLIENTE PERANTE A LGPD

Como cliente, é importante que você esteja ciente de seus direitos e das melhores práticas para manter seus dados pessoais seguros.

A seguir estão algumas boas práticas que a serem seguidas:

Leia as políticas de privacidade das empresas	Antes de compartilhar seus dados pessoais com uma empresa, certifique-se de ler as políticas de privacidade da empresa. Certifique-se de que está confortável com as informações que a empresa está solicitando e com a forma como ela pretende usar essas informações.
Mantenha suas senhas seguras	Use senhas fortes e únicas para suas contas on-line e evite usar a mesma senha para várias contas. Altere as senhas regularmente e nunca compartilhe as senhas com outras pessoas.
Não compartilhe informações pessoais sensíveis	Evite compartilhar informações pessoais, como números de documentos, senhas, informações financeiras ou de saúde, a menos que seja absolutamente necessário. Mesmo que uma empresa solicite essas informações, certifique-se de que ela tenha medidas adequadas de segurança em vigor.
Fique atento a e-mails suspeitos	Se receber um e-mail suspeito, não clique em nenhum *link* ou anexo. Verifique se o endereço de e-mail do remetente é legítimo e verifique se há erros gramaticais ou ortográficos no e-mail. Nunca compartilhe informações pessoais por e-mail, a menos que tenha certeza de que a solicitação é legítima.

Mantenha o software do computador atualizado	Manter o *software* do computador atualizado pode ajudar a garantir que o computador esteja protegido contra vulnerabilidades de segurança conhecidas. Isso inclui atualizações para o sistema operacional, navegador da *web*, *software* antivírus e outros programas importantes.
Use uma conexão segura	Ao acessar sites que exigem informações pessoais, certifique-se de que a conexão seja segura. Verifique se o endereço do site começa com "https" em vez de "http". Isso indica que a conexão é criptografada e que as informações que compartilha estão protegidas.
Fique atento a golpes de *phishing*	Golpes de *phishing* são tentativas de enganar você para fornecer informações pessoais ou financeiras. Fique atento a e-mails ou mensagens de texto que solicitam informações pessoais ou financeiras ou que solicitam que você clique em um *link*. Verifique sempre se o site é legítimo antes de compartilhar informações.

Com o aumento da quantidade de informações que são compartilhadas *on-line*, é fundamental adotar medidas de segurança para garantir que as informações pessoais permaneçam protegidas. Ao seguir as boas práticas apresentadas, o cliente protegerá seus dados pessoais contra possíveis ameaças cibernéticas, garantindo a privacidade e a segurança de informações sensíveis

Vale ressaltar que a conscientização sobre a LGPD e a adoção de boas práticas de segurança são fundamentais para manter seus dados pessoais seguros. Além disso, é importante que os clientes fiquem atentos a possíveis ameaças à sua segurança e denunciem atividades suspeitas às autoridades competentes. Por isso, proteger seus dados pessoais é um direito e uma responsabilidade de todos, e seguir as boas práticas de segurança cibernética é essencial para garantir a privacidade e a segurança dos dados pessoais.

O setor de RH é uma das áreas mais afetadas pela LGPD, uma vez que coleta e processa muitos dados pessoais de funcionários e candidatos. Para se adequar às exigências da LGPD, o RH deve adotar uma abordagem proativa e sistemática, estabelecendo políticas e procedimentos claros e seguros para o tratamento desses dados.

Uma das principais medidas que o setor de RH pode adotar para se adequar à LGPD é a conscientização dos funcionários sobre a importância da proteção de dados pessoais e a necessidade de se adaptar às exigências da lei. Além disso, é importante que o RH identifique todos os dados pessoais que são coletados e processados e estabeleça políticas e procedimentos claros e seguros para o tratamento desses dados, garantindo que as solicitações dos titulares dos dados sejam atendidas.

No contexto do *home office*, o setor de RH também precisa adotar medidas adicionais para garantir a proteção de dados pessoais, incluindo a adoção de medidas de segurança para dispositivos remotos, a utilização de ferramentas de videoconferência seguras, o acesso remoto controlado, a orientação sobre as políticas de privacidade e a utilização de contratos e termos de responsabilidade.

Nesse sentido, a LGPD traz novos desafios para o setor de RH, mas também oferece oportunidades para melhorar as práticas de privacidade e segurança de dados nas empresas. A adoção de medidas de proteção de dados pessoais pode ajudar a fortalecer a confiança dos funcionários e candidatos nas empresas e evitar possíveis sanções e prejuízos financeiros e de imagem.

Paralelamente a isso, vale destacar também que a LGPD estabeleceu regras claras para empresas em relação ao tratamento e proteção de dados pessoais, mas também como sendo de responsabilidade também do cliente adotar medidas de segurança para garantir que suas informações estejam protegidas. Por meio das boas práticas de utilização de e-mail e computador apresentadas nesta cartilha, o cliente pode reduzir os riscos de possíveis ameaças, além de garantir a privacidade e a segurança de suas informações pessoais.

Com isso, ao seguir essas boas práticas, o cliente terá mais controle sobre suas informações pessoais e contribuirá para um ambiente digital mais seguro e protegido. Lembre-se sempre de ficar atento às possíveis ameaças à segurança cibernética e de tomar medidas adequadas para proteger seus dados pessoais. Juntos, podemos criar um ambiente digital mais seguro e protegido para todos.

5.6 PLANO DE RESPOSTA (ANPD)

Alessandra C. Puig Casariego[86]

A Lei Geral de Proteção de Dados (LGPD) estabelece que os agentes de tratamento de dados pessoais (controladores e operadores) adotem medidas para a prevenção de ocorrência de danos aos titulares em razão de suas atividades.

Assim, na eventualidade de um incidente de segurança, uma medida fundamental de mitigação de danos é a comunicação da ocorrência aos titulares dos dados pessoais violados. Desse modo, os titulares poderão tomar conhecimento do ocorrido e adotar as medidas de precaução para a mitigação dos riscos aos quais foram expostos em razão do incidente.

Aos controladores é atribuído o dever de comunicação aos titulares e à ANPD, quanto à ocorrência de incidentes que possam causar riscos ou danos relevantes aos titulares, por força do art.48 da LGPD. Esta comunicação ocorrerá por meio do processo de Comunicação de Incidente de Segurança (CIS).

Destaca-se que, recentemente, a Autoridade Nacional de Proteção de Dados (ANPD) publicou a Resolução nº 15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança (RCIS)[87]. O referido normativo tem como finalidade:

86 Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG. Membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas - FGV. Master of Business Administration - MBA em Advocacia Corporativa e Governança pela Escola Superior da Advocacia - ESA OAB. Pós-graduação em Direito Bancário pela Fundação Getúlio Vargas - FGV. Certificação em Compliance pela KPMG. Certificação em Investigações Corporativas pela KPGM. Curso de Extensão em Lei Geral de Proteção de Dados pela PUC-RS.

87 BRASIL. Resolução CD/ANPD Nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

- mitigar ou reverter prejuízos gerados por incidentes;
- assegurar a responsabilização e a prestação de contas;
- promover a adoção de boas práticas de governança, prevenção e segurança;
- fortalecer a cultura de proteção de dados pessoais no País e;
- fornecer subsídios para as atividades regulatória, fiscalizatória e sancionatória da Autoridade Nacional de Proteção de Dados (ANPD).

QUAIS SÃO OS PROCEDIMENTOS PARA A COMUNICAÇÃO DE INCIDENTE À ANPD?

A comunicação do incidente de segurança para a ANPD deve ser realizada de forma clara, objetiva e detalhada, por meio de formulário eletrônico disponibilizado pela ANPD, na forma da regulamentação vigente.

O controlador deve fornecer as seguintes informações na referida comunicação: (i) descrição da natureza e categoria dos dados pessoais afetados; (ii) número de titulares, indicando o número de crianças, adolescentes e idosos, quando aplicável; (iii) medidas técnicas e segurança adotadas, antes e depois do incidente; (iv) riscos e impactos aos titulares; (v) justificativa do atraso da comunicação, se realizada fora do prazo estabelecido pela ANPD; (vi) medidas adotadas ou futuras para reversão ou mitigação do incidente; (vii) data da ocorrência do incidente e data do conhecimento pelo controlador; (viii) dados do encarregado ou representante do controlador; (ix) identificação do controlador; (x) se agente de tratamento de pequeno porte, declaração nesse sentido; (xi) identificação do operador, quando aplicável; (xii) descrição do incidente, se possível indicando a causa principal; e (xiii) total de titulares afetados pelo incidente. Ademais, ressalta-se que a comunicação de incidente de segurança deverá ser realizada pelo controlador, por meio do encarregado, devendo estar acompanhada de documentação comprobatória do vínculo contratual, empregatício ou

funcional do encarregado, ou por meio de representante constituído, acompanhada de instrumento contendo os devidos poderes de representação junto à ANPD.

Por fim, caberá ao controlador solicitar à ANPD, mediante justificativa, o sigilo de informações protegidas por lei, indicando a necessidade de restrição de acesso, para hipóteses, como por exemplo, relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

QUAIS INCIDENTES DE SEGURANÇA DEVEM SER COMUNICADOS AOS TITULARES E À ANPD?

Na forma do Artigo 4º da Resolução nº15/2024[88], o primeiro critério a ser observado para a classificação quanto à necessidade de comunicação ou não do incidente se refere à possibilidade do incidente acarretar risco ou dano relevante aos titulares.

Além disso, a normativa define que o incidente de segurança pode acarretar risco ou dano relevante aos titulares, na hipótese de poder afetar significativamente interesses e direitos fundamentais dos titulares e, ainda, simultaneamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;
II - dados de crianças, de adolescentes ou de idosos;
III - dados financeiros;
IV - dados de autenticação em sistemas;
V - dados protegidos por sigilo legal, judicial ou profissional; ou
VI - dados em larga escala.

88 BRASIL. Resolução CD/ANPD Nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

QUAIS INFORMAÇÕES DEVEM FAZER PARTE DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA AO TITULAR?

A comunicação de incidente de segurança ao Titular deve conter as seguintes informações: (i) descrição da natureza e categoria de dados pessoais afetados pelo incidente; (ii) medidas técnicas e de segurança adotadas para a proteção de dados, resguardados os segredos comercial e industrial; (iii) riscos relacionados e possíveis impactos; (iv) justificativa do atraso, se a comunicação ocorrer fora do prazo regulatório; (v) medidas adotadas e futuras para reversão e mitigação do incidente, quando aplicável; (vi) data do conhecimento do incidente; e (vii) contato para obtenção de informações e dados de contato do encarregado, quando aplicável.

Alguns critérios devem ser observados para a aderência regulatória da comunicação de incidente de segurança ao Titular, tais como, o uso de linguagem simples e de fácil entendimento; realização, se possível, de forma direta e individualizada, ou seja, pelos meios usuais de contato com o Titular, como por exemplo, telefone, e-mail, SMS, WhatsApp, mensagem eletrônica em geral ou carta.

Na hipótese de impossibilidade de comunicação de individualizada ao Titular, o controlador deverá promovê-la pelos meios de divulgação disponíveis, podendo ser seu sítio eletrônico, aplicativos, mídias sociais e canais de atendimento ao Titular. O importante é permitir que a comunicação alcance o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de 03 (três) meses.

Outra obrigação relevante atribuída ao controlador na hipótese de incidente de segurança é a necessidade de comprovação da comunicação aos titulares no processo de comunicação de incidente, devendo constar os meios de comunicação ou divulgação utilizados. Esta diligência deve ser realizada em até 03 (três) dias úteis, contados

do término do prazo da comunicação previsto no *caput* do Artigo 9º da Resolução nº 15/2024.

Os prazos estabelecidos na Resolução em comento, no que se refere à comunicação de incidente de segurança ao Titular, são contados em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

QUAL É O PRAZO PARA A COMUNICAÇÃO DE UM INCIDENTE DE SEGURANÇA?

A ANPD, por meio da Resolução nº 15/2024, regulamentou o prazo para a realização da comunicação estabelecendo o seguinte:

A comunicação do incidente de segurança para a ANPD e para o Titular deverá ser realizada pelo controlador, no prazo de 03 (três) dias úteis, contado do conhecimento pelo controlador de que o incidente afetou dados pessoais.

O Controlador também deve manter registros detalhados de todas as etapas do processo de notificação e remediação, que podem ser solicitados pela ANPD para fins de fiscalização e investigação.

Os prazos estabelecidos na Resolução em comento, no que se refere à comunicação de incidente de segurança à ANPD, são contados em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

COMO DEVE SER REALIZADO O REGISTRO DE INCIDENTE DE SEGURANÇA?

Não restam dúvidas quanto à obrigatoriedade do registro de incidente de segurança pelo controlador, mesmo quando o incidente não atender aos critérios de classificação para a comunicação à ANPD e titulares.

Conforme estabelecido por regulamentações e normativas pertinentes, é imprescindível que as organizações adotem medidas adequadas para documentar e relatar quaisquer incidentes que possam vir a comprometer a confidencialidade, integridade, ou disponibilidade de informações sensíveis.

Nesse contexto, a Resolução nº 15/2024 traz a obrigatoriedade de manter o registro dos incidentes de segurança com dados pessoais, inclusive daquele não comunicado à ANPD e aos titulares, por ao menos 05 (cinco) anos, contado a partir da data do registro.

Esses registros deverão conter, ao menos, as seguintes informações: (i) data do conhecimento do incidente; (ii) descrição geral das circunstâncias; (iii) natureza e categoria dos dados afetados; (iv) número de titulares afetados; (v) avaliação de risco e possíveis dados aos titulares; (vi) medidas de correção e mitigação de efeitos; (vii) forma e conteúdo da comunicação à ANPD e aos titulares, se aplicável; e (viii) motivos da ausência de comunicação, se aplicável.

QUAIS AS CONSEQUÊNCIAS EM CASO DE DESCUMPRIMENTO QUANTO AO DEVER DE COMUNICAÇÃO?

Cabe ressaltar que o não cumprimento das obrigações previstas na LGPD, bem como na Resolução nº 15/2024, entre elas a comunicação de um incidente de segurança, pode resultar na instauração de processo sancionador, sem prejuízo de sanções administrativas que podem variar desde uma simples advertência até multas no valor de

até 2% (dois por cento) do faturamento da empresa, limitado a R$ 50 milhões por infração[89].

89 BRASIL. Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf

5.7 PLANO DE RESPOSTA (TITULAR)

Carlos Henrique Almeida Salgado[90]

A Lei Geral de Proteção de Dados (LGPD) estabelece direitos que podem ser exercidos pelos titulares mediante o controlador dos dados pessoais. Por esse motivo, é importante que a empresa esteja preparada para lidar com as exigências dos titulares.

É no artigo 18 da LGPD que estão relacionados os direitos específicos que podem ser exercidos pelo titular de dados pessoais. De acordo com a redação desse artigo, *"o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição".*[91]

Contudo, diferentemente do que a redação do artigo 18 pode sugerir, não há obrigatoriedade de atendimento de toda e qualquer requisição do titular. O próprio § 4º do artigo 18, aliás, prevê que uma solicitação do titular pode ser inexequível, e cabe esclarecer que é possível a existência de requisições dos titulares de dados pessoais cujo atendimento não será possível. O que é obrigatório é que o titular obtenha uma resposta acerca de sua solicitação.

Dessa forma, a empresa, na figura de controladora dos dados pessoais, deve possuir um Plano de resposta ao titular dos dados, que terá como objetivo formalizar os procedimentos internos que devem ser adotados para o processamento das requisições dos titulares de dados pessoais ou de seus representantes legais relativas ao exercício de

90 Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP e Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

91 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 mar.2023.

direitos relacionados ao tratamento dos dados pessoais reconhecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD define titular dos dados como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, tendo este titular o direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- confirmação da existência de seus dados pessoais, ou seja, o direito de solicitar ao controlador a confirmação quanto à realização do tratamento de seus dados pessoais;
- acesso aos seus dados pessoais, ou seja, o direito de obter acesso ou solicitar uma cópia de todos seus dados pessoais tratados pelo controlador;
- retificação de seus dados pessoais, significa o direito de corrigir dados pessoais incompletos, inexatos ou desatualizados;
- portabilidade de seus dados pessoais, ou seja, ter o direito de solicitar uma cópia de seus dados pessoais em formato estruturado, legível por máquinas, bem como o direito de postá-los a outro agente de tratamento, mediante requisição expressa, observados os segredos comerciais e industriais;
- solicitação de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, significa o direito de solicitar o bloqueio do tratamento de seus dados pessoais desnecessários ou excessivos;
- revogação do consentimento anteriormente prestado;
- solicitação da eliminação de seus dados pessoais tratados com base em seu consentimento, exceto nas hipóteses previstas em Lei;
- direito de ser informado sobre as consequências em não fornecer o consentimento para o tratamento previsto;
- direito de ser informado sobre quais entidades públicas e privadas com as quais o controlador compartilhou os seus dados pessoais;

- possibilidade de se opor, ou seja, ter o direito de contestar o tratamento dos dados pessoais realizados pelo controlador; e
- direito de ser informado sobre quais os critérios e procedimentos utilizados pelo controlador nas decisões automatizadas, observados os segredos comercial e industrial.

O recebimento das requisições para exercício de direitos do titular dos dados pessoais deve ser facilitado e possibilitado que seja feito por meio de diferentes canais, tais como formulário on-line disponibilizado no site ou aplicativo do controlador, e-mail específico, presencialmente, via entrega de cartas entre outros.

As requisições devem ser registradas para acompanhamento e controle do Encarregado pelo Tratamento de Dados Pessoais. A análise formal pelo Encarregado pelo Tratamento de Dados Pessoais deve contemplar: I) o nome completo do titular dos dados pessoais, telefone, endereço completo, e-mail ou outro canal para retornar a sua solicitação; II) cópia (física ou digitalizada) de documento vigente para identificar a identidade do titular dos dados pessoais; III) caso a requisição seja feita pelo representante legal do titular dos dados pessoais, documento comprobatório da responsabilidade do representante legal; IV) descrição ou razões sobre os direitos que se pretende exercer; e, sempre que possível, informações que facilitem a localização dos dados pessoais.

O Encarregado pelo Tratamento de Dados Pessoais deve fazer uma análise formal da requisição. Caso a requisição não preencha os requisitos formais descritos, deve ser recusada e informada ao requerente/titular a oportunidade de complementar os dados e reenviar novamente a requisição.

O controlador possui um prazo de 15 (quinze) dias corridos, a partir do registro da requisição, para responder à requisição relacionada à confirmação de existência ou disponibilização de acesso aos dados pessoais. As Áreas de Negócio da empresa devem

ser acionadas e envolvidas, a depender da natureza da requisição dos dados para solução ou execução das ações requeridas.

A LGPD reconhece diversos direitos do titular, havendo, para cada um deles, um correspondente dever do agente de tratamento de dados.

O Plano de respostas ao titular (modelo anexo) detalha os direitos dos titulares, os procedimentos internos para o recebimento das requisições e as formas adequadas de recebimento e tratamento de cada demanda e a forma correta de atendê-los.

5.8 PLANO DE RESPOSTA (VAZAMENTO - TITULAR) - PARTES INTERESSADAS (MÍDIA)

Aline Pelet Teles de Menezes[92]

Quando há a ocorrência de um incidente de segurança que tenha potencial de afetar significativamente interesses e direitos fundamentais dos titulares, o controlador tem o dever de comunicar aos titulares o Incidente e as possíveis violações ou vazamentos de dados que possam ter ocorrido.

Nesse sentido, o dever de comunicação previsto no art. 48 da LGPD deve estar previsto nos procedimentos internos da empresa, com critérios objetivos estabelecidos, respeitando inclusive o art. 6º do Regulamento da ANPD, que estabelece o prazo de 3 (três) dias úteis, contados do conhecimento do incidente de segurança, para realizar a comunicação, devendo conter informações como: a natureza e categoria dos dados pessoais afetados, riscos e impactos ao titular, data e hora do conhecimento do incidente, medidas segurança adotadas, dados do Encarregado de dados e as informações sobre o operador, quando necessário.

Deve-se levar em consideração na hora de comunicar o cliente, propósitos múltiplos como a proteção do titular, a efetivação do princípio da responsabilização e prestação de contas, até a promoção da cultura de proteção de dados e o principal: informar ao titular a respeito da ameaça de direitos fundamentais, cumprindo o princípio da transparência e a mitigação de riscos e danos, na realidade fática.

Do ponto de vista operacional, o controlador deve notificar o titular pelos meios de comunicação existentes e que tenham eficácia, observando se foi possível identificar a totalidade de titulares afetados ou não. Diante disso, recomenda-se que, quando o controlador

92 Advogada inscrita na OAB/MG nº 211.427, especialista em Direito Empresarial pela PUC-MG e pós-graduanda em Direito Digital, Proteção de Dados e Compliance Trabalhista pela EMD, graduada em Direito e Relações Internacionais. Vice-presidente da Comissão de Direito Digital e Proteção de dados da 45ªSubseção da OAB, ANAD e Comissão Estadual de Proteção de Dados da OAB/MG.

consegue mensurar e qualificar os titulares afetados, a comunicação deve ser feita de forma individualizada, por e-mail, aplicativo de mensagens como whatsapp, redes sociais, correspondência física enviada via correios.

Quando não é possível identificar todos os titulares afetados, o controlador deve utilizar meios de comunicação que cheguem ao maior número possível de pessoas, como rádio, televisão, jornais de grande circulação, mídias sociais oficiais do controlador, por meio de ferramentas de e-mail marketing, no qual o controlador possui uma rede de contatos cadastrados.

O primordial aqui é se atentar aos detalhes, quanto mais específico e detalhado for o documento de comunicação de Incidentes de segurança, menores são os riscos de o operador ser penalizado com sanções mais severas junto à ANPD. Uma notificação de incidente de segurança generalizada pode ser considerada inválida, pois pode gerar o problema das subnotificações, no qual se notifica menos do que o esperado, prejudicando até mesmo a mensuração da realidade fática dos Incidentes de segurança.

5.9 POLÍTICA DE PRIVACIDADE INTERNA (COLABORADORES) - LGPD

Elaine Cristina Pereira dos Santos Nery[93]

A política interna de privacidade de dados pessoais existe para dar transparência sobre o tratamento dos dados pessoais realizados pela Empresa em face do titular dos dados pessoais (Colaborador) e ainda deve estar em consonância com toda a legislação vigente e garantir conformidade a LGPD em todos os setores da Organização, devendo ainda facilitar todo o gerenciamento das atividades de tratamento de dados pessoais existentes, sem que isso atrapalhe a finalidade do negócio da Empresa, tendo como premissa básica a boa prática e governança da Instituição.

Na Lei Geral de Proteção de dados, na seção que descreve boas práticas e governança dentro da empresa, em seu art. 50, aponta a competência do Controlador e do Operador de dados para formular o regulamento de boas práticas e de governança.

A Organização, quando adota processos e políticas internas de boas práticas, assegura a boa-fé de seus procedimentos e demonstra que tem interesse de deixar claro como os dados dos Titulares são tratados, observando assim a aplicação da lei, conforme § 2º do art. 50 da LGPD.

Ademais, boas práticas estabelecem uma boa cultura organizacional e fortalecem o negócio, trazendo maior reputação e credibilidade, tanto dentro como fora da empresa.

A política é única, e é baseada no negócio da Empresa. Por isso, é preciso adequar toda a organização com as legislações existente, como

93 Advogada. Pedagoga e Professora de Educação Física. Especialista em Direito Empresarial, Trabalhista e Direito Público. Especialista em Privacidade e Proteção de dados. Especialista em Adequação a LGPD no Setor de Recursos Humanos – RH, Especialista em Adequação a LGPD na Área da Saúde. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora e Palestrante em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão de Proteção de Dados da OAB/MG e Membro da Comissão de Proteção de Dados da UFVJM.

é o caso da legislação trabalhista, previdenciária, Código de Defesa do Consumidor, o Marco Civil da Internet, Lei Geral de Proteção de Dados (LGPD) e outras legislações que se encaixem no negócio da Empresa.

Após esta adequação, os colaboradores se sentem mais seguro com o estabelecimento. Assim, elementos mínimos devem constar em uma política de privacidade:

- Conceitos legais;
- Princípios legais da proteção de dados pessoais;
- Por que tratamos seus dados pessoais;
- Finalidade do tratamento;
- Coleta de dados pessoais: Dados coletados no site da empresa, Dados de candidatos;
- Dados de colaboradores, Dados coletados dos dependentes legais dos colaboradores, Dados de diretores, Dados de visitantes, Dados de fornecedores, prestadores de serviço, terceiros e trabalhadores avulsos;
- Compartilhamento com terceiros;
- Direitos legais dos titulares dos dados;
- Responsabilidade;
- Descumprimento da política interna: Terceiros Sem Vínculo Empregatício, Empregados Com Vínculo Empregatício;
- Segurança dos dados pessoais;
- Cookies;
- Tempo de retenção de dados;
- Transferências internacionais de dados pessoais;
- Armazenamento dos dados;
- Eliminação dos dados pessoais;
- Descumprimento da política;
- Confidencialidade;
- Vigência;
- Canal de contato.

Os elementos acima devem ser detalhados para dar maior transparência para o titular dos dados (Colaborador/terceiros que acessam de alguma forma os dados pessoais de clientes/fornecedores da empresa).

Por fim, sempre que ocorrer mudança no processo, a Organização deverá atualizar a política e dar total transparência para o Colaborador (titular).

5.10 POLÍTICA DE COOKIES

Emily Matias Assumpção[94]

É muito comum aparecer em todos os sites a mensagem de "Esse site utiliza cookies para melhorar sua experiência, você deseja aceitar o uso de cookies?".

Mais comum ainda são as pessoas clicarem no "li e aceito", sem ao menos saber o que estão aceitando. Desse modo, é essencial entender o que são cookies e qual a sua importância.

Cookies são pequenos arquivos textos que podem ser armazenados no computador, pelo navegador web, enquanto se navega em um site. De forma objetiva, o referido armazenamento serve para lembrar, mapear e registrar as atividades de navegação do usuário, por exemplo, dados pessoais: nome, e-mail, dados de cartão de crédito, entre outros.

Para tanto, os cookies são importantes para registrar padrões de acesso e comportamentos do usuário. Ocorre que é imprescindível que o site que coleta cookies avise de forma clara e transparente para o usuário se há coleta de cookies, bem como se estes são dados pessoais.

Vale dizer que, em outubro de 2022, a Autoridade Nacional de Proteção de Dados – ANPD, publicou o guia orientativo "Cookies e Proteção de Dados Pessoais", que se encontra disponível no sítio eletrônico da própria Autoridade.

A ANPD dispõe que o referido guia possui o seguinte objetivo:

O material foi elaborado com o objetivo de orientar os agentes de tratamento sobre as boas práticas na área, além de traçar um panorama geral sobre o assunto, abordando desde questões mais conceituais como a classificação desta tecnologia de acordo com

94 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

diversos parâmetros, até pontos mais técnicos como as boas práticas a serem observadas na sua utilização em sites eletrônicos.

É certo que a ANPD exerce um papel pedagógico, buscando ensinar e trazer as diretrizes para o correto tratamento de dados, bem como o uso adequado dos cookies. Ademais, o guia discorre desde o ensinamento básico de "o que são cookies", até a explicação sobre suas categorias e demais hipóteses, sendo leitura indispensável para qualquer profissional que atua na área da proteção de dados.

Logo, segue abaixo um *template* com as principais informações que devem conter no aviso de cookies. Ressalta-se, que o *template* serve como base e as informações podem mudar a depender do porte do escritório.

Aviso de Cookies
Explicar detalhadamente sobre o uso de cookies
Categorizar os cookies
Finalidade do uso dos cookies
Como os cookies são utilizados?
Qual o prazo de utilização dos cookies
Gerenciamento dos cookies
Canal de comunicação
Aviso sobre atualizações

5.11 AVISO DE PRIVACIDADE

Emily Matias Assumpção[95]

O Aviso de Privacidade é um documento direcionado a clientes e prestadores de serviços, com o objetivo de demonstrar transparência no uso, coleta, armazenamento, transferência de dados, entre outros.

Ainda existem muitas dúvidas entre a diferença da Política de Privacidade para o Aviso de Privacidade, mas vale dizer que a Política de Privacidade visa estabelecer as diretrizes para o uso correto dos dados pessoais, ou seja, nela constam as regras e direcionamentos para que os colaboradores saibam como está sendo realizado o correto tratamento dos dados pessoais em seu dia a dia. Logo, tem-se que a Política de Privacidade é um documento interno para os colaboradores.

Portanto, observa-se que o Aviso de Privacidade é um documento voltado para o público externo, que, na maioria das vezes, fica exposto no *website* das empresas e não existe uma forma, ou padrão, preestabelecida, isso significa que vai depender da criatividade do Encarregado de Dados e seu Comitê, visto que o aviso pode ser feito em formato de vídeo, animações, quadrinhos, texto, entre outros.

Mas, independentemente do formato, é imprescindível que a comunicação seja simples, acessível e objetiva ao titular, sem "juridiques", com a finalidade de transparência e conscientização.

Para tanto, segue abaixo um *template* com as principais informações que devem conter no aviso de privacidade. Ressalta-se, que o *template* serve como base e as informações podem mudar a depender do porte do escritório.

95 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

Aviso de Privacidade

Agente de tratamento (informar o nome do escritório e informações necessárias)

Definições importantes (explicar os principais conceitos exemplo: dado pessoal, dado pessoal sensível, tratamento, titular, dentre outros).

Como acontece o tratamento de dados

Qual a finalidade do tratamento dos dados

Se há transferência internacional de dados

Quais são os mecanismos de segurança para proteger os dados pessoais

Ciclo de vida dos dados pessoais (Coleta até o descarte)

Tratamento de dados de criança e adolescentes

Com quem compartilha os dados pessoais

Quais são os direitos dos titulares

Incidentes de Segurança

Canal de comunicação com o Encarregado (exemplo: e-mail, telefone)

Informações sobre os cookies (explicar para que serve, como funcionam, se os cookies são dados pessoais)

Alteração nas políticas

Por fim, é de extrema importância manter o aviso de privacidade sempre atualizado e de acordo as normativas da LGPD e ANPD.

5.12 CONSTRUINDO UM PROCEDIMENTO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Gabriel Campos Cunha[96]

Transferência internacional de dados pessoais, nos termos do artigo 5º, XV da LGPD, é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Isso acontece devido à atividade dos Controladores de dados que precisam tratar dados pessoais em suas unidades em outros países, com outros controladores (ex.: parceiros comerciais, órgãos públicos ou outras instituições) ou, ainda, que contratam serviços realizados por operadores, fora do Brasil (ex.: armazenamento de dados em nuvem).

Havendo transferência internacional de dados, o responsável pelo tratamento deve respeitar os princípios de proteção de dados e garantir os direitos dos titulares. A LGPD traz em seu artigo 33 as hipóteses e condições em que a transmissão de dados é permitida:

> Art. 33: A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> (a) Os países ou organismos internacionais proporcionarem grau de proteção de dados pessoais adequado ao previsto na LGPD (Art. 33, I, da LGPD). Segundo o art. 34 da LGPD o nível de proteção de dados do país estrangeiro ou do organismo internacional deverá ser avaliado pela ANPD.
> (b) O Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD. A proteção dos dados e dos direitos dos titulares é responsabilidade do Controlador.

96 Advogado, consultor em Governança Corporativa, ESG, Compliance, Integridade, Proteção de Dados. Auditor de Sistemas De Gestão da Qualidade, Meio Ambiente, Saúde e Segurança do Trabalho. Auditor da Conformidade Legal nos temas de Proteção de Dados, Privacidade, Meio Ambiente e Saúde e Segurança do Trabalho.

(c) A transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (Art. 33, III, da LGPD).
(d) A transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros (Art. 33, IV, da LGPD).
(e) A autoridade nacional autorizar a transferência (Art. 33, V, da LGPD).
(f) A transferência resultar em compromisso assumido em acordo de cooperação internacional (Art. 33, VI, da LGPD).
(g) A transferência for necessária para a execução de política pública ou atribuição legal do serviço público (Art. 33, VII, da LGPD).
(h) O titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta e outras finalidades Art. 33, VIII, da LGPD); ou
(i) É necessária para atender as hipóteses previstas nos incisos II, V e VI do Art. 7º da LGPD (Art. 33, IX, da LGPD), isto é respectivamente: para o cumprimento de obrigação legal ou regulatória pelo Controlador, quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

É recomendável que a organização elabore documento registrando as nuances quanto ao tratamento de dados que realiza, contendo informações, análises e práticas. Tal procedimento, a título de sugestão, pode estar estruturado em 3 tópicos:

Sobre a Transferência Internacional de Dados Pessoais:	Requisitos para a Realização da Transferência Internacional de Dados Pessoais:	Ocasiões em que a empresa realiza Transferência de Dados Pessoais:
Conceito, aplicações de segurança aplicáveis, formas de realizar, normas aplicáveis.	Informa quais são as ocasiões para se verificar a possibilidade da transferência, questionamentos precedentes a realização e outros critérios: Finalidade da Transferência; Necessidade da Transferência; O país para o qual será feita a transferência possui leis compatíveis com a LGPD quanto à privacidade e segurança da informação.	Lista das ocasiões em que são realizadas transferências internacionais de dados pessoais na organização de acordo com o levantamento de processos da empresa.

É de extrema importância que uma empresa conduza um processo de *due diligence* com seus fornecedores internacionais. Esse procedimento é fundamental para garantir que a empresa estabeleça contratos com organizações que estejam em conformidade não apenas com a LGPD, mas também com a legislação de privacidade e proteção de dados do país em que estão sediadas.

5.13 REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ROPA)

Isabela Cristina Maia da Cruz[97]

ROPA ou Registro das Operações de tratamento de dados pessoais trazidos pela Lei Geral de Proteção de Dados é todo ou qualquer registro dentro de uma organização que envolva de alguma forma o tratamento dos dados pessoais. Esses registros/tratamentos devem ser realizados pelos Controladores e pelo Operadores[98], por meio de formulário/inventário.

Em síntese, o ROPA trata-se de um compilado de informações que poderá ser utilizado como meio de prova em caso de um possível vazamento de dados, ou até mesmo, para conhecer todos os processos da empresa, bem como localizar e saber onde está cada informação da empresa – setor por setor.

A Autoridade Nacional de Proteção de Dados ANPD elaborou um Guia para auxiliar ao Controlador e ao Operação no registro das Operações. Esse guia elaborado pela ANPD, pode ser acessado por meio do link chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Entretanto deixamos abaixo uma lista de possíveis perguntas que deverão fazer parte do ROPA.

- Identificação dos serviços;
- Identificação dos Agentes de Tratamento e do(s) Encarregado(s) de Proteção de Dados;
- Fases do Ciclo de Vida do Tratamento Dados Pessoais;

97 Advogada, especialista em Direito Digital e compliance, Presidente da comissão proteção de dados, subseção Vespasiano, membro da Comissão Lei Geral de Proteção de Dados-OAB/MG.

98 Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

- De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados;
- Escopo e Natureza dos Dados Pessoais;
- Finalidade do Tratamento de Dados Pessoais;
- Categoria de Dados Pessoais;
- Categorias de Dados Pessoais Sensíveis;
- Frequência e totalização das categorias de dados pessoais tratados;
- Tipo de Categoria;
- Dados pessoais compartilhados;
- Tipo de medida de segurança e privacidade;
- Transferência Internacional de Dados Pessoais;
- Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio.

A capacidade do mapeamento dos processos de forma exata dar-se-á pela totalidade do levantamento de informações dos dados tratados e coletados, agindo em compliance, sobretudo ao permitir que cada área avalie, no que cerne à necessidade e fundamentação das coletas realizadas, além da importância quanto ao seu cumprimento legal.

Sendo assim, o Registro das Operações de Tratamento é de extrema importância, devendo ser atualizado, ampliando de forma permanente, mantendo-se alinhado com os objetivos das diretrizes determinadas pela ANPD.

5.14 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Emily Matias Assumpção[99]
Izabela Nunes Pinto[100]

A Lei Geral de Proteção de Dados Pessoais – LGPD, dispõe em seu art.5º, XVII, sobre o Relatório de Impacto à Proteção de Dados Pessoais – RIPD, assim sendo:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Apesar de muitos profissionais que atuam com a proteção de dados desconhecerem a existência do RIPD, este se encontra previsto em Lei, e, inclusive, vem sendo discutido na agenda regulatória da Autoridade Nacional de Proteção de Dados – ANPD.

Para tanto, o RIPD é um documento considerado como entregável no processo de adequação à LGPD, que deve conter a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco

99 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

100 Advogada. Membro nomeado da Comissão de Proteção de Dados da OAB/MG. Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Curso de Direito para Startups na Europa (envolvendo GDPR, LGPD e outros temas relacionados ao Direito Digital) pela Academy da Platzi. Finalista, ocupando o 3º Lugar Geral do Brasil da 1a Edição do LawCamp - 1a Competição de Implementação da LGPD no Brasil. Palestrante (Adequação/Implementação da LGPD e Direito Digital).

à garantia dos princípios e fundamentos, bem como às liberdades civis e aos direitos fundamentais do titular de dados.

É importante que o documento disponha sobre todas as medidas, salvaguardas e mecanismos de mitigação de risco, de modo a atender ao dispositivo legal.

Embora o art. 38 explique que a ANPD poderá determinar ao controlador que este elabore o RIPD, é uma boa prática e recomendação que o operador também elabore, quando incorrer em situações no tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais.

Para tanto, a ANPD recomenda o seguinte:

A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como:

> Nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);
> Quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º)
> Para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32);
> Para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).
> Portanto, haverá situações em que o controlador elaborará o RIPD para atender à determinação da ANPD ou, em atenção ao princípio da responsabilização e prestação de contas (art. 6º, X), ao verificar que o tratamento a ser realizado pode implicar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.

Vale dizer, que na hipótese de um melhor cenário, o recomendado é que se elabore o RIPD antes mesmo de se iniciar o tratamento de

dados pessoais, contudo, a realidade nos processos de adequação à LGPD em escritórios de advocacia e nas demais empresas é mapear os processos quando o tratamento de dados já ocorre.

Logo depois de finalizar o mapeamento de dados pessoais (*data mapping*), é importante que, assim que se identificar um tratamento que possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais, se elabore o RIPD.

Não se tem um modelo ou metodologia específica, o escritório de advocacia deve buscar a metodologia que melhor atende à sua realidade para realizar o gerenciamento de riscos.

A ANPD explicita ainda sobre o tema:

> Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos:
> a) a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;
> b) a metodologia usada para o tratamento e para a garantia da segurança das informações; e
> c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.
> É importante que o relatório seja suficientemente detalhado, para que a ANPD e o próprio controlador tenham compreensão ampla de como ocorre o tratamento dos dados pessoais e os possíveis riscos associados a ele.
> Assim, recomenda-se ao controlador descrever os tipos de dados pessoais tratados, as operações de tratamento (art. 5º, X, da LGPD), suas finalidades (incluindo interesses legítimos) e hipóteses legais, e avaliar a necessidade e a proporcionalidade das operações de tratamento, os riscos para os direitos e liberdades dos titulares de dados e as medidas a serem adotadas para minimizar esses riscos.

Vale dizer que o RIPD não é um documento sigiloso, podendo ser apresentado ao titular, como forma de "boas práticas".

Por fim, após elaborado o RIPD, cabe ao consultor, ou DPO, verificar a possibilidade e os riscos de prosseguir com o tratamento de dados pessoais que ensejaram a elaboração deste ou a necessidade de remodelação do tratamento, bem como do negócio.

Nesse sentido, segue abaixo *template* com as principais informações que devem conter no RIPD, que inclusive são orientações da própria ANPD. Ressalta-se que o *template* serve como base e as informações podem mudar a depender do porte do escritório.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Identificação dos agentes de tratamento e do encarregado;
Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos;
Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros);
Projeto/Processo que justifica a elaboração do RIPD;
Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;
Tratamento de dados;
Descrição do tratamento (desde a coleta até a eliminação);
Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa);
Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratadas, de forma completa);
Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços);
Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver;
Volume de dados pessoais tratados e número de titulares envolvidos no tratamento;
Fonte de coleta;
Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado);
Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver);
Política de armazenamento (descrever os prazos de retenção e métodos de descarte);
Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento;
Análise de princípios da LGPD;
Riscos identificados ao titular;
Resultado apurado com base na metodologia utilizada pelo agente de tratamento (probabilidade e impacto);
Medidas, salvaguardas e mecanismos de mitigação de risco;
Descrever as medidas adotadas para mitigação do risco;
Registro dos resultados e conclusões do RIPD na visão do Encarregado De Proteção de Dados (DPO);
Responsável pela elaboração;
Aprovações e datas.

5.15 TESTE DE PONDERAÇÃO OU LEGITIMATE INTERESTS ASSESSMENT (LIA)

Priscila Silva Ribeiro[101]

O legítimo interesse é uma das bases legais previstas para fundamentar o tratamento de dados pessoais, de acordo com a Lei Geral de Proteção de Dados, conforme seu artigo 7º, IX.

A referida norma autoriza o tratamento de dados pessoais quando houver necessidade de se atender ao legítimo interesse do controlador ou de terceiros.

O controlador é quem tem o poder de decisão sobre o tratamento de dados pessoais. Isso está claro. Porém, quem seria o terceiro? Infere-se que seria uma pessoa estranha à relação incialmente entabulada, sem poderes decisórios, mas que pode ser impactado por este tratamento de dados.

Mas o que seria legítimo interesse? Segundo a definição semântica do termo[102], algo legítimo é o que encontra respaldo em lei, que seja fundamentado e amparado por ela, o que é justificado, explicado pelo bom-senso, o que é justo e razoável. Ao passo que interesse é algo importante, útil, vantajoso, moral ou socialmente.

Logo, apesar da subjetividade intrínseca trazida por esta base legal, é importante que ela seja utilizada estritamente em situações em que exista o legitimo interesse, por meio dos conceitos acima abordados.

Assim, o legítimo interesse pode ser compreendido como algo legal, justo e razoável, que é importante, útil ou vantajoso, moral, social ou materialmente para o controlador ou um terceiro. Ou seja, apesar de ser uma importante ferramenta para os negócios, esta base

101 Data Protection. Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPCPD pela Legal Ethics and Compliance. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

102 Definição segundo o dicionário Online de Português. https://www.dicio.com.br/legitimo/.

legal não pode ser utilizada de forma arbitrária e indiscriminada, ou que viole os direitos dos titulares, que desequilibre a relação com estes de forma gritante, ou que viole direitos e garantias fundamentais dos titulares.

Dessa forma, sempre deve ser feito o exercício de ponderação e equilíbrio entre o interesse/objetivo pretendido e o direito dos titulares de dados. Logo, razoabilidade, proporcionalidade e bom-senso não podem faltar nesta equação.

A utilização desta base legal é dotada de grande subjetividade e, do mesmo modo, relevante importância, pois a organização por muitas vezes precisa tratar dados pessoais para o regular desenvolvimento do seu negócio, porém, não encontra outra fundamentação.

No entanto, é importante ter cautela quanto ao seu uso. Como exemplos aceitáveis para a utilização desta base legal pode-se mencionar o marketing direto, canais para envio de denúncias, segurança da informação, pesquisa e desenvolvimento de produtos e serviços, entretanto, cada situação deverá ser analisada de forma individualizada.

Por meio de uma análise apurada das disposições contidas na LGPD, infere-se que o legítimo interesse poderá ser cogitado como uma base legal quando:

- Não há uma obrigação legal a ser cumprida, para o tratamento daquele dado pessoal. Porém, há um interesse legítimo do controlador ou de terceiros;
- Existe uma situação concreta a ser analisada;
- Há uma expectativa por parte do titular de dados quanto ao tratamento de seus dados pessoais, ou seja, é algo razoável a ser considerado;
- O controlador entende ser inviável solicitar o consentimento ao titular de dados, ao menos neste momento; ou, compreende ser desnecessário incomodar o titular com solicitação de consentimento desgastantes, quando é

improvável que haja a oposição por parte deste, em virtude da relação preexistente.
- Quando o controlador assume o risco quanto ao tratamento de dados pessoais do titular, em virtude de determinado objetivo desde que ele consiga demonstrar a justificativa para tanto.

Em um primeiro momento parece que o Legitimo interesse é uma base legal a ser utilizada de forma corriqueira e frequente em virtude de sua subjetividade e flexibilidade. Todavia, isso não corresponde à realidade. Ademais existem pontos a serem observados, sendo eles:

- Não se aplica para toda situação;
- Não é uma base legal para ser utilizada de forma irrestrita;
- Não tem prioridade sobre as outras bases legais;
- Não pode se sobrepor aos direitos e garantias individuais dos titulares;
- Inicialmente pode parecer uma opção mais fácil para a utilização, porém ele eleva o nível de responsabilidade do controlador de dados;
- Não pode ser utilizado para tratamento de dados pessoais sensíveis.

Em que pese a previsão expressa contida no artigo 10 da LGPD, sobre o tratamento de dados fundamentado no legítimo interesse, não há diretrizes claras e práticas na Lei sobre a forma como ela deve ser utilizada. Nem mesmo o regulamento europeu, o GDPR, *General Data Regulation Protection*, o qual foi utilizado como base para a elaboração da lei brasileira, detalha como deve ser realizada uma Avaliação de Legítimo interesse.

Sobre o tema, importante ainda salientar que a ANPD também não emitiu qualquer pronunciamento a este respeito até o momento.

Em virtude dos critérios subjetivos envolvidos, para que esta base seja utilizada de forma adequada, é necessária a realização do LIA, *Legitimate Interests Assesment* ou teste de ponderação.

A grande pergunta é, se não existe previsão específica na Lei nacional, nem mesmo na estrangeira, e, considerando a ausência de manifestação da ANPD até o momento sobre o tema, como realizar um LIA adequadamente?

A fim de conferir maior segurança ao controlador de dados, usualmente são utilizadas as orientações trazidas pelo WP29, que foi um grupo de trabalho europeu independente, que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018. Foi este grupo, inclusive, que, em 2014, inicialmente aventou a necessidade de utilização do teste do legítimo interesse.[103]

Em 2014 o grupo trouxe já algumas considerações sobre a utilização desta base legal para o tratamento de dados, tais como: Se o tratamento de dados por esta base legal seria necessário para o exercício de um direito fundamental; Se é do interesse público ou beneficia reconhecidamente a comunidade. Se o impacto sobre o titular de dados e suas expectativas razoáveis sobre o que acontecerá com seus dados, ou seja, se o titular pode esperar, em virtude da relação já estabelecida, que seus dados poderiam ser tratados dessa forma; bem como a natureza dos dados e como são processados.

Também já foi contemplada a necessidade quanto à utilização e salvaguardas adicionais que poderiam limitar o impacto indevido sobre o titular de dados, como a minimização destes, além da utilização de tecnologias de reforço da privacidade, maior transparência, assim como o direito incondicional de *opt-out* e portabilidade de dados.[104]

Para transformar a base teórica construída e aventada pelo WP29 em uma metodologia prática, são utilizadas as diretrizes emanadas pela ICO – *Information Commissioner's Office*, que é uma autoridade independente do Reino Unido criada para defender os direitos de

103 Curso Legítimo interesse teoria e prática. Udemy. DODT, Carlos, 2021.
104 Curso Legítimo interesse teoria e prática. Udemy. DODT, Carlos, 2021.

informação no interesse público, o qual propõe a realização do teste em 03 etapas, seguida por uma fase de decisão.[105]

Fonte: Elaborado pelo próprio autor do texto.

Abaixo segue a sugestão de como o teste de viabilidade pode ser realizado:

ETAPA 1: TESTE DE PROPÓSITO – AVALIAR SE HÁ UM LEGÍTIMO INTERESSE NO TRATAMENTO
1 - Por qual motivo a empresa decidiu tratar este (s) dados?
2 - Quais benefícios o tratamento de dados com esta finalidade trará para a organização?
3 - Terceiros se beneficiarão do tratamento fundamentado no legítimo interesse? Quais serão estes benefícios?
4 - Qual seria o impacto se a organização não pudesse utilizar o legítimo interesse como base legal para o tratamento de dados?
5 - A organização está seguindo outras leis que impactam nesta base legal (LIA)?
6 - Existem outras questões éticas relacionadas ao tratamento de dados por este fundamento?

ETAPA 2: TESTE DE NECESSIDADE – AVALIAR SE O TRATAMENTO É NECESSÁRIO PARA O PROPÓSITO IDENTIFICADO
1 - Esse tratamento leva a organização a atingir seus objetivos de forma concreta?
2 – A organização pode atingir o mesmo objetivo, mas de outra forma menos agressiva?
3 – A organização pode atingir o objetivo sem o tratamento por esta base legal?

105 Curso Legítimo interesse teoria e prática. Udemy. DODT, Carlos, 2021.

4 – Existe proporcionalidade entre o tratamento e a finalidade pretendida?
ETAPA 3: TESTE DE PONDERAÇÃO OU BALANCEAMENTO – AVALIAR OS IMPACTOS SOBRE OS INTERESSES, DIREITOS E LIBERDADES DOS TITULARES E AVALIAR SE ISSO SE SOBREPÕE AOS SEUS INTERESES LEGÍTIMOS
Natureza dos Dados Pessoais Tratados
1 - São dados de categorias especiais ou sensíveis?
2 - São dados que as pessoas provavelmente consideram particularmente "privados"
3 - Serão tratados dados pessoais de crianças e adolescentes ou dados relacionados a outras pessoas vulneráveis?
4 - Os dados pessoais que serão tratados incluem informações sobre os titulares em um contexto pessoal ou profissional?
Expectativas razoáveis do titular
1 - A organização já possui um relacionamento existente com o titular?
2 - Qual é a natureza do relacionamento e como a organização usou os dados do titular no passado?
3 - Sua organização coletou os dados diretamente do titular? O que foi informado no momento da coleta?
4 - Se sua organização obteve os dados por meio de terceiros, o que eles disseram aos titulares sobre a reutilização por terceiros para outros fins? Sua organização foi mencionada?
5 - Há quanto tempo sua organização coletou os dados? Houve alguma mudança na tecnologia ou no contexto desde então que afetaria as expectativas dos titulares?
6 - O propósito e método de tratamento pretendidos são amplamente compreendidos?
7 - Sua organização pretende fazer algo novo ou inovador com os dados do titular?
8 - Sua organização possui alguma evidência sobre as expectativas do titular (e.g. pesquisas de mercado, grupos de foco ou outras formas de consulta) para o tratamento pretendido?
9 – Existem outros fatores nas circunstâncias particulares que significam que os titulares de dados pessoais esperariam ou não o tratamento?

Possíveis Impactos ou Impacto Provável
1 - Quais são os possíveis impactos do tratamento para os titulares?
2 - Os titulares perderão qualquer controle sobre o uso de seus dados pessoais?
3 - Qual é a probabilidade e severidade de qualquer impacto potencial?
4 - É provável que algumas pessoas se oponham ao tratamento ou o considerem intrusivo?
5 - Sua organização ficaria feliz em explicar publicamente este tratamento aos titulares?
6 - Sua organização pode adotar alguma proteção para minimizar o impacto do tratamento (e.g. minimização dos dados, tecnologias de reforço da privacidade e portabilidade de dados)?
7 - Titulares têm acesso facilitado à possibilidade de se opuserem ou serem excluídos (opt-out) do tratamento pretendido?

Concluídas as análises acima expostas, haverá a constatação sobre a conformidade ou não do tratamento de dados pessoais com base no legítimo interesse. Importante salientar que a reprovação em qualquer das fases do teste ponderação (LIA) deixará inviabilizada a utilização desta base legal.

Em caso de utilização do legítimo interesse como a base legal adequada ao Tratamento de Dados, é necessário que haja a devida fundamentação, ou seja, quais foram os motivos aptos a embasar a escolha por esta base legal. Sugere-se que esta fase, denominada fase decisória ou de decisão, seja realizada da seguinte maneira:

ETAPA 4: DECISÃO	
O Legítimo Interesse é considerado uma base legal adequada ao tratamento pretendido?	( ) SIM ( ) NÃO
Foi identificada a necessidade de criar um Relatório de Impacto à Proteção de Dados Pessoais (RIPDP)?	( ) SIM ( ) NÃO
Existe algum comentário importante para o momento?	

Fonte: Curso Legítimo interesse teoria e prática. Udemy. DODT, Carlos, 2021

O LIA cria evidências das decisões e da justificativa para tratar dados com base no Legítimo Interesse, ajudando a demonstrar conformidade com as exigências da LGPD, que também englobam os princípios insculpidos no artigo 6º da Lei (Brasil, 2018), quais sejam: finalidade, adequação, necessidade, prevenção, responsabilização e prestação de contas, conferindo maior transparência, credibilidade e segurança ao processo.

Importante ainda salientar que o LIA consiste em um processo formal, o qual deve ser devidamente documentado, a fim de que o controlar possa apresentar a documentação, caso seja solicitado tanto à ANPD quanto às partes envolvidas.

Para que o teste seja realizado de forma adequada e contundente, é importante que este seja formulado de forma clara, objetiva, com linguagem formal, transparente, específica sobre o tema e que reflita de fato a realidade do tratamento de dados. Isso otimizará o processo e o deixará mais eficaz e eficiente, observando a conformidade com a LGPD.

Importante ainda mencionar a estrutura do documento, como ele deve ser formatado, realizado e apresentado, devendo conter: formatação e identidade visual, capa, introdução, análise de legítimo interesse, decisão, aprovação e arquivamento.

É importante enfatizar que, na introdução, será feito um breve explicativo sobre o dado que se pretende tratar e o motivo de ser cogitado o tratamento pelo legítimo interesse. Após, deverão ser expostas as análises, conforme acima explicado. No documento, deverá constar ainda quem foi/foram os responsáveis pelo relatório, quem revisou, quem aprovou o processo, assim como a data de sua elaboração.

Por isso, é aconselhável que se coloque uma data de validade para o LIA, a fim de realizar uma revisão com certa periodicidade. É aconselhável que seja observada a revisão ao final do período de um ano. Sugere-se a seguinte forma:

NOME COMPLETO	CARGO	DATA	ASSINATURA	OBSERVAÇÃO ADICIONAL

Mesmo após a realização das etapas acima demonstradas, é importante que se identifique se há a necessidade quanto à criação de um Relatório de Impacto à Proteção de Dados Pessoais (RIPDP), a fim de se detalhar de forma mais esmiuçada os riscos contidos no processo.

A utilização do Legítimo Interesse do controlador como base legal para tratamento de dados pessoais reveste-se de extrema importância para o desenvolvimento regular do negócio. Todavia é imperioso resguardar o direito do titular de dados, motivo pelo qual o seu uso de ser feito por meio da ponderação do binômio razoabilidade x proporcionalidade.

5.16 PLANO DE RESPOSTA A INCIDENTES

Adiel Ribeiro[106]

Incidentes de Segurança da Informação devem ser detectados e respondidos por meio de processos testados e documentados o mais rápido possível para minimizar o impacto negativo ao negócio, estes processos podem ser chamados de playbooks e se possível devem ser automatizados.

Eles servem para que a empresa volte a operar normalmente no menor tempo possível e devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinados com a estimativa de impacto ao negócio prevista.

Após a erradicação completa do incidente deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente, documentando o processo e atentando principalmente, para que ele não se repita.

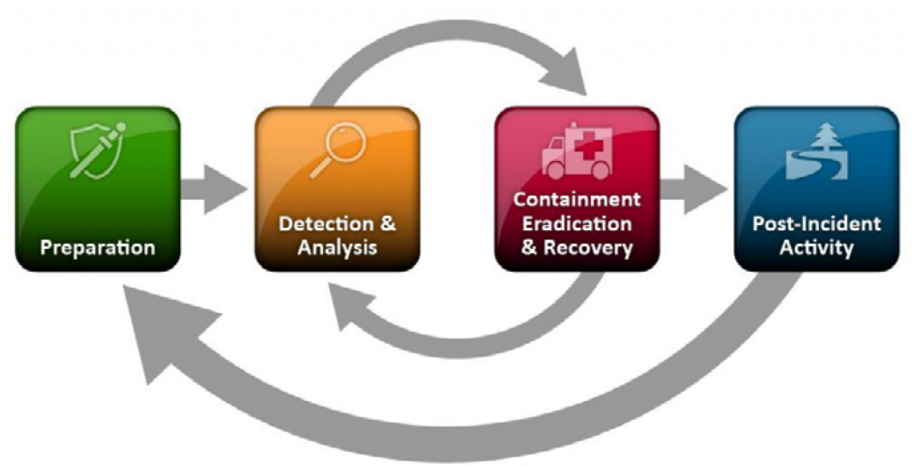
Normalmente devem ser executadas simulações de Resposta a Incidentes anualmente, para avaliar a efetividade do Plano de Resposta a Incidentes e implementar melhorias constantemente.

Devem ser planejados e implementados grupos de resposta a incidentes, cada um respondendo adequadamente à responsabilidade atribuída a ele.

Grupo de contenção do incidente; Grupos de restauração dos serviços; Grupo de comunicação do incidente; Grupo de Segurança da Informação; Grupo de apoio jurídico; entre outros, tudo conforme a realidade da empresa.

106 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net.

Figura 1: Plano de resposta a incidentes



Para que um Plano de Resposta a Incidentes seja efetivo, todas as etapas dos capítulos anteriores devem estar implementadas, a exemplo, Inventário de Ativos, Mapeamento de Dados, Implementação de processos e Implementação de controles. Do contrário, não há como a empresa ter uma ideia sobre como ou quando o incidente ocorreu ou a possibilidade de ocorrer e baseado nisso, nem como se recuperar com sucesso.

A premissa básica para a recuperação de um incidente é que a auditoria esteja ativa e íntegra, conforme preconiza a ISO 27002:2022 o item 5.28, coleta de evidências.

É bom enfatizar que a ISO 27002:2022 pode ajudar com o Plano de Resposta a Incidentes, conforme trazido no item 5.26 - Resposta a incidentes de segurança da informação.

Além da ISO o item 17 da metodologia CIS Critical Security Controls – versão 8 contém uma lista completa e bem detalhada sobre como implementar um Plano de Resposta a Incidentes.

A empresa de posse dessas informações mencionadas, já pode executar a elaboração do plano de resposta a incidentes, bem como colocá-lo em prática e principalmente, testá-la conforme calendário definido de acordo com regras de negócio.

5.17 PLANO DE CONTINUIDADE DO NEGÓCIO

Adiel Ribeiro[107]

Assim como o Plano de Resposta a Incidentes, o Plano de Continuidade de Negócios segue na mesma linha, de ter os times específicos e etapas cumpridas previamente para que o negócio continue em operação durante a disrupção. Ele depende do Plano de Resposta a Incidentes e dita como a empresa deve funcionar durante e após a recuperação de um incidente.

Para ter um Plano de Continuidade de Negócios eficaz, é necessário identificar e valorar os ativos da empresa, de modo que o nível adequado de proteção e funcionalidade mínima aceitável sejam testados e implementados. A exemplo disso, seria os sistemas que não podem ficar inoperantes, pois são críticos ao funcionamento da empresa.

Para que a empresa continue operando normalmente, mesmo em caso de catástrofe, deve haver redundância, backup, proteção em nível de rede, criptografia, auditoria, detecção de anomalias, resposta em tempo real, entre outros, que são itens que permitem com que ela se recupere rapidamente e, na pior das hipóteses, opere em funcionalidade mínima até a normalização. Para empresas que utilizam a tecnologia de nuvem, existe a opção de redundância distribuída, que permite a duplicidade de recursos em localidades dispersas, permitindo a continuidade das operações mesmo que um datacenter inteiro seja destruído.

Itens de extrema importância que devem ser avaliados:

- tempo de recuperação - RTO;
- quantidade de dados que pode ser perdida – RPO;
- nível de impacto do incidente na empresa,

107 Gestão de Vulnerabilidades e Segurança em nuvem AWS. http://nuvym.net.

Baseado nisso, a empresa identifica e disponibiliza os recursos e grupos de pessoas necessários as suas operações em caso de crise.

A ISSO 27002:2022 no item 5.30 traz a questão de prontidão de TIC para continuidade de negócios das empresas a serem desenvolvidas em um Plano de Continuidade de Negócios que atenda aos requisitos da organização.

A título de auxílio para as empresas o NIST CSF é um framework completo e bem detalhado sobre como implementar as etapas que possibilitam que uma empresa continue operando, mesmo em caso de catástrofe. Segue uma tabela demonstrativa:

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Gestão de ativos	Controle de acesso	Eventos e anomalias	Plano de respostas	Recuperação
Gestão de riscos	Treinamento	Monito-ramento contínuo	Comuni-cação	Melhorias
Cadeia de suprimento	Segurança de dados	Processos de detecção	Análise	Comuni-cação

Tabela: NIST CSF

5.18 PLANO DE TREINAMENTOS - A PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Renato Almeida Viana[108]

O direito à privacidade, segundo Carlos Alberto Bittar[109], seria espécie do que a doutrina moderna chama de direitos da personalidade que são: "os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, a honra, a intelectualidade e outros tantos"

Já a segurança da informação é definida na norma técnica ISSO/IEC 27002 como sendo "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."

É importante esclarecer que segurança da informação não se confunde com o direito à proteção de dados pessoais. Ricardo Villas Bôas Cueva[110] esclarece que: "a segurança da informação é indissociável da proteção de dados pessoais. É um pré-requisito, uma condição de possibilidade para que se tutelem efetivamente os direitos dos titulares dos dados pessoas."

---

108 Coordenador do Comitê de LGPD do Centro de Estudos das Sociedades de Advogados de Minas Gerais – CESA/MG. Membro do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Escola Superior da Advocacia. Advogado.

109 - BITTAR, Carlos Alberto. Os Direitos da Personalidade. Rio de Janeiro: Forense Universitária, 1989. Disponível em: https://www.conjur.com.br/2006-set-02/breves_consideracoes_direito_privacidade#:~:text=O%20direito%20%C3%A0%20privacidade%20%C3%A9,defesa%20de%20valores%20inatos%20no. Acesso em: 19 de out, de 2023.

110 CUEVA, Villas Bôas Ricardo. A Lei Geral de Proteção de Dados Pessoais: LGPD - Ed. 2021. Denise de Souza Luiz Francoski, Fernando Antonio Tasso . Editor: Revista dos Tribunais .PARTE I - A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO SETOR PÚBLICO. CAPÍTULO 20. SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS Página RB-20.2 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/259453871/v1/page/RB-20.2. Acesso em: 19 de out, de 2023.

Nesse contexto, a área de Tecnologia da Informação ("TI") do escritório é fundamental para garantir a segurança da informação, porém não deve agir sozinha, sendo imprescindível, para a manutenção e a continuidade de um serviço seguro, o treinamento das pessoas daquela estrutura. Conforme leciona Domingo Montanaro (2022)[111]: "Não é só porque a área de tecnologia da informação lida no dia a dia com sistema de informação que ela obrigatoriamente conhece todas as possíveis fraquezas às quais os sistemas estão sujeitos."

Em outras palavras, para se obter um ambiente mais seguro para as informações é fundamental promover o equilíbrio entre as questões técnicas, as pessoas e os seus aspectos comportamentais.

Domingo Montanaro ainda esclarece que segurança da informação envolve, no mínimo, a[112]:

1. Confidencialidade: somente as pessoas que devem ter acesso àqueles dados efetivamente o terão;
2. Integridade: o conjunto de dados será sempre o mesmo que deve ser, independentemente da mídia, do tempo ou do meio pelo qual foi transmitido.
3. Disponibilidade: o conjunto de dados estará sempre ao alcance de quem precisa acessá-lo.

Ao abordar o programa de gestão de vulnerabilidades em seus pilares (tecnologia, processos e pessoas), Domingo Montanaro explica que, em relação aos colaboradores, é necessário mapear os principais skills que precisam ser melhorados no time e traçar um plano de

111 MONTANARO, Domingo, in NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Editor: Revista dos Tribunais IV – SEGURANÇA DA INFORMAÇÃO. Capítulo 9. Gestão de Vulnerabilidades Capítulo 9. Gestão de Vulnerabilidades .Página RB-10.1 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1. Acesso em: 19 de out, de 2023.

112 MONTANARO, Domingo in , NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Editor: Revista dos Tribunais IV – SEGURANÇA DA INFORMAÇÃO. Capítulo 9. Gestão de Vulnerabilidades Capítulo 9. Gestão de Vulnerabilidades .Página RB-10.1 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1

treinamentos, priorizando aqueles skills que, quando deficientes, facilitam a exploração de vulnerabilidade que denotarão um maior impacto ao negócio[113].

Eliane Silva Ferreira (2020)[114] destaca que "os treinamentos dos colaboradores devem ser constantes, porque sempre surgem novas ameaças e as pessoas precisam estar atualizadas e preparadas diante dos riscos para não tropeçarem em novas ameaças". A autora ensina ainda que os cuidados de treinamento e educação das pessoas devem contemplar tópicos como:

1. a importância do controle de acesso e ambiente organizacional;
2. a apropriada classificação e tratamento da informação de acordo com seu valor como ativo organizacional;
3. tópicos de necessidades orientados de acordo com a análise de riscos;
4. a importância da mesa limpa e tela limpa;
5. providenciar segurança nas comunicações;
6. incrementar o uso com segurança devida e a proteção dos dispositivos móveis;
7. cuidar da devida proteção e privacidade da informação de identificação pessoal;
8. implementar controles criptográficos;
9. realizar backups rotineiros.

Entre os planejamentos preventivos que devem fazer parte do treinamento, destacam-se a implementação de um plano

113 NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Editor: Revista dos Tribunais IV – SEGURANÇA DA INFORMAÇÃO. Capítulo 9. Gestão de Vulnerabilidades Capítulo 9. Gestão de Vulnerabilidades .Página RB-10.1 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1

114 SILVA, Eliane Ferreira da. Boas Práticas em Segurança da Informação. Rio de Janeiro: Edições Dalagaia, 2020.

de contingência e a implementação de controle de acesso dos colaboradores.

O plano de contingência deve estar preparado para ser colocado em prática diante de algum incidente. Ele tem a função de impedir ou amenizar os impactos.

Quanto à implementação de controle de acessos, o seu principal objetivo seria estabelecer parâmetros que darão mais segurança ao acesso, tais como: o computador só deve ser acessado por pessoas autorizadas; limitar o número de tentativas e tempo máximo de logon sem sucesso; registrar a data e a hora do último logon com sucesso.

Outra prática comum de treinamento quanto à segurança da informação é a orientação dos colaboradores em relação às senhas: manter a confidencialidade das senhas, não compartilhando-as com outras pessoas; evitar registrar as senhas fisicamente; selecionar senhas de boa qualidade; alterá-las sistematicamente; alterar as senhas temporárias no primeiro acesso ao sistema, entre outras.

As regras de controle de acesso devem estar devidamente definidas na política da organização, que deverá ser amplamente divulgada para as pessoas daquela estrutura tomarem conhecimento dos requisitos de segurança estabelecidos.

Como visto acima, apesar de a segurança da informação não se confundir com a proteção de dados pessoais, elas estão intrinsicamente relacionadas. Nesse sentido, o art. 46 da LGPD[115] exige que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas

115 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTCAS. SEÇÃO I Da Segurança e do Sigilo de Dados. Art. 46. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 de maio de 2023.

> de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A segurança da informação tem papel fundamental na LGPD, uma vez que, conforme disposto no art. 48[116], o controlador deverá comunicar à autoridade nacional (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A LGPD ainda determina em seu art. 49[117] que:

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Vale ressaltar que a LGPD apresenta ainda uma seção específica (Seção II do Capítulo VII) para tratar das boas práticas e da governança, determinando, em seu art. 50, § 1º[118], que, ao estabelecer regras de boas práticas, o controlador e operador levarão em consideração, em relação ao tratamento de dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de

116 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTCAS. SEÇÃO I Da Segurança e do Sigilo de Dados. Art. 48, §2º, I II. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 de maio de 2023.

117 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTCAS. SEÇÃO I Da Segurança e do Sigilo de Dados. Art. 49. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 de maio de 2023.

118 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTCAS. SEÇÃO I Da Segurança e do Sigilo de Dados. Art. 49. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 de maio de 2023.

tratamento de dados do titular. O § 2º[119] do mesmo artigo estabelece que o controlador poderá implementar programa de governança em privacidade que, no mínimo:

1. demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
2. seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
3. seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
4. estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
5. tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
6. esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
7. conte com planos de resposta a incidentes e remediação; e
8. seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional (art. 50, §3º).

119 Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTCAS. SEÇÃO I Da Segurança e do Sigilo de Dados. Art. 50, §2º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 de maio de 2023.

Portanto, a segurança da informação deve ser um pilar sólido na implementação da LGPD e, para tanto, o plano de treinamento exerce papel fundamental, pois estimula as pessoas a terem uma conscientização dos valores culturais daquela organização, evitando ou minimizando os riscos de incidentes e, por consequência, a segurança das informações envolvidas.

5.19 TREINAMENTOS ISOLADOS POR SETORES

Alan de Souza Pinto[120]

A Lei Geral de Proteção de Dados (LGPD) é uma legislação importante que estabelece regras e diretrizes para o tratamento de dados pessoais por empresas, organizações e entidades públicas no Brasil. Com a entrada em vigor da LGPD, é essencial que as empresas promovam treinamentos para seus setores isolados para que todos os colaboradores compreendam a importância da proteção de dados pessoais.

Para garantir o cumprimento da LGPD, é fundamental que as empresas ofereçam treinamentos específicos para os setores isolados, a fim de conscientizar seus colaboradores sobre a importância da proteção de dados pessoais. Conforme Oliveira (2021), os treinamentos são pertinentes para que os colaboradores entendam as implicações da LGPD em seu trabalho e possam tomar as medidas necessárias para proteger os dados pessoais dos clientes e usuários.

Bioni (2019) destaca que os treinamentos devem abordar não apenas as questões técnicas e legais relacionadas à LGPD, mas também a cultura da privacidade e a importância da proteção de dados para a reputação e a confiança da empresa junto aos clientes e usuários.

O treinamento sobre a LGPD é essencial porque os dados pessoais são informações particulares e, se mal utilizados, podem causar prejuízos irreparáveis aos titulares dos dados. Além disso, a LGPD estabelece sanções para empresas que violarem as regras de proteção de dados, o que pode prejudicar a imagem e a reputação das empresas. Conforme afirmam Soares e Barros (2020), os treinamentos específicos podem contribuir para reduzir os riscos de violações à legislação, já que capacitam os colaboradores a identificarem possíveis

120 Mestre em Inovação Tecnológica, pela UFMG, Bolsista CAPES; Pós-graduado em Direito Digital e Proteção de Dados, pela EBRADI; Pós-graduado em Direito Civil Aplicado, pela PUC Minas; Graduado em Direito, pela PUC Minas; Membro da Comissão de Proteção de Dados da OAB/MG; Consultor em Privacidade e Proteção de Dados Pessoais; Professor; Advogado.

vulnerabilidades e adotar as medidas necessárias para proteger os dados pessoais dos usuários.

Um dos principais objetivos do treinamento é garantir que os funcionários compreendam as regras da LGPD e saibam como aplicá-las no seu trabalho diário. Isso inclui saber como coletar, armazenar e tratar dados pessoais de forma segura e responsável, além de saber como lidar com situações de risco ou incidentes de segurança. Com isso, o treinamento é um suporte aos funcionários para que saibam como lidar com as solicitações dos titulares dos dados, como o direito de acesso, retificação e exclusão das informações pessoais. Essas solicitações precisam ser atendidas dentro dos prazos estabelecidos pela LGPD, o que requer conhecimento e treinamento adequados.

Paralelamente a isso, tal qualificação auxilia a promover a cultura de proteção de dados dentro das empresas, sensibilizando os funcionários sobre a importância da privacidade e da segurança das informações pessoais. Isso é essencial para criar um ambiente de trabalho mais seguro e confiável, além de aumentar a confiança dos clientes e parceiros na empresa. Ademais, pode ser usado para promover uma cultura de responsabilidade social e ética dentro da empresa. Isso inclui promover a conscientização sobre a importância da privacidade e dos dados pessoais, bem como promover ações para proteger a privacidade dos titulares dos dados.

Além disso, o treinamento pode ajudar a criar uma vantagem competitiva para a empresa. Isso porque, ao promover uma cultura de proteção de dados pessoais, a empresa pode ganhar a confiança dos clientes e parceiros, o que pode resultar em um aumento de negócios e melhores oportunidades de parceria.

Os treinamentos também podem auxiliar a criar uma cultura de transparência dentro da empresa. Isso porque a LGPD exige que as empresas informem aos titulares dos dados sobre como seus dados estão sendo tratados. Essa transparência pode ajudar a promover a confiança dos clientes e parceiros na empresa.

Nesse sentido, é uma ferramenta a desenvolver a cultura de inovação dentro da empresa. Isso ocorre porque a LGPD exige que

as empresas desenvolvam soluções inovadoras para lidar com dados pessoais. O treinamento pode ser usado para promover a criatividade e a inovação entre os funcionários. Além disso, o aperfeiçoamento em proteção de dados pode ajudar a promover a cultura de respeito à privacidade dos dados. Isso inclui promover a conscientização sobre a importância da privacidade e do respeito aos direitos dos titulares dos dados.

Além disso, os treinamentos podem ser adaptados às necessidades específicas de cada setor da empresa. Por exemplo, o setor de RH pode precisar de treinamento específico sobre como lidar com dados pessoais de candidatos e funcionários, enquanto o setor financeiro pode precisar de treinamento sobre como lidar com dados bancários e financeiros.

Somado a isso, o treinamento também pode ajudar a identificar e prevenir possíveis violações da LGPD. Isso porque os funcionários treinados serão capazes de identificar situações de risco e tomar medidas para proteger os dados pessoais, reduzindo o risco de violações e sanções. Desse modo, podem ser usados como uma oportunidade para atualizar as políticas internas da empresa relacionadas à LGPD. Isso pode incluir a revisão e atualização dos procedimentos de segurança da informação, a criação de políticas específicas para lidar com dados sensíveis e a definição de diretrizes para lidar com incidentes de segurança.

Outro efeito é quanto ao fortalecimento das parcerias entre empresas e fornecedores, uma vez que as empresas podem exigir que seus fornecedores também promovam treinamentos para seus funcionários. Isso ajudará a garantir que todas as partes envolvidas no tratamento de dados pessoais estejam cumprindo as regras da LGPD. Assim, tem como efeito evitar possíveis perdas financeiras para a empresa. Isso porque as empresas que não cumprem as regras da LGPD estão sujeitas a multas e sanções que podem prejudicar a saúde financeira da empresa. Por isso, o treinamento é uma forma de evitar essas perdas financeiras.

Outra vantagem do treinamento sobre a LGPD é a possibilidade de identificar possíveis vulnerabilidades nos sistemas de segurança da empresa. Isso ocorre porque os funcionários treinados serão capazes de identificar e reportar situações de risco, o que pode levar a melhorias nos sistemas de segurança da empresa.

Além disso, o treinamento pode ser usado para promover a inovação dentro da empresa. Isso ocorre porque as empresas que cumprem as regras da LGPD estão em melhores condições de desenvolver soluções inovadoras que utilizem dados pessoais de forma ética e responsável. Desse modo, também é um meio de promover a conscientização sobre a importância da segurança da informação. Isso inclui a criação de políticas internas para lidar com senhas, acessos aos sistemas, backups e outras medidas de segurança.

Vale ressaltar que o treinamento poderá promover a colaboração entre os setores da empresa. Isso ocorre porque a LGPD exige que todas as áreas da empresa estejam envolvidas no tratamento de dados pessoais. O treinamento pode ser usado como uma oportunidade para promover a colaboração entre as áreas e garantir que todas estejam cumprindo suas obrigações. Outro aspecto a destacar é quanto a atualização regular para acompanhar as mudanças na legislação e nas práticas de segurança da informação. As empresas devem estar sempre atualizadas e conscientes das novidades relacionadas à LGPD para garantir a proteção dos dados pessoais dos titulares.

Entre as questões relevantes que devem ser abordadas nos treinamentos sobre a LGPD estão a definição de dados pessoais e dados sensíveis, as obrigações das empresas em relação ao tratamento desses dados, os direitos dos titulares dos dados, as penalidades por violações da LGPD e as medidas de segurança que devem ser adotadas pelas empresas.

Por fim, é pertinente lembrar que a proteção de dados pessoais é um direito fundamental dos cidadãos e uma obrigação legal das empresas. Os treinamentos sobre a LGPD são essenciais para garantir que as empresas estejam cumprindo suas obrigações e protegendo os dados pessoais dos titulares. A falta de treinamentos adequados

pode resultar em violações da LGPD e consequentes sanções legais e prejuízos financeiros para as empresas. Portanto, é fundamental investir em treinamentos sobre a LGPD para garantir a proteção dos dados pessoais e manter a segurança da informação.

5.20 TREINAMENTO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Alessandra C. Puig Casariego[121]

A conscientização em segurança da informação é um processo importante e essencial que deve ser implementado em todas as organizações para garantir a proteção adequada dos dados e informações confidenciais.

Nesse contexto, apresenta-se a seguir algumas práticas recomendadas para treinar e conscientizar os funcionários e colaboradores acerca do tema segurança da informação:

Política de Segurança da Informação:	Elabore uma política de segurança da informação clara e concisa. A política deve ser escrita de forma clara, objetiva e de fácil entendimento, para que os funcionários e colaboradores possam aderir às suas diretrizes e segui-la facilmente. A política deve incluir informações sobre questões relacionadas ao uso de senhas, controles de acessos, proteção de informações confidenciais, como se evitar phishing, entre outras orientações.

121 Advogada com experiência há mais de 20 anos no mercado financeiro. Gestora de Compliance em instituição financeira, com foco em conformidade regulatória, privacidade e proteção de dados e prevenção à lavagem de dinheiro e financiamento ao terrorismo. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da comissão da Mulher Advogada da OAB/MG. Membro da comissão de direito bancário da OAB/MG. Master of Business Administration - MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas - FGV. Master of Business Administration - MBA em Advocacia Corporativa e Governança pela Escola Superior da Advocacia - ESA OAB. Pós-graduação em Direito Bancário pela Fundação Getúlio Vargas - FGV. Certificação em Compliance pela KPMG. Certificação em Investigações Corporativas pela KPGM. Curso de Extensão em Lei Geral de Proteção de Dados pela PUC-RS.

Treinamentos Periódicos: Realize	Treinamentos regulares e periódicos. É importante realizar treinamentos regulares para manter os funcionários e colaboradores atualizados sobre as ameaças mais recentes e as melhores práticas de segurança. Os treinamentos podem ser realizados presencialmente ou de forma remota (on-line).
Suporte da liderança:	Suporte da liderança: Envolva a liderança. Os líderes da organização/escritório devem ser os principais defensores e embaixadores da segurança da informação e devem participar dos treinamentos, incentivando os funcionários e colaboradores a seguir as políticas e as melhores práticas.
Segurança da Informação na prática:	Utilize exemplos práticos. Ao apresentar exemplos práticos facilitamos o entendimento e a aplicação das informações. Isso pode incluir histórias de phishing ou vazamentos de dados reais que ocorreram em outras empresas.
Simulações:	Faça simulações de ataques. As simulações de ataques podem auxiliar os funcionários e colaboradores a reconhecer os sinais de um ataque real e a agir corretamente em resposta a ele. As simulações podem incluir testes de phishing, simulações de ransomware, entre outras.
Conscientização Periódica:	Mantenha a conscientização regularmente. Não se faz a conscientização em segurança da informação uma única vez. É essencial manter a conscientização de forma periódica e regular para reforçar as melhores práticas com frequência.

Canal de Denúncias:	Incentive os funcionários a relatar problemas segurança da informação, disponibilizando um canal aberto para estas situações, uma espécie de canal de denúncias. Isso pode incluir suspeitas de phishing, perda ou roubo de dispositivos, ou qualquer outro problema relacionado à segurança.

Seguindo as práticas recomendadas acima, a empresa/escritório poderá implementar uma forte cultura de segurança da informação e garantir a proteção adequada de dados e informações confidenciais.

5.21 TREINAMENTO GERAL SOBRE TODAS AS MUDANÇAS EM TERMOS DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Carlos Henrique Almeida Salgado[122]

A adoção de boas práticas e de mecanismos de segurança são obrigações previstas na LGPD para todas as empresas que realizem tratamento de dados pessoais. Uma das formas de demonstrar esse compromisso é por meio da realização de capacitação contínua dos colaboradores e terceiros sobre os limites e riscos relacionados à segurança da informação e ao tratamento adequado dos dados pessoais, instrumentalizado por meio do Plano de Treinamentos quanto à Privacidade, conforme visto no item 4.15.

Após a elaboração do Plano de Treinamentos quanto à Privacidade e Segurança da Informação, é preciso colocá-lo em prática.

A norma ISO 27002 estabelece que os treinamentos em segurança da informação precisam ser realizados de forma regular e passarem por constantes atualizações (ISO 27002, 7.2.2).

Por ser uma lei relativamente nova em nosso ordenamento jurídico, por existirem muitos debates sobre sua aplicação na prática empresarial nacional e pela constante regulamentação pela Autoridade Nacional, as mudanças regulatórias da LGPD demandam um esforço do controlador em se atentar aos impactos dessas medidas sobre as atividades de tratamento de dados pessoais ao seu negócio.

Tal situação exige um maior acompanhamento do controlador das práticas adotadas no mercado e das normas regulatórias relativas à privacidade e segurança da informação para manter seus

122 Advogado com atuação no Terceiro Setor, consultor de Privacidade e Proteção de Dados, com ampla experiência em adequação de organizações à Lei Geral de Proteção de Dados (LGPD); Data Protection Officer (DPO)/Encarregado de Proteção de Dados certificado pela EXIN; Mestrando em Inovação Tecnológica e Propriedade Intelectual pela UFMG; Especialista em Direito Digital pela IBMEC-SP; MBA em Gestão e Segurança da Informação na UNIDERP e Pós-graduado em Compliance e Integridade Corporativa pela PUC MINAS.

regulamentos internos sempre atualizados e para confirmar se, com o passar do tempo, a empresa segue adaptada à lei.

As mudanças regulatórias podem gerar a necessidade de revisões de processos internos ou externos já formalizados e podem resultar na revisão de suas políticas internas, em especial a Política de Privacidade e a Política de Segurança da Informação, interferindo diretamente no risco das atividades operacionais de tratamento de dados pessoais da empresa.

Portanto é de suma importância que a empresa aprimore continuamente seu programa de privacidade, dando cumprimento ao seu plano de treinamento de forma regular e atualizado, para o bom funcionamento empresarial.

O Treinamento Geral sobre todas as mudanças em termos de Privacidade e Segurança da Informação deve ser inserido em forma de um programa de educação continuada na empresa, que permitirá a inserção ao colaborador em um cenário de disciplina, o qual possibilite a exigência da responsabilidade dos colaboradores e atenção aos processos da empresa.

Os Treinamentos regulares possibilitarão aos colaboradores o aperfeiçoamento e o desenvolvimento de habilidades necessárias para a realização de um bom trabalho dentro do escopo de funções exigidas em suas funções sempre atento à política de privacidade dos dados e à política de segurança da informação da empresa.

A comprovação da efetividade desse programa pode ser exigida pela Autoridade Nacional de Proteção dos Dados (ANPD) a qualquer momento. Dessa forma, os treinamentos periódicos são indispensáveis para explicar e fomentar a cultura da Lei Geral de Proteção de Dados na empresa (GUERRA, Elaine).

5.22 RELATÓRIO DE ENTREGA DE PROJETO

Elaine Cristina Oliveira Guerra[123]

O objetivo do relatório de entrega do projeto é fornecer suporte ao cliente na gestão das atividades delineadas no plano de ação. Isso é especialmente relevante, já que, em diversas situações, o cliente decide implementar internamente o plano de ação, independentemente do andamento do projeto. Consequentemente, este relatório de entrega desempenha um papel fundamental para orientar o cliente quanto a cada documento fornecido ao longo do projeto, garantindo, assim, que o projeto não sofra intermediários.

CRONOGRAMA - PROJETO LGPD		

Fonte: Do próprio autor.

É crucial destacar que o relatório serve como uma diretriz para o cliente, no entanto, é fundamental que o consultor forneça assistência abrangente durante todo o andamento do projeto.

123 Mestranda em Inovação Tecnológica e Propriedade Intelectual. Especialista em Direito, Inovação e Tecnologia. Especialista em Direito Digital e Proteção de Dados. Especialista em Advocacia Trabalhista. Pesquisadora da USP/SP. Certificada Internacionalmente pela ISO 27001 (Segurança e Proteção de Dados) e a Privacy Foundation (PDPF), Privacy and Data Protection Practitione (PDPP), obtendo com estas três certificações o título de Data Protection Officer (DPO) pela EXIN. Autora de capítulo de livro jurídico. Autora do "Manual Prático de Adequação da LGPD com enfoque nas Relações do Trabalho". Diretora do Núcleo de Prática de OAB/MG. Pesquisadora da USP/SP e da UFMG/MG. Mentora em projetos de LGPD. Advogada. Professora de Pós-Graduação.

5.23 TERMO DE ENCERRAMENTO DE PROJETO - TEP

Elaine Cristina Pereira dos Santos Nery[124]

O Termo de Encerramento de Projeto (TEP) é a formalização oficial de encerramento de um projeto.

Segundo o Guia PMBOK[125], o processo de finalização de um projeto é o momento em que as atividades de todos os grupos de gerenciamento são concluídas. Em se tratando da formalização do encerramento é preciso deixar clara a necessidade do cumprimento de todas as fases.

De acordo com Project Builder, 2018, o gerente de projeto e toda a equipe envolvida precisam ter o máximo de cuidado ao encerrar o trabalho (ou uma fase dele). O termo processual tem funções específicas, que visam garantir:

- Satisfação com os critérios de sucesso do projeto;
- Verificação e a documentação das entregas;
- Formalização da aceitação das entregas;
- Transferência dos produtos e serviços do projeto para a próxima fase;
- Audição do sucesso ou fracasso;
- Registro das lições aprendidas e informações úteis para o uso futuro da organização;
- Arquivamento de toda a documentação coletada;
- Investigação e documentação do cancelamento do projeto.

124 Advogada. Especialista em Direito Público. Especialista em Privacidade e Proteção de dados. Presidente da Comissão de Proteção de Dados da 27ª Subseção da OAB-Unaí. Consultora em Privacidade e Proteção de Dados Pessoais. Servidora Pública Federal na UFVJM. Membro da Comissão de Proteção de Dados do Estado (OAB/MG), Membro da Comissão de Proteção de Dados da Universidade Federal dos Vales do Jequitinhonha e Mucuri- UFVJM.

125 Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (Guia PMBOK) terceira edição 2004 - Project Management Institute.

A conclusão do projeto com elaboração do TEP precisa conter elementos importantes que visem garantir o aceite sem vícios. Geralmente há uma reunião de encerramento do projeto, na qual será objeto de verificação o alcance, ou não, de todas as finalidades, da mesma forma haverá a análise da existência de algum retorno financeiro ou da possibilidade de o produto ter a qualidade esperada.

Gisele Carvalho, 2002, descreve que gerenciar é prever problemas, planejar e acompanhar a execução. O gerente do projeto deve se manter alerta e flexível com os acontecimentos do dia a dia, mas deve estar atento ao planejamento inicial para não perder o controle. A principal qualidade do gerente de projeto é saber se comunicar bem com todos. Ele é o ponto focal das informações, nele convergem as informações que ele depois deverá processar e divulgar para todo o restante da equipe.

Poderá ser proposta ainda uma reunião com a equipe para análise das lições, na qual deverá ser verificada a existência de problemas, quais as soluções encontradas, e se houve estratégias bem-sucedidas. Ressalta-se que será gerado um documento desta reunião indicando os pontos positivos e negativos das lições observadas.

Outro elemento importante a ser observado é o fator interno, no qual acontece o encerramento por todas as equipes envolvidas, (elemento identificado como administrativas, os quais constarão fluxogramas, planilhas, calendários, informações financeiras, contratos encerrados, contábeis, técnicas, jurídicas, patrimoniais, orçamentária, entre outros).

O Termo de encerramento de projeto é dinâmico e pode ser consultado várias vezes, uma vez que o projeto pode ser encerrado em cada fase, ter várias versões ou ser consultado para analisar algum documento, como relatório de enceramento, cronogramas, pendências, lições aprendidas, histórico de versões dos documentos.

Há ainda o elemento externo, o qual se materializa na forma de aceite, prevendo pendências, versões, relatório final, homologando a entrega do serviço/produto, após revisado os objetivos inicialmente intencionados, e o próprio encerramento do projeto.

Por fim, a importância do TEP é homologar o encerramento do projeto, apontando que (não) restam problemas em abertos no projeto.

6

MELHORIAS CONTÍNUAS

6.1 REVISÃO DOS PROCESSOS/REVISÃO DOS TREINAMENTOS/REVISÃO DAS POLÍTICAS

Emily Matias Assumpção[126]

É sabido que o processo de adequação tem um início, meio, nem sempre terá um fim, visto que existe uma necessidade intrínseca de revisão e melhorias contínuas dos processos, treinamentos e políticas.

Além disso, com o passar do tempo, um processo sem revisão se torna defasado e deixa de gerar os resultados pretendidos, que, no caso da LGPD, é proteger os dados dos titulares.

O que ocorre também de forma muito comum em empresas e escritórios é uma mesma pessoa ser responsável por vários processos, o que pode acarretar a falta de atualização de dados, índices e indicadores de forma devida.

Por esse motivo, após a fase de cumprimento de todos o plano de ação, é necessário que se estabeleça prazos de periodicidade das revisões dos processos da empresa/escritório.

Nesse sentido, o Sebrae Alagoas publicou o artigo como a revisão de processos pode melhorar os resultados do seu negócio? que discorre o seguinte:

> Além disso, a revisão de processos também pode envolver outro tipo de mudança nas empresas. No segundo semestre de 2020, por exemplo, a Coca-Cola criou uma diretoria de inclusão. A intenção é levar mais mulheres aos cargos de liderança, além de buscar a equidade salarial entre os gêneros.
> Esse é uma mudança que pode melhorar o clima organizacional e fazer com que todos os funcionários se sintam ouvidos e valorizados. Com essa alteração

126 Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. DPO Data Protection Office em LGPD (Encarregado de dados), especialista em proteção de dados, especialista em contratos, especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Compliance Officer – CPCA, Especialista em Compliance e Anticorrupção.

> no ambiente, a produtividade tende a crescer e as pessoas passam a se sentir mais inclinadas a "vestir a camisa" da companhia.

Nota-se que a revisão de processos com o objetivo de trazer melhorias contínuas no processo de adequação à LGPD agrega em produtividade, documentos atualizados, diminui os problemas de comunicação interna e externa (titular e ANPD), bem como garante informações fidedignas e a segurança dos dados pessoais.

Logo, é de extrema importância, estabelecer o prazo para revisão dos processos, treinamentos e políticas, indicando o profissional e setor responsável e incluir nos prazos de auditoria e monitoramento.

6.2 REVISÃO E RECICLAGEM DOS TREINAMENTOS INTERNOS - PROMOÇÃO DA PRIVACIDADE E PROTEÇÃO DE DADOS

Gabriel Campos Cunha[127]

Um ponto fundamental para a aderência da organização às diretrizes da LGPD é a realização de treinamentos constantes com os colaboradores e partes interessadas que sejam relevantes para a conformidade do tema na empresa. A constância do treinamento, sua periodicidade, complexidade e demais características depende de cada empresa, sobretudo de acordo com o volume e complexidade do tratamento de dados pessoais que realiza.

Entretanto, um ponto em comum para os diversos tipos de empresa é que, havendo alterações nas normas de referência nos processos em que fluam dados pessoais, elaboração de novos processos que tratem dados pessoais ou mesmo passado muito tempo da realização do último treinamento sobre o tema, recomenda-se que seja realizada uma nova rodada de treinamentos além, é claro, da atualização deles.

É fundamental que todos os treinamentos e suas atualizações envolvam o time de RH ou o departamento de treinamentos. Entretanto os treinamentos e suas atualizações não necessitam que sejam realizados apenas pelo time de RH, podendo serem executados por profissionais de áreas específicas ou terceiros contratados para a tarefa.

A área responsável pela segurança da informação também deve estar envolvida com a elaboração dos conteúdos dos treinamentos, sua atualização e, ainda, no processo de transmissão das informações.

Para auxiliar no processo de realização das reciclagens, alguns passos são importantes:

127 Advogado, consultor em Governança Corporativa, ESG, Compliance, Integridade, Proteção de Dados. Auditor de Sistemas De Gestão da Qualidade, Meio Ambiente, Saúde e Segurança do Trabalho. Auditor da Conformidade Legal nos temas de Proteção de Dados, Privacidade, Meio Ambiente e Saúde e Segurança do Trabalho.

- Definir a periodicidade dos treinamentos, levando em consideração as principais ocasiões de reciclagem descritas acima;
- Selecionar o conteúdo a ser abordado nos treinamentos, considerando os temas descritos acima;
- Definir os colaboradores que devem participar de cada treinamento, de acordo com suas funções e responsabilidades em relação ao tratamento de dados pessoais;
- Agendar as datas e horários dos treinamentos e comunicá-los aos colaboradores;
- Realizar os treinamentos com a participação de um instrutor qualificado e experiente em LGPD, se possível;
- Certificar-se de que os colaboradores compreenderam o conteúdo abordado nos treinamentos e que estão aptos a aplicá-lo em suas atividades diárias;
- Monitorar o cumprimento do procedimento de atualização de treinamentos e realizar ajustes sempre que necessário.

Por fim, sugerimos que, ao realizar a atividade de reciclagem e atualização dos treinamentos, sejam percorridos alguns temas fundamentais conforme os exemplos abaixo:

- Conceitos básicos de privacidade e proteção de dados pessoais;
- Regras e princípios da LGPD;
- Procedimentos de tratamento de dados pessoais;
- Papéis e responsabilidades dos colaboradores e gestores em relação à proteção de dados;
- Processos de gerenciamento de incidentes de segurança e de proteção de dados;
- Novidades e atualizações relevantes em relação à LGPD e à política de privacidade da empresa.

6.3 PADRONIZAÇÃO DAS NORMAS E PROCEDIMENTOS (POP)

Izabela Nunes Pinto[128]

Após identificadas diferenças entre os resultados planejados e obtidos, é hora de aplicar as mudanças que visam à melhoria do plano de ação para adequação à LGPD.

Dessa forma, com o fim de resolver ou mitigar vulnerabilidades, deverão ser executados serviços para promover o alinhamento à LGPD, abrangendo as questões jurídicas, de processos (Governança) e de segurança da informação.

Nesse aspecto, visando à melhoria do processo de adequação, bem como a fim de evitar problemas de execução e garantir a qualidade dos serviços prestados, torna-se indispensável a criação de um documento que registre o passo a passo de uma operação ou processo, garantindo que qualquer funcionário da empresa consiga realizá-lo.

Para que a implementação da LGPD ocorra de forma eficaz, faz-se necessária a estruturação da Padronização das Normas e Procedimentos (POP), com o objetivo de conscientizar os colaboradores sobre as exigências da Lei e as possíveis consequências do seu não cumprimento. Por isso, imprescindível será a criação de uma cultura da proteção de dados pessoais, bem como ações de capacitação interna, que serão fundamentais para que as orientações sejam conhecidas por todos os profissionais da empresa.

A Padronização das Normas e Procedimentos (POP) é um documento com todas as condutas que foram estabelecidas no Plano de Ação para adequação à LGPD. Sua elaboração precisa ser

128 Advogada. Membro nomeado da Comissão de Proteção de Dados da OAB/MG. Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual. Curso de Direito para Startups na Europa (envolvendo GDPR, LGPD e outros temas relacionados ao Direito Digital) pela Academy da Platzi. Finalista, ocupando o 3º Lugar Geral do Brasil da 1a Edição do LawCamp - 1a Competição de Implementação da LGPD no Brasil. Palestrante (Adequação/Implementação da LGPD e Direito Digital).

interdisciplinar e coordenada, pois é a partir dele que diversos serviços para promoção da conformidade à LGPD serão executados. O objetivo é garantir que as atividades sejam executadas de forma padronizada e eficaz.

Vale destacar que o documento de Padronização das Normas e Procedimentos (POP) deverá conter uma linguagem clara e simples, uma vez que é por meio dele que a empresa comunicará aos colaboradores o que deve ser feito e como deve ser feito.

De acordo com o art. 41, §2º inciso III, da LGPD, o DPO deverá orientar os funcionários e os contratados da instituição a respeito das práticas a serem adotadas em relação à proteção de dados pessoais. Assim, é imperioso que, como responsável pelo documento (POP), o DPO, juntamente com a equipe multidisciplinar escolhida pela empresa, periodicamente acompanhe e revise a execução das atividades dispostas no neste.

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> (...)
> § 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.

Para melhor atendimento às exigências da LGPD, recomenda-se a divulgação clara, extensiva e periódica a todos os colaboradores, de modo a conscientizá-los sobre a importância da proteção de dados

pessoais de funcionários, fornecedores, clientes e seus dependentes e da responsabilidade da instituição sobre eles.

Recomenda-se também a criação de um plano de comunicação voltado para o público interno, que possa esclarecer que procedimentos serão adotados pela entidade, em especial aqueles que terão impacto na operação dos serviços e ações, indicando os canais para dúvidas e sugestões.

É imprescindível a capacitação dos colaboradores diretamente envolvidos em atividades que exijam o tratamento de dados, além da realização de uma comunicação extensiva e periódica que conscientize toda a Instituição, disseminando e internalizando a cultura de proteção de dados.

6.4 MONITORAMENTO CONTÍNUO

Priscila Silva Ribeiro[129]
Renato Almeida Viana[130]

Finalizado o projeto de adequação do escritório de advocacia aos ditames previstos na Lei Geral de Proteção de Dados, mostra-se imprescindível o monitoramento interno das novas práticas adotadas de forma periódica, a fim de testar sua eficácia e eficiência.

A verificação do cumprimento das normas e das diretrizes internas adotadas sobre a privacidade de dados se faz imprescindível. É importante que o controlador de dados estabeleça processos, crie normas internas e monitore o seu funcionamento.

Ainda, é importante que as organizações acompanhem as Resoluções publicadas pela Agência Nacional de Proteção de Dados, sobre a aplicação da LGPD, a fim de atuar em conformidade com elas.

No aspecto, a realização de auditorias de forma periódica se mostra importante aliada das organizações, pois analisa de forma aprofundada o efetivo cumprimento da Lei e das boas práticas, conforme determina o artigo 50 da LGPD (BRASIL, 2018).

Por meio da realização do procedimento de forma regular, é possível a identificação robusta pelas organizações sobre os pontos falhos existentes, assim como sobre as melhorias necessárias.

Assim, constatando-se a falha em qualquer aspecto existente, novas atitudes devem ser adotadas a fim de corrigir o erro e manter a segurança e privacidade dos dados pessoais. A adequação a LGD é um projeto vivo, constante, que demanda o efetivo envolvimento de todos os que compõe a organização.

---

129 Data Protection. Advogada. Membro da Comissão de Proteção de Dados da OAB/MG. Consultora em Privacidade de Dados. Certificada em Compliance em Proteção de Dados CPCPD pela Legal Ethics and Compliance. Especialista em Direito Processual Cível pela PUC MINAS. Especialista em Direito e Processo do Trabalho.

130 Coordenador do Comitê de LGPD do Centro de Estudos das Sociedades de Advogados de Minas Gerais – CESA/MG. Membro do Núcleo de Prática da Comissão de Proteção de Dados da OAB/MG. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Escola Superior da Advocacia. Advogado.

O monitoramento contínuo, devidamente documentado, conforme dispõe o artigo 37 da LGPD (BRASIL, 2019), servirá não apenas para que o escritório, teste de forma empírica a efetividade das medidas existentes, mas também embasando eventual relatório de conformidade solicitado Agência Nacional de Proteção de Dados.

Neste sentido é o artigo 37 da sobredita LGPD:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

O relatório de conformidade detalhará as práticas adotadas pelas organizações ao tratar dados pessoais. Ele deverá conter os requisitos mínimos elencados no parágrafo único do artigo 38 da LGPD (BRASIL, 2019), quais sejam: a descrição dos tipos de dados coletados; a metodologia utilizada para a coleta e para a garantia da segurança das informações; a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Constata-se que é recomendável para todo aquele que trata dado pessoal com finalidade econômica, seguir e documentar, as seguintes diretrizes, a fim de se resguardar, bem como atender às solicitações provenientes da ANPD:

- Manter registro das operações de tratamento de dados pessoais que realizar;
- Saber com exatidão quais os dados pessoais coletados pela empresa;
- apenas tratar os dados pessoais de forma justificada e embasada, de acordo com as bases legais previstas na LGPD;
- ter detalhado todo o ciclo de vida dos dados dentro da organização, desde a coleta, até o descarte;
- como os dados foram armazenados durante o período de tratamento dentro da empresa;

- justificar a necessidade quanto à manutenção dos dados mesmo após o término do tratamento? Com qual finalidade?
- Quais as medidas o controlador tem adotado para garantir a segurança e privacidade dos dados pessoais coletados? Estas medidas podem variar desde realização de treinamentos dos empregados, a instalação de antivírus em todos os computadores, restrição de acessos aos dados pessoais tratados pela organização entre outros. O importante é que o escritório comprove a efetiva ação direcionada a fim de mitigar os riscos inerentes.

No contexto dos escritórios de advocacia, tratar dados pessoais é prática imprescindível para a manutenção do negócio. Logo, é importante que as organizações adotem medidas a fim de garantir a segurança dos dados coletados, monitorem a efetividade das medidas adotadas e documentem todos as ações implementadas internamente.

REFERÊNCIA

ABNT NBR ISO/IEC 15504-2: Tecnologia da informação – Processos de ciclo de vida de software, parte 2: Framework para avaliação de processo.

ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO/IEC 27002:2022. Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da Informação.

ABNT ISO GUIA ISO 31000:2009 Gestão de riscos — Princípios e diretrizes *Risk management – Principles and guidelines*ABNT NBR ISO 31000:2009.

ABNT ISO GUIA ISO 73:2009 Gestão de riscos – Vocabulários - 12 páginas.

ANPD; Perguntas Frequentes – ANPD — português (Brasil) (www.gov.br), 2021. [Online] acessado em 20 de outubro de 2023; ANPD;

Afinal, que caminho preciso percorrer para me adequar à Lei Geral de Proteção de Dados Pessoais? Disponível em: https://baptistaluz.com.br/wp-content/uploads/2020/05/BLuz-Metodologia-LGPD.pdf Acessado em 24 de fev. de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, ANPD lança guia orientativo "Cookies e Proteção de Dados Pessoais". Disponível em: (https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/anpd-lanca-guia-orientativo-201ccookies-e-protecao-de-dados-pessoais201d) Acesso em: 05 de maio de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd) Acesso em: 30 de maio de 2023.

BIONI, Bruno. LGPD - Lei Geral de Proteção de Dados Pessoais: Comentários Artigo por Artigo. São Paulo: Revista dos Tribunais, 2019.

BISSOLI CARVALHO, Leandro. LGPD na prática: guia de implementação. São Paulo: Alura, 2020.

BITTAR, Carlos Alberto. Os Direitos da Personalidade. Rio de Janeiro: Forense Universitária, 1989. Disponível em: https://www.conjur.com.br/2006-set-02/breves_consideracoes_direito_privacidade#:~:text=O%20direito%20%C3%A0%20privacidade%20%C3%A9,defesa%20de%20valores%20inatos%20no. Acesso em: 19 de out, de 2023.

BLUM, OPICE; e-book: Melhores práticas de Governança e Conformidade com a LGPD. Disponível em: (https://28563dcd-7409-4c-91-96aa-c236d9f0a871.usrfiles.com/ugd/28563d_6971dd5b77484c2c9d-0c26388a324cf6.pdf). Acesso em: 01 de agosto de 2023.

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (Coordenadores). Data Protection Office (Encarregado): teoria e prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters, 2020;

BRASIL. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF. Abril 2022Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf .Acesso em: 05 jan. de 2023.

BRASIL. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF. Abril 2022 Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 05/01/2023.

BRASIL. Lei nº 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Disponível

em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 06 jan. de 2023.

BRASIL. Lei nº 9.029 de 1995. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: < https://www2.camara.leg.br/legin/fed/lei/2002/lei-10406-10-janeiro-2002-432893-publicacaooriginal-1-pl.html>. Acesso em 02 mar.2023.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2022. Institui o Código Civil. Art. 982. Salvo as exceções expressas, considera-se empresária a sociedade que tem por objeto o exercício de atividade própria de empresário sujeito a registro (art. 967); e, simples, as demais. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm . Acesso em: 05 de jan. 2023.

BRASIL., LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 25 fev. 2023.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Dispõe sobre a Proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências.

BRASIL. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Publicado em 28/01/2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022 376562019. Acesso em: 05 jan. de 2023

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.227.240-SP (2010/0230258-0), Rel. Ministro Luis Felipe Salomão, Data de Julgamento 26/05/2015.

BROGIATO, Arley; RIBEIRO, Filipe; MAIA, Douglas. E-book: UMA VISÃO 360º SOBRE A LGPD: 6 passos para a privacidade de dados. Volume 01. Ano: 2020. Expediente: Textos- GADCOM Comunicação.

BUCCI, Paulo. LGPD - Lei Geral de Proteção de Dados Pessoais: comentada. São Paulo: Forense, 2020.

CÂMARA FEDERAL; Projeto de Lei da Câmara nº 53/2018, 2018. [Online]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/ materia/133486. Acessado em 20 de outrubro de 2023.

CAMARGO, Robson. Matriz de responsabilidades: saiba tudo sobre essa ferramenta de gestão. Universidade de Caxias do Sul, 2020. Disponível em: https://robsoncamargo.com.br/blog/Matriz-de-responsabilidades-no-gerenciamento-de-projetos-saiba-tudo. Acesso em: 04 março 2023.

Candido, Roberto. Gerenciamento de projetos... et. Al.] – Curitiba: Aymará, 2012. - (Série UTFinova), ISBN 978-85-7841-776-5 (material virtual).

Carlos Eduardo Martins Diagramação e revisão de texto realizada no âmbito do acordo de Cooperação Técnica FUB/CDT/Laboratório Latitude e ENAP. © ENAP, 2014 ENAP Escola Nacional de Administração Pública, Diretoria de Comunicação e Pesquisa

CGE-RO, Plano de Ação para Adequação à LGPD. Disponível em:(https://rondonia.ro.gov.br/wp-content/uploads/2022/09/CGE_Plano_de_Adequacao_da_CGE_a_LGPD.pdf). Acesso em: 01 de agosto de 2023.

CGU, Portaria Normativa SE/CGU Nº 12, de 6 de junho de 2022. Disponível em:(https://repositorio.cgu.gov.br/bitstream/1/68252/5/Portaria_Normativa_12_2022.pdf). Acesso em: 27 de fevereiro 2023.

CHAVES, Luis Fernando Prado. Responsável pelo tratamento, subcontratante e DPO. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). Comentários ao GDPR – Regulamento Geral de Proteção de Dados da União Europeia São Paulo: Ed. RT, 2018. p. 134-135.

CHECKLIST DE MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf> Acessado em 20 de outubro de 2023.

CIS Critical Security Controls. Disponível em: <https://www.cisecurity.org/controls_pre>. Acessando em: 29 de maio de 2023.

CIS Critical Security Controls. Disponível em: <https://www.cisecurity.org/controls_pre>. Acessando em: 20 de outubro de 2023

COMISSÃO EUROPEIA, article 29 data protection working party, Opinion 1/2010 on the concepts of "controller" and "processor", 2010, [Online] Disponível em: MARKT-2001-05060-00-00-FR-TRA-00 (EN) (europa.eu), Acessado em 20 de outubro de 2023.

Comunicação de incidente de segurança. https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis Acessado em 19 de outubro de 2023.

CONJUR, Escritório orienta empresas a se adequarem. Disponível em: (https://www.conjur.com.br/2020-jul-25/escritorio-orienta-empresas-adequarem-lgpd). Acesso em: 01 de agosto de 2023.

CUEVA, Villas Bôas Ricardo. A Lei Geral de Proteção de Dados Pessoais: LGPD - Ed. 2021. Denise de Souza Luiz Francoski, Fernando

Antonio Tasso . Editor: Revista dos Tribunais .PARTE I - A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO SETOR PÚBLICO. CAPÍTULO 20. SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS Página RB-20.2

Curso de Compliance em Proteção de Dados. LEC. Legal Ethics Compliance. Coordenação: GONSALES, Alessandra; CINELLI, Gianfranco Fogaccia; CHO, Tae Young. Páginas 46 e 47.

Curso de Compliance em Proteção de Dados. LEC. Legal Ethics Compliance. Coordenação: GONSALES, Alessandra; CINELLI, Gianfranco Fogaccia; CHO, Tae Young. Páginas 117, 323 e 325.

Curso de Compliance em Proteção de Dados. LEC. Legal Ethics Compliance. Coordenação: GONSALES, Alessandra; CINELLI, Gianfranco Fogaccia; CHO, Tae Young. Páginas 117, 323 e 325.

Curso Legítimo interesse teoria e prática. Udemy. DODT, Carlos, 2021.

DA MOTA ALVES, LGPD: Mais que uma lei de obrigações, uma lei de direitos – Migalhas, 2021, [Online]. Disponível em: https://www.migalhas.com.br/ depeso/342256/lgpd-mais-que-uma-lei-de-obrigacoes-uma-lei-de-direitos. Acessado em 20 de outubro de 2023.

Dicionário Online de Português. https://www.dicio.com.br/legitimo/

FAPES, Regimento Interno do Comitê de Proteção de Dados. Disponível em:(https://www.fapes.com.br/arquivos/20220711/041ae53a-67fe415d8e1ebc32606b5f71.pdf). Acesso em: 27 de fevereiro 2023.

FILHO, José Bezerra da Silva. O Gerenciamento de Projetos tem um Novo Direcionamento com o Guia PMBOK® – 7ª Edição. 2021. Disponível em (https://www.linkedin.com/pulse/um-primeiro-olhar-sobre-o-novo-guia-pmbok-7%C2%AA-edi%-

C3%A7%C3%A3o-jos%C3%A9/?originalSubdomain=pt) acesso em 25 de fevereiro 2023.

Gisele S. B. CARVALHO Arquiteta com especialização em Gerenciamento de Projetos, Diretora da Myssior Gestão de Projetos gisele@myssior.com.br Associação Brasileira dos Escritórios de Arquitetura, ASBEA – Manual de Escopo de Projetos Fabrício, M. M. Projetos Simultâneos na Construção de Edifícios. Tese (Doutorado) – Escola Politécnica. Universidade de São Paulo, São Paulo, 2002 – 308p.

GENERAL DATA PROTECTION REGULATION. GDPR. Regulation (EU) 2016/679. 25 de Maio de 2018. Disponível em: https://gdpr-info.eu/. Acesso em: 09 jan. de 2023.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

Gov.br. Guias e modelos. Acessado em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd> >. Acessado em: 29 de maio de 2023.

GOV.BR, A Política de Segurança da Informação e a Estrutura de Governança da CGU. Disponível em: (https://www.gov.br/cgu/pt-br/acesso-a-informacao/privacidade-e-protecao-de-dados/a-politica-de-seguranca-da-informacao-e-a-estrutura-de-governanca-da-cgu). Acesso em: 27 de fevereiro 2023.

GOV.BR, Plano de Ação para adequação à LGPD. Disponível em: (https://www.gov.br/agu/pt-br/composicao/ouvidoria-1/ouvidoria/plano-de-acao-para-adequacao-a-lgpd). Acesso em: 01 de agosto de 2023.

Guerra, Elaine Manual Prático de Adequação à LGPD: com enfoque nas relações de trabalho/Elaine Guerra, Selma Carloto. - 1. ed. - São Paulo: Ltr, 2021.

Guia de Elaboração de Inventário de Dados Pessoais – LGPD. Disponível em < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf >. acesso em 19 de outubro de 2023.

Guia do Framework de Privacidade e Segurança da Informação. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de dados/ppsi/guia_framework_psi.pdf

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, maio de 2021, Brasília/DF. [Online] disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acessado em 20 de outubro de 2023;

ISO 27002. Disponível em: https://www.iso.org/standard/75652.html - Acessado em 20 de outubro de 2023

ISO.ORG <https://www.iso.org/standard/71670.html> Acessado em 20 de outubro de 2023

Joia, Luiz Antônio. Gerenciamento de riscos de projetos... [et. Al.] – 3º edi. - Rio de Janeiro: Editora FGV, 2013.

Leme e Black, Jurisprudência e legislação sanitária comentadas Lei Geral de Proteção de Dados e segurança da informação na área da saúde- Cad. Ibero-amer. Dir. Sanit., Brasília, 9(3): jul./set., 2020, 218,

disponível em: <http://dx.doi.org/10.17566/ciads.v9i3.690>. Acesso em: 23 fevereiro 2023.

LIA *Legitimate Interests Assessment* e sua relação com a LGPD. Disponível em: <https://cipher.com/pt/blog/lia-legitimate-interests-assessment-e-sua-relacao-com-a-lgpd/>. Acesso em 08 de maio de 2023.

Legitimate interests assessment o que e quando deve ser utilizado. Disponível em: <https://www.fius.com.br/legitimate-interests-assessment-o-que-e-quando-deve-ser utilizado/>Acesso em 08 de maio de 2023.

MACHADO, Ana Paula; ALVES, André; MALDONADO, Viviane (Coord.). Manual de implementação da LGPD: Lei Geral de Proteção de Dados Pessoais. 1. ed. São Paulo: Editora Revista dos Tribunais, 2021.

MALDONADO, V. N. (Coordenadora). LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. São Paulo: Thomson Reuters, 2019.

MAIA, Fernanda (Coordenadora); LGPD: Aplicação Prática das Bases Legais – Acadêmico - Creative Commons Publicado em 19.08.2020, [Online] Disponível em: ebook.indd (bibliotecadesegurança.com.br), 2020. Acessado em 20 de outubro de 2023.

Matriz RACI: o que é, benefícios e como utilizar? Fia Business School, junho de 2020. Disponível em: https://fia.com.br/blog/matriz-raci-o-que-e-beneficios-e-como-utilizar/. Acesso em 04 de março de 2023. Curso PM3. Disponível em: https://cursospm3.com.br/blog/matriz-raci/?amp&gclid=Cj0KCQiA9YugBhCZARIsAACXxeIZQz5ExJbWyZGmrHw7kDSuzuBvmK4iF24OGrFZqt3D-5ZjOM5mBm8aAqAQEALw_wcB. Acesso em: 04 março 2023.

MARTINS, Letícia de Souza. Scrum framework e sua usabilidade com a ferramenta de princípios ágeis, Trello. Disponível em (https://m.

uniara.com.br/arquivos/file/cca/artigos/2016/leticia-souza-martins.pdf) acesso em: 25 de fevereiro 2023.

MENEZES, Ana Paula. LGPD e Recursos Humanos: Os Impactos da Lei nas Relações de Trabalho. Revista Síntese Trabalhista e Previdenciária. v. 29, n. 343, 2021.

MONTES, Eduardo. Introdução ao Gerenciamento de Projetos: Como gerenciar projetos pode fazer a diferença na sua vida, 1ª Ed. São Paulo; 2017.

MONTANARO, Domingo, in NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Editor: Revista dos Tribunais IV – SEGURANÇA DA INFORMAÇÃO. Capítulo 9. Gestão de Vulnerabilidades Capítulo 9. Gestão de Vulnerabilidades .Página RB-10.1 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1. Acesso em: 19 de out de 2023,.

MONTANARO, Domingo in , NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Editor: Revista dos Tribunais IV – SEGURANÇA DA INFORMAÇÃO. Capítulo 9. Gestão de Vulnerabilidades Capítulo 9. Gestão de Vulnerabilidades .Página RB-10.1. https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1. Acesso em: 19 de out. 2023.

MONTANARO, Domingo. LGPD: Lei Geral de Proteção de Dados Pessoais - Manual de Implementação - Ed. 2022. Capítulo IV – Segurança da Informação. Capítulo 9, Gestão de Vulnerabilidade. Disponível em: Página RB-10.1 https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1. Acesso em: 19 de out de 2023.

NIST CSF. Disponivel em: NIST Cybersecurity Framework | NIST – Acessado em 20 de outubro de 2023

NÓBREGA, Maldonado Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais – Manual de Implementação, Gestão de Vulnerabilidades, Ed. 2022. Revista dos Tribunais. Capítulo 9. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/206179087/v3/page/RB-10.1. Acesso em: 19 de out de 2023.

OLIVEIRA, Priscilla M. de. A importância dos treinamentos em proteção de dados pessoais: análise do contexto brasileiro. Revista Brasileira de Direito Digital e Tecnologia da Informação, v. 6, n. 1, p. 51-69, jan./jun. 2021.

OLIVEIRA, Renato. LGPD: Da teoria à prática. São Paulo: Novatec, 2020.

O que a LGPD diz sobre o consentimento do cidadão em relação a seus dados pessoais. Disponível em https://guialgpd.com.br/o-que-a-lgpd-diz-sobre-o- consentimento/. Acesso em 20/10/2023.

O que é metodologia Scrum? disponível em (https://www.digite.com/pt-br/agile/metodologia-scrum/) acesso em: 24 de fevereiro 2023.

PMI - PROJECT MANAGEMENT INSTITUTE. Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, terceira edição, Pennsylvania: PMI, 2004.

PMI - PROJECT MANAGEMENT INSTITUTE. Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, sexta edição, Pennsylvania: PMI, 2017

PMI. Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK), Project Management Institute, 6ªed – Newtown Square, PA: Project Management Institute, 2017. © 2021 Project BuilderPolítica de privacidadeSistema de Gestão de Projetos Asana https://asana.

com/pt/templates/project-closure 3/4 . Escrito por Project Builder em 19/11/2018. Postado em Projetos.

PMBOK) terceira edição 2004 - Project Management Institute. Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos.

PORTOS DO PARANÁ, Comitê Gestor de Proteção de Dados Pessoais. Disponível em: (https://www.portosdoparana.pr.gov.br/Pagina/Comite-Gestor-de-Protecao-de-Dados-Pessoais#:~:text=O%20Comit%C3%AA%20Gestor%20de%20Prote%C3%A7%C3%A3o,ordin%C3%A1rias%20com%20aquelas%20do%20Comit%C3%AA). Acesso em: 27 de fevereiro 2023.

PRIVACY FRAMEWORK. Disponível em: <https://www.nist.gov/privacy-framework/nist-sp-800-115> Acessando em: 29 de maio de 2023.

Project Builder, PMPOK. Disponível em (https://www.projectbuilder.com.br/blog/o-que-e-pmbok/) acesso em: 25 de fevereiro 2023.

RABELO, Guilherme, O que é 5W2H e como ela pode aumentar produtividade? Disponível em (https://www.siteware.com.br/metodologias/o-que-e-5w2h/) acesso em: 19 de março 2023.

Relatório de conformidade é chave para adequação à LGPD, escreve Breno Oliveira. Disponível em https://www.poder360.com.br/opiniao/relatorio-de-conformidade-e-chave-para-adequacao-a-lgpd-escreve-breno-oliveira/. Acesso em 19/10/2023.

Relatório de conformidade é chave para adequação à LGPD, escreve Breno Oliveira. Disponível em https://www.poder360.com.br/opiniao/relatorio-de-conformidade-e-

Regulamento de Comunicação de Incidentes de Segurança de Dados Pessoais. Disponível em: <https://www.gov.br/participamais-brasil/regulamento-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais> Acesso em: 21 de outubro de 2023.

SEBRAE, Como a revisão de processos pode melhorar os resultados do seu negócio? Disponível em: <https://blog.sebraealagoas.com.br/gestao/como-a-revisao-de-processos-pode-melhorar-os-resultados-do-seu-negocio/> Acesso em: 04 de maio de 2023.

SEBRAE, Entenda o que é pop e qual sua importância para gestão da qualidade. Disponível em: (https://sebrae.com.br/sites/PortalSebrae/artigos/entenda-o-que-e-pop-e-qual-sua-importancia-para-a-gestao-da-qualidade,58abbbd38f896810VgnVCM1000001b00320aRCRD). Acesso em 02 de agosto de 2023.

SIEGHART, Paul. Da Privacidade à Proteção de Dados Pessoais. Ed. 2021. Editora Revista dos Tribunais. Capítulo 1 Pessoa e Privacidade na Sociedade da Informação. 1.1 Um panorama do direito à privacidade. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-1.1. Acesso em: 19 de out, 2023.

SILVA, Eliane Ferreira. Boas Práticas em Segurança da Informação. Rio de Janeiro. Edições Dalagaia, 2020.

SILVA, Fabrício Lima; PINHEIRO, Iuri; BOMFIM, Volia. Manual do Compliance Trabalhista. 2ª edição. Salvador.JusPODIVM.2021

SILVA, Laércio de Souza et al. Proteção de Dados desafios e soluções na adequação à Lei. Ed. 2ª, Editora Forense. 2021.

SOARES, Rafael; BARROS, Tiago. Treinamentos em proteção de dados pessoais: uma análise da Lei Geral de Proteção de Dados. In: Anais do 8º Congresso Internacional de Direito e Contemporaneidade,

2020. Disponível em: https://doi.org/10.26512/direitocontemporaneidade.v8i1.36602. Acesso em: 23 abr. 2023.

SOUZA, Adriano; MELO, Gabriel. Proteção de dados pessoais: Lei Geral de Proteção de Dados Pessoais – LGPD - Lei nº 13.709, de 14 de agosto de 2018. São Paulo: Revista dos Tribunais, 2020.

TAFAILE, Cinthia. LGPD e os escritórios de advocacia: muito além de um novo nicho de mercado. Nextlaw academy. Data de publicação: 04/02/2021. Disponível em: https://www.nextlawacademy.com.br/blog/lgpd-e-os-escritorios-de-advocacia-muito-alem-de um-novo-nicho-de-mercado#:~:text=Ou%20seja%2C%20a%20LGPD%20atinge,%2C%20associados%2C%20fornecedores%2C%20etc. Acesso em: 05 Jan de 2023.

Temas de repercussão geral. Disponível em: <https://www.tst.jus.br/documents/10157/71997c14-b8e2-4104-866c-0218709bb8e9>. Acesso em 23 de março de 2023.

VAINZOF, Rony. In: MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato (Coord.). LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2022. Revista dos Tribunais LEI 13.709, DE 14 DE AGOSTO DE 2018 CAPÍTULO I. DISPOSIÇÕES PRELIMINARES Art. 5º. Página RL-1.2https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.2

VAINZOF, Rony. In: MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato (Coord.). LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2021. Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018. CAPÍTULO I. DISPOSIÇÕES PRELIMINARES. Art. 5º. Página RL-1.2 https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v3/page/RL-1.2

VAINZOF, Rony. In: MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato (Coord.). LGPD: Lei Geral de Proteção de Dados

Pessoais Comentada - Ed. 2022. Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018. CAPÍTULO I. DISPOSIÇÕES PRELIMINARES. Art. 5º.. Página RL-1.2

https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.2

VAINZOF, Rony. In: MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato (Coord.). LGPD: Lei Geral de Proteção de Dados Pessoais Comentada - Ed. 2021. Revista dos Tribunais. LEI 13.709, DE 14 DE AGOSTO DE 2018 CAPÍTULO I. DISPOSIÇÕES PRELIMINARES Art. 5º. Página RL-1.2 https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v3/page/RL-1.2

ZHUKOVA, Nathália. Matriz RACI ou de responsabilidade: quando e como deve ser aplicada. Semrusk Blog, 2022. Disponível em https://pt.semrush.com/blog/matriz-raci/. Acesso em: 04 março 2023.

APÊNDICE

ANEXO A - Modelo de proposta técnica e comercial

(*Local e Data*)

A/C xxxxxxxxx (*indique o destinatário da proposta*)

REF - Proposta de adequação e implementação da LGPD (especificar quais serviços, por exemplo: adequação à LGPD ou implementação da LGPD.)

Prezados,

Agradecendo a confiança e atendendo à solicitação, formalizamos nossa proposta de honorários para (*especificar quais serviços, por exemplo: adequação à LGPD ou implementação da LGPD*).

QUEM SOMOS

Somos um escritório especializado em privacidade e proteção de dados, formado por sócios com especialização no tema. *(Neste tópico você apresentará o seu escritório, profissionais, área de atuação, especialidades, formações entre outros pontos fundamentais).*

ONDE ATUAMOS

(Neste tópico você apresentará a área de atuação do seu escritório).

QUAIS SÃO AS VANTAGENS DOS NOSSOS SERVIÇOS?

Equipe especializada: Contamos com uma equipe de profissionais com especialização no tema privacidade e proteção de dados para todos os itens da Lei Geral de Proteção de Dados (regulatório, legal, segurança da informação, TI).

Segurança Jurídica: Todo o trabalho do escritório é realizado por profissionais e advogados especialistas.

Tratamento Personalizado: Nosso trabalho é realizado e desempenhado conforme a necessidade de cada cliente.

ESCOPO E OBJETIVOS

Os trabalhos desenvolvidos terão por objeto *(especificar o objeto da prestação de serviços - Se o escopo do trabalho contemplar a*

implementação e adequação à LGPD, recomendamos seguir o passo a passo abaixo. Lembrando que cada etapa do trabalho deve ser cuidadosamente especificada no passo seguinte.

PLANO DE AÇÃO PARA IMPLEMENTAÇÃO E ADEQUAÇÃO À LGPD:

Mapeamento e registro das atividades de tratamento *(recomenda-se a elaboração de um questionário para ser respondido por todas as áreas).*

Estruturação de Governança em Privacidade: definir papéis e responsabilidades; estabelecer a estrutura de comitês sobre o tema, qual ou quais serão as áreas responsáveis pelo assunto, quem será o DPO (encarregado de dados) e quem serão os embaixadores de privacidade; estabelecer a estrutura de governança de dados, incluindo o mapeamento dos dados, definição das bases legais, elaboração das políticas de expurgo ou retenção de dados, gestão de terceiros, gestão de incidentes e atendimento ao exercício dos direitos dos titulares.

Elaboração ou Revisão da Política de Segurança da Informação e de Privacidade.

Adequação Jurídica: realizar a revisão dos Contratos e avisos de privacidade nos sites e política de cookies.

Implementação do Programa de Conscientização/Aculturamento que deve conter a realização de palestras e treinamentos para os colaboradores, elaboração de cartilhas.

CRONOGRAMA

Apresente o cronograma detalhado de cada etapa do trabalho.

ORÇAMENTO

Descreva detalhadamente o investimento para a prestação dos serviços propostos.

PRAZO DE VALIDADE DESTA PROPOSTA

Descreva o prazo de validade da Proposta.

PRIVACIDADE E PROTEÇÃO DE DADOS

Descrever o ciclo de vida dos dados pessoais na proposta técnica e comercial.

Em caso de aceitação desta proposta, formalizamos a parceria profissional mediante elaboração e assinatura do respectivo "Contrato de Prestação de Serviços de adequação e implementação da LGPD", onde serão definidas as demais condições da atuação do escritório contratado.

Colocamo-nos à disposição para quaisquer outros esclarecimentos e aguardamos um retorno a fim de que possamos iniciar os trabalhos.

Texto elaborador por: Alessandra C. Puig Casariego

ANEXO B - Modelo de contrato de prestação de serviços

CONTRATADA: qualificação completa da/a contratada/o

CONTRATANTE: contratante

Decidem as partes, na melhor forma de direito, celebrar o presente CONTRATO DE PRESTAÇÃO DE SERVIÇOS, que vai se reger mediante as cláusulas e condições adiante estipuladas.

CLÁUSULA PRIMEIRA – DO OBJETO

Descrever o objeto do contrato

CLÁUSULA SEGUNDA – DO ESCOPO E OBJETIVOS DO TRABALHO

Descrever detalhadamente o escopo do trabalho e seus objetivos

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA

Descrever as obrigações da contratada

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATANTE

Descrever as obrigações da contratante

CLÁUSULA QUINTA - DO PREÇO E DAS CONDIÇÕES DE PAGAMENTO

Descrever o valor dos serviços e as condições para pagamento

CLÁUSULA SEXTA – DO DESCUMPRIMENTO

Descrever as consequências em caso de descumprimento de uma das partes

CLÁUSULA SETIMA – DO PRAZO DE VALIDADE

Descrever o prazo de validade do contrato

CLÁUSULA OITAVA – DA PRIVACIDADE E DA PROTEÇÃO DE DADOS

Descrever as condições específicas do contrato que envolvem a privacidade a proteção de dados.

CLÁUSULA NONA – DO FORO

Descrever o foro onde serão resolvidos os litígios referentes a este contrato.

Texto elaborador por: Carlos Henrique Almeida Salgado

ANEXO C – Modelo de termo de abertura de projeto - TAP

IDENTIFICAÇÃO DO PROJETO
Projeto:
Área:
Início Previsto:
Término Previsto:

DETALHAMENTO DO PROJETO

É o momento de descrever e apontar o início, as premissas, as restrições, de demostrar quem será o gerente do projeto e seus auxiliares, bem como outras informações pertinentes ao detalhamento do projeto.

EQUIPE EXECUTORA DO PROJETO
Nome:
Papel:
Telefone:
E-mail:
DEMANDA
Descrever o que será feito.

JUSTIFICATIVA

Apontar quais foram os motivos que justificaram a propositura do projeto;

OBJETIVOS/BENEFÍCIOS

Inserir objetivos gerais e específicos;

ESCOPO DO PRODUTO

O "escopo do projeto", define "o trabalho que precisa ser realizado para entregar um produto, serviço ou resultado com as características e funções especificadas" (PMI, 2004, p. 104).

FORA DO ESCOPO

Descrever o que será considerado como fora do escopo.

CRONOGRAMA

Retrata início e fim para concluir o projeto, podendo predizer o tempo em que cada fase será desenvolvida e concluída, horas destinadas por dia, mês, e ano dependendo do tamanho da empresa.

Fases do Projeto: 1º mês; 2º mês, 3º mês....

CUSTO ESTIMADO

Descrever o custo estimado com o "investimento"

RISCOS INICIAIS DO PROJETO

Descrever os riscos e lacunas iniciais considerados no projeto;

Apontar os principais impactos dos riscos constatados e o seu responsável;

Descrever o plano de ação para cada risco e como serão monitorados e com qual frequência, entre outros.

APROVAÇÃO DO PROJETO

Nome:

Cargo:

Data:

Texto elaborador por: Elaine Cristina Pereira dos Santos Nery

ANEXO D – Modelo de termo de encerramento de projeto – TEP

1. IDENTIFICAÇÃO DO PROJETO

1.1 Projeto Corporativo: [Nome do projeto]

1.2 Unidade Idealizadora (demandante): [Setor que demandou o projeto;

Nome e cargo da pessoa que idealizou o projeto]

1.3 Gerente de Projeto: [Nome do Gerente do projeto; Telefone e-mail].

2. ENTREGAS DO PROJETO

2.1 Lista de produtos/serviços do projeto gerados e entregue(s) ao(s) cliente(s): [relacione todos os produtos/serviços que foram entregues no decorrer do projeto].

2.2 Documentos de gerenciamento de projetos: [relacione os documentos de gerenciamento gerados durante o projeto, tais como: Termo de abertura do projeto;

Plano Geral do Projeto; Relatórios de Acompanhamento do Projeto; Documentos relacionados às mudanças, que se fizerem pertinentes].

2.3 Outros documentos: [relacione outros documentos utilizados durante o projeto, tais como: documentação legal; processos utilizados e documentos técnicos que contribuíram com o projeto.

3. CONSIDERAÇÕES FINAIS SOBRE O PROJETO

Descreva, de forma geral, se o projeto atingiu o resultado, objetivos, necessidades desejadas e o nível de satisfação dos interessados.

3.1. Considerações do Gerente

Esta parte, deverá ser preenchida pelo Gerente do Projeto com suas considerações.

4. PENDÊNCIAS
Classificação/Pendências:
Resolução:
Responsável:
Unidade Operacional:

5. LIÇÕES APRENDIDAS
Descrever as Lições aprendidas (previsíveis ou imprevisíveis)
Fases do projeto:
Fato/área do conhecimento:
Categoria:
Previsíveis/Não:
Favorável/desfavorável:
Aprendizado adquirido:

6. MOTIVO DO ENCERRAMENTO DO PROJETO
( ) Projeto Finalizado
( ) Projeto Cancelado
(...) Projeto adiado

7. RELATÓRIO
Descrever o motivo do encerramento e/ou do cancelamento.
Descrever de forma resumida - avaliação de todo o projeto, analisando se os objetivos foram atingidos.

8. ACEITE E APROVAÇÃO DO PROJETO
Data:
Aprovado por:
Assinatura:

Texto elaborador por: Elaine Cristina Pereira dos Santos Nery

ANEXO E – Modelo de termo de nomeação do encarregado de proteção de dados (DPO)

Neste ato, [Qualificação completa], denominado "Controlador", nomeia como Encarregado pelo Tratamento de Dados Pessoais, nos termos do art. 41, da Lei Geral de Proteção de Dados Pessoais (LGPD), o xxx, nacionalidade, estado civil, profissão, inscrito no CPF sob o nº xxx, com domicílio profissional no endereço xxx, e-mail: xxxxxx

A nomeação entra em vigor na data de assinatura do presente termo e possui vigência de xxx (xxx) meses, sendo que ao final do prazo inicial de vigência passará a vigorar por prazo indeterminado.

O Encarregado pelo Tratamento de Dados Pessoais executará as seguintes tarefas em conformidade com o art. 41, §2º, da Lei Geral de Proteção de Dados Pessoais:

*Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

*Receber comunicações da autoridade nacional e adotar providências;

*Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

*Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O Encarregado está ciente que a Agência Nacional de Proteção de Dados ("ANPD") poderá estabelecer normas complementares sobre definição e atribuições do encarregado, conforme disposto no art. 41, §3º, da LGPD, hipótese na qual tais atribuições deverão ser automaticamente incorporadas ao presente termo.

Caso o Encarregado não aceite assumir tais atribuições e assim se manifeste expressamente, no prazo de xxx (xxx) dias contados da divulgação pela ANPD, o presente termo ficará automaticamente sem efeito, podendo o Controlador indicar novo encarregado.

O Encarregado concorda e aceita em fornecer suas informações de contato e identidade de forma clara e objetiva no site eletrônico do

Controlador, em cumprimento ao art. 41, §1º, da LGPD, pelo tempo da vigência deste termo.

A ANPD poderá determinar ao Controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, observados os segredos comercial e industrial (art. 38, LGPD). Neste caso, o Encarregado deverá auxiliar o Controlador na elaboração do referido Relatório.

O Encarregado garante observar e cumprir fielmente todas as medidas de segurança, técnicas e administrativas adotadas pelos agentes de tratamento aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentes ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, na forma do art. 46 da LGPD.

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (art. 37, LGPD), assumindo o Encarregado a responsabilidade por manter tais registros.

O Encarregado deverá comunicar imediatamente ao Controlador a ocorrência de incidente de segurança que possa acarretar risco ou danos aos titulares dos dados pessoais. O Controlador, por sua vez, com a assessoria do Encarregado, deverá comunicar à autoridade nacional e ao titular sobre a ocorrência (art. 48 da LGPD).

A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo (art. 48, §1º, LGPD):

*A descrição da natureza dos dados pessoais afetados;

*As informações sobre os titulares envolvidos;

*A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

*Os riscos relacionados ao incidente;

*Os motivos da demora, no caso de a comunicação não ter sido imediata; e

*As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Preceitua o art. 42 da LGPD que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Dispõe ainda o art. 43. Da LGPD que os agentes de tratamento só não serão responsabilizados quando provarem:

*Que não realizaram o tratamento de dados pessoais que lhes é atribuído;

*Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

*Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Caso o dano causado seja comprovadamente atribuído ao Encarregado, este deverá ressarcir integralmente o Controlador e/ou operador pelo valor corrigido monetariamente, acrescido de multa de xxx% (xxx), sem prejuízo da rescisão imediata deste Contrato.

O Encarregado declara que as atividades que desempenhará de acordo com esse termo não serão objeto de qualquer remuneração adicional, razão pela qual nada poderá ser exigido nesse sentido do Controlador.

Cidade e data

Controlador:

Encarregado:

Texto elaborador por: Renato Almeida Viana

ANEXO F – Modelo de contrato de prestação de serviços de encarregado de proteção de dados (DPO)

I – PARTES

xxxxxxx, pessoa jurídica de direito xxxxx, inscrita no CPNJ/CPF nº xxxxx, com sede no endereço xxxxx, cidade, Estado, CEP xxxxx, neste ato representado por seus representantes legais constituídos no contrato social, doravante denominado "Controlador/Contratante" e;

xxxxxx, pessoa física/jurídica], inscrita no CPNJ/CPF nº xxxxx, com sede no endereço xxxxx, doravante denominado "Encarregado/ Contratado".

CONTROLADOR e ENCARREGADO doravante denominados, em conjunto "Partes" e, isoladamente, "Parte";

II - CONSIDERANDOS

II.1 - Considerando que o art. 5º, inciso VIII, da Lei Geral de Proteção de Dados ("LGPD"), determina que o encarregado é a 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).

II.2 - Considerando que o art. 41 da LGPD determina que o controlador deverá indicar encarregado pelo tratamento de dados pessoais;

II.3 - Considerando que a LGPD não distingue se o encarregado deve ser pessoa física ou jurídica, e se deve ser um funcionário da organização ou um agente externo;

Resolvem as Partes celebrar o presente Contrato de Prestação de Serviços de Encarregado, doravante denominado simplesmente "Contrato", que se regerá pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – OBJETO

1.1. Constitui objeto deste Contrato a formalização da nomeação do **ENCARREGADO** para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de

Proteção de Dados ("ANPD"), bem como por zelar pelo cumprimento das políticas de proteção dos dados pessoais atuais e que vierem a ser implementadas pelo **CONTROLADOR**.

1.2. Para a execução do Contrato, o **ENCARREGADO** deverá observar a legislação aplicável, sobretudo a Lei nº 13.709, de 14 de agosto de 2018, e demais Resoluções e Publicações da Agência Nacional de Proteção de Dados.

CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. Este Contrato entrará em vigor na data de sua assinatura pelas Partes, devendo vigorar até **xx/xx/xxxx**, podendo ser prorrogado mediante celebração de aditivo contratual.

CLÁUSULA TERCEIRA – OBRIGAÇÕES DO ENCARREGADO

3.1. O **ENCARREGADO** garante que tem conhecimento da Legislação aplicável e que cumprirá com as bases legais e princípios da LGPD relativas à proteção de dados pessoais.

3.2. O **ENCARREGADO** ficará responsável pela execução das atividades estabelecidas no art. 41, §2º, da LGPD, a saber:

*Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

*Receber comunicações da autoridade nacional e adotar providências;

*Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

*Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

3.3. O **ENCARREGADO** concorda e aceita em fornecer suas informações de contato e identidade de forma clara e objetiva no site eletrônico do **CONTROLADOR**, em cumprimento ao art. 41, §1º, da LGPD, pelo tempo da vigência deste Contrato.

3.4. O **ENCARREGADO** está ciente de que a ANPD poderá estabelecer normas complementares sobre definição e atribuições

do encarregado, conforme disposto no art. 41, §3º, da LGPD, hipótese na qual tais atribuições deverão ser automaticamente incorporadas ao presente Contrato. Caso o Encarregado não aceite assumir tais atribuições e, assim, se manifeste expressamente no prazo de 05 (cinco) dias contados da divulgação pela ANPD, o Contrato ficará automaticamente rescindido, sem ônus para qualquer das Partes.

3.5. A ANPD poderá determinar ao **CONTROLADOR** que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, observados os segredos comercial e industrial (art. 38, LGPD). Neste caso, o **ENCARREGADO** deverá auxiliar o **CONTROLADOR** na elaboração do referido Relatório.

3.6. O **ENCARREGADO** garante observar e cumprir fielmente todas as medidas de segurança, técnicas e administrativas adotadas pelos agentes de tratamento aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentes ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, na forma do art. 46 da LGPD.

3.7. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (art. 37, LGPD), assumindo o **ENCARREGADO** a responsabilidade por manter tais registros.

3.9. O **ENCARREGADO** deverá comunicar imediatamente ao **CONTROLADOR** a ocorrência de incidente de segurança que possa acarretar risco ou danos aos titulares dos dados pessoais. O **CONTROLADOR**, por sua vez, com a assessoria do **ENCARREGADO**, deverá comunicar à autoridade nacional e ao titular sobre a ocorrência (art. 48 da LGPD).

3.10. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo (art. 48, §1º, LGPD):

*A descrição da natureza dos dados pessoais afetados;

*As informações sobre os titulares envolvidos;

*A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

*Os riscos relacionados ao incidente;

*Os motivos da demora, no caso de a comunicação não ter sido imediata;

*As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

CLÁUSULA QUARTA – PENALIDADES

4.1. Preceitua o art. 42 da LGPD que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

4.2. Dispõe ainda o art. 43 da LGPD que os agentes de tratamento só não serão responsabilizados quando provarem:

*Que não realizaram o tratamento de dados pessoais que lhes é atribuído;

*Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

*Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

4.3. Caso o dano causado seja comprovadamente atribuído ao **ENCARREGADO**, este deverá ressarcir integralmente o **CONTROLADOR** e/ou operador pelo valor corrigido monetariamente, acrescido de multa de 10% (dez por cento), sem prejuízo da rescisão imediata deste Contrato.

CLÁUSULA QUINTA – RESCISÃO CONTRATUAL

5.1. O **CONTROLADOR** terá o direito de resolver total ou parcialmente o presente Contrato, mediante simples notificação, nos seguintes casos:

*Inadimplemento de qualquer das cláusulas do presente Contrato, não obstante a aplicação das penalidades previstas neste Instrumento;

*No caso de o **ENCARREGADO** deixar de prestar as informações solicitadas pelo Controlador ou dificulte a supervisão deste nos termos do Contrato.

5.2. Se o **CONTROLADOR** rescindir este Contrato em decorrência de inadimplemento do **ENCARREGADO**, este pagará àquele, além das demais multas e penalidades previstas neste Contrato, multa no montante de 10% (dez por cento) do valor do prejuízo causado, sem prejuízo de perdas e danos.

5.3. O **ENCARREGADO** terá o direito de rescindir o Contrato, mediante o envio de notificação, caso o **CONTROLADOR** deixar de efetuar qualquer pagamento não controverso, em seu vencimento, e não sane esse inadimplemento dentro de 30 (trinta) dias após o recebimento da notificação do **ENCARREGADO**.

5.4. As Partes também poderão rescindir o presente Contrato, sem qualquer ônus, mediante aviso por escrito com 30 (trinta) dias de antecedência.

CLÁUSULA SEXTA – CONFIDENCIALIDADE

6.1. O **ENCARREGADO** reconhece que, em razão da celebração e execução deste Contrato, poderá ter acesso a informações exclusivas ou confidenciais do **CONTROLADOR** ou de terceiros.

6.2. Por essa razão, o **ENCARREGADO** compromete-se a manter total sigilo e confidencialidade em relação a todos os termos e condições deste Contrato bem como em relação a todos os dados (incluindo, mas não se limitando aos pessoais) e informações, verbais ou escritas, relativos às operações e negócios do **CONTROLADOR**, incluindo, sem limitação, todos os segredos e/ou informações financeiras, operacionais, econômicas, técnicas e jurídicas, bem assim dos contratos, pareceres e outros documentos, cópias ou registros destes, contidos em qualquer meio eletrônico ou físico a que tiver acesso em virtude deste Contrato.

6.3. O descumprimento da obrigação de sigilo, atinente à revelação de informações e dados confidenciais ou facilitação de sua revelação, poderá acarretar:

*A rescisão contratual;

*Em qualquer hipótese, na responsabilidade por penalidades e perdas e danos;

*Adoção das medidas judiciais cabíveis por força da legislação aplicável.

6.4. A obrigação de sigilo prevista nesta cláusula continuará vigente pelo prazo de 5 (cinco) anos contados do término deste Contrato, independentemente de sua causa.

CLÁUSULA SÉTIMA – PREÇO E PAGAMENTO

7.1 O **CONTROLADOR** pagará ao **ENCARREGADO** pela plena execução do serviço na forma, prazo e qualidade estabelecidos o preço mensal fixo no montante total de R$ **[-]** (**[-]**) ("Preço").

7.2 Os pagamentos serão realizados por meio de depósito em conta-corrente do **ENCARREGADO**, conforme dados informados abaixo:

Banco, Agência, C/C, CPF/CNPJ

7.3 Em caso de atraso de qualquer das parcelas mensais de pagamento, pelo **CONTROLADOR**, o **ENCARREGADO** fará jus ao recebimento do valor em atraso corrigido pelo índice **[xxxx]** somado a juros moratórios de 1% (um por cento) ao mês *pro rata die* calculados desde a data do vencimento até a data do respectivo pagamento e multa penal compensatória de 0,5% (meio por cento), incidentes sobre o valor em atraso.

CLÁUSULA OITAVA – FORO

8.1. Todos os litígios decorrentes deste Contrato serão resolvidos no foro da comarca de **[xxxx]**, renunciando as Partes a qualquer outro, por mais privilegiado ou especial que seja.

E, por estarem as Partes justas e contratadas, firmam o presente Contrato, juntamente com as testemunhas que o também assinam.

Cidade e data.

Controlador:

Encarregado:

Testemunhas:

Texto elaborador por: Renato Almeida Viana

ANEXO G – Modelo de termo de consentimento

I - PARTES

[XXXX] [inserir aqui a qualificação completa do Escritório], neste ato representado pelo sócio administrador, doravante denominado **ESCRITÓRIO**.

[XXXX] [inserir aqui a qualificação completa do Titular], doravante denominado **TITULAR.**

II - CONSIDERANDOS

II.1 - Considerando que a Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), em seu artigo 5º, inciso XII, prevê o consentimento como uma das bases legais para o tratamento dos dados pessoais do seu titular;

II.2 - Considerando que o tratamento do dado pessoal é, nos termos do artigo 5º, inciso X, da LGPD, "a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração";

II.3 - Considerando que a LGPD exige que o consentimento decorra de "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada";

II.4 - Considerando que o **ESCRITÓRIO** zela pelo cumprimento da LGPD e para tanto solicita neste instrumento o consentimento do **TITULAR** para a finalidade descrita na Cláusula Primeira;

II.5 - Considerando que o **TITULAR**, por livre e espontânea vontade, deseja formalizar o seu consentimento, estando ciente de que a sua recusa ou mesmo revogação não poderá causar a ele qualquer sanção, prejuízo, etc.;

Resolvem as Partes firmar o presente Termo de Consentimento, que será regido pelas seguintes cláusulas e condições.

CLÁUSULA PRIMEIRA – FINALIDADE DO CONSENTIMENTO

O **ESCRITÓRIO** declara que a finalidade para a qual o consentimento do **TITULAR** está sendo obtido é [descrever aqui de maneira objetiva e clara a finalidade a que se destina o consentimento e se haverá necessidade de compartilhá-los com terceiros e em que condições haverá esse compartilhamento].

O **ESCRITÓRIO** compromete-se a tratar os dados pessoais do **TITULAR** apenas para a finalidade aqui definida e em estrita observância às permissões concedidas pelo **TITULAR**.

CLÁUSULA SEGUNDA – DADOS PESSOAIS QUE SERÃO TRATADOS

O **ESCRITÓRIO** declara que os seguintes dados pessoais do **TITULAR** serão tratados: [descrever aqui de maneira exaustiva os dados pessoais e de que forma eles serão tratados]

Os dados mencionados nesta cláusula serão armazenados [descrever aqui onde esses dados serão armazenados: servidor local, na nuvem...], pelo prazo de **xxxx** [dias/meses/anos].

CLÁUSULA TERCEIRA – CONSENTIMENTO DO TITULAR

Neste ato, o **TITULAR** dá o seu consentimento para que o **ESCRITÓRIO** trate os seus dados pessoais, conforme descrito na cláusula anterior, para a finalidade específica prevista na Cláusula Primeira. Fica permitido ao **ESCRITÓRIO** manter e utilizar os dados pessoais durante todo o período estabelecido neste Termo, salvo se houver outra base legal que permita a manutenção ou utilização dos dados pessoais para além do prazo.

§1º - Nos termos do § 5º, do art. 8º da LGPD, o **TITULAR** declara ter ciência que, a qualquer momento, o consentimento ora formalizado poderá ser revogado, bastando para tanto que o **TITULAR** encaminhe um e-mail nesse sentido para o seguinte endereço eletrônico: xxxxx@xxxxx.com.br, aos cuidados do Sr. **[xxxx],** que é o Encarregado designado pelo **ESCRITÓRIO**.

§2º - De igual forma, é direito do **TITULAR** solicitar, a qualquer momento, a correção, o descarte, o bloqueio ou a anonimização dos seus dados, hipóteses nas quais deverá adotar o mesmo procedimento previsto no parágrafo anterior.

CLÁUSULA QUARTA – PROTEÇÃO DOS DADOS PESSOAIS DO TITULAR

O **ESCRITÓRIO** informa ao **TITULAR** que adota várias medidas de proteção no tratamento dos dados pessoais, podendo destacar entre elas as seguintes: [descrever aqui de maneira resumida as medidas de segurança que são efetivamente adotadas pelo Escritório, por exemplo: antivírus, acesso limitado aos dados pessoais, identificação de acesso, vedação de compartilhamento de senhas, treinamento periódico do pessoal, *backup,* etc.]

CLÁUSULA QUINTA – FORO

As Partes elegem o foro da cidade de **[xxxx]**, para dirimir quaisquer dúvidas oriundas deste termo, renunciando as Partes a quaisquer outros que tenham ou venham a ter, por mais privilegiados que sejam.

Por estarem assim, justos e contratados, assinam o presente, na presença das testemunhas abaixo.

Local, data.

Titular:

Empresa:

Texto elaborador por: Renato Almeida Viana