UNIVERSIDADE DE BRASÍLIA (UNB)
FACULDADE DE CIÊNCIA DA INFORMAÇÃO (FCI)
CURSO DE GRADUAÇÃO EM BIBLIOTECONOMIA

ANA CAROLINA RAMALHO SAMPAIO

ESTRUTURAÇÃO DOS DADOS, INFORMAÇÕES E PROCESSOS EM CONFORMIDADE A LEI GERAL DE PROTEÇÃO DE DADOS: estudo de caso do GALT Vestibulares

Brasília
2023

ANA CAROLINA RAMALHO SAMPAIO

ESTRUTURAÇÃO DOS DADOS, INFORMAÇÕES E PROCESSOS EM CONFORMIDADE A LEI GERAL DE PROTEÇÃO DE DADOS: estudo de caso do GALT Vestibulares

Monografia apresentada à banca examinadora como requisito parcial para a obtenção do título de Bacharela em Biblioteconomia pela Faculdade de Ciência da Informação da Universidade de Brasília.

Orientador: Dr. Márcio de Carvalho Victorino

Brasília
2023

Universidade de Brasília

FOLHA DE APROVAÇÃO

Título: ESTRUTURAÇÃO DOS DADOS, INFORMAÇÕES E PROCESSOS EM CONFORMIDADE A LEI GERAL DE PROTEÇÃO DE DADOS: estudo de caso do GALT Vestibulares

Autor(a): Ana Carolina Ramalho Sampaio

Monografia apresentada de forma remota em **23 de Fevereiro de 2023** à Faculdade de Ciência da Informação da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Bacharel em Biblioteconomia.

Orientador(a) (FCI/UnB): Dr. Márcio de Carvalho Victorino
Membro Interno (FCI/UnB): Dra. Fernanda Farinelli
Membro Interno (STI/UnB): Me. Rodrigo da Fonseca Silveira

Em 20/10/2022.

Documento assinado eletronicamente por **Marcio de Carvalho Victorino**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 24/02/2023, às 15:15, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Fernanda Farinelli**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 24/02/2023, às 15:39, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Rodrigo da Fonseca Silveira**, **Analista de Tecnologia da Informação da Secretaria de Tecnologia da Informação**, em 25/02/2023, às 15:39, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **9379495** e o código CRC **CD70BF10**.

Dedico este trabalho a minha mãe, minhas avós e minhas titias, meus exemplos de vida e amor, por me mostrarem o caminho das pedras e me acompanharem a cada conquista e dificuldade.

AGRADECIMENTOS

Sou grata a minha mãe, Aline, por ser a minha base, meu maior exemplo de ser humano, por me apresentar com excelência a ciência da informação, e como é o trabalho impecável de uma gestora e líder.

Às minhas avós, Joalmina, Lourdes e Maria de Fátima, por serem meus exemplos de acolhimento, amor e força. Sei que me olham sempre de onde estejam e me dão forças para continuar.

Às minhas titias, por sempre me apoiarem em todos meus passos, por serem meus anjos da guarda e me proverem tantas oportunidades de vida e conhecimento.

Ao meu pai, Luiz, por ser um meu apoio racional e emocional em tantos momentos, por sempre me impulsionar a fazer meu melhor, ser autoconfiante e por me trazer a tecnologia da informação.

Aos meus irmãos Daniel, João Paulo, Davi, Lucas, Isabela, Anne, Enzo e Clarissa, por serem as pessoas que mais amo, por trazerem tanta alegria e conhecimento pra minha vida.

À minha esposa, Beatriz, pelo companheirismo, pela nossa mudança para o outro lado do oceano, por me incentivar a ir sempre além e por ser meu exemplo de pesquisadora científica.

Aos meus amigos, que facilitaram muito minha caminhada, pelas manhãs, tardes e noites na FCI e por sempre me lembrarem de como a vida é melhor na companhia de pessoas que brilham.

À Mariana Cavalcante, pela forte amizade que criamos, pela paciência de revisar o trabalho, me apoiar e por ter sido minha maior fonte de conhecimento sobre a LGPD.

Ao GALT Vestibulares, à Isabel Bispo e à equipe de Compliance e Proteção de Dados por me darem o prazer de descobrir a minha área de pesquisa e por uma experiência de crescimento singular.

Ao meu orientador, Prof. Dr. Márcio de Carvalho Victorino, por aceitar conduzir meu trabalho, pela paciência, incentivos e correções.

À Universidade de Brasília, à Faculdade de Ciência da Informação e ao corpo docente por me darem a oportunidade de aprender e gerar conhecimento científico.

“Entre a vida e a morte, há uma biblioteca. E, dentro dessa biblioteca, as prateleiras não tem fim. Cada livro oferece uma oportunidade de experimentar outra vida que você poderia ter vivido. De ver como as coisas seriam se tivesse feito outras escolhas.”

Matt Haig

RESUMO

A gestão de segurança da informação consiste em um processo administrativo com objetivo de gerenciar e assegurar a proteção dos dados e das informações. Uma das ferramentas utilizadas é a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, que tem como objetivo garantir a livre formação de personalidade de cada indivíduo, a segurança do dado pessoal, a liberdade e a privacidade. Como proposta, este trabalho visa, por meio de um estudo de caso, estruturar os dados institucionais e informações de alunas e alunos, de voluntárias e voluntários do cursinho preparatório GALT Vestibulares, de acordo com a Lei Geral de Proteção de Dados, com intuito de mitigar a ação da engenharia social. Nesse sentido, o trabalho tem como objetivos específicos: Explicar o plano de providências para implementação da lei no contexto do GALT Vestibulares; Apresentar as ações tomadas em relação a gestão da segurança da informação; Mensurar o efeito da implementação da Lei Geral de Proteção de Dados no cursinho; Verificar se o desenvolvimento organizacional relacionado a implementação foi correspondente ao plano de providências. A metodologia utilizada se caracteriza como uma pesquisa qualitativa e de natureza aplicada quanto à abordagem, e tem caráter explicativo. O ponto de vista que será apresentado é interno em relação à organização, com maior importância do contexto da pesquisa e quantidade de fonte de dados ampla. As informações apresentadas permitem compreender conceitos da Lei Geral de Proteção de Dados e como foi realizada a implementação da lei no contexto de um cursinho voluntário. Portanto, foi possível realizar a implementação e a estruturação dos dados, mitigando a ação da engenharia social e evitando o vazamento dos dados, mesmo com empecilhos devido à dificuldade em relação à resistência da cultura organizacional com enfoque na importância da segurança da informação para alcançar os objetivos do projeto.

Palavras-chave: Segurança da Informação. Lei Geral de Proteção de Dados. Gestão de Segurança da Informação. Engenharia Social. GALT Vestibulares.

ABSTRACT

Information security management is an administrative process with the purpose of managing and ensuring the protection of data and information. One of the tools used is the General Law on Data Protection, number 13709 of 14 August 2018, which aims to guarantee each individual's free personality formation, personal data security, freedom and privacy. As a proposal, this work aims, through a case study, to structure the institutional data and information of students and volunteers of the voluntary preparatory school GALT Vestibulares, according to the General Law of Data Protection, in order to avoid the action of social engineering. In this sense, the work has as specific objectives: To explain the plan of action for the implementation of the law in the context of GALT Vestibulares; To present the actions taken in relation to information security management; To measure the effect of the implementation of the General Law of Data Protection in the preparatory school; To verify if the organizational development related to the implementation was corresponding to the plan of action. The methodology adopted, as to the approach, is characterized as a qualitative research of an applied nature, with an explanatory character. The point of view that will be presented is internal in relation to the organization, with greater importance of the research context and ample amount of data source. The information presented allows understanding concepts of the General Law on Data Protection and how the implementation of the law was carried out in the context of a voluntary course. Therefore, it was possible to carry out the implementation and structuring of the data, mitigating the action of social engineering and avoiding the loss of data, even with difficulties due to the resistance of the organizational culture focusing on the importance of information security to achieve the project objectives.

Keywords: Information Security. General Law of Data Protection. Information Security Management. Social Engineering. GALT Vestibulares.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD - Associação Nacional de Proteção de Dados

BR - Brasil

CF - Constituição Federal

CCPA - *California Consumer Privacy Act*

FBI - *Federal Bureau Investigation*

GDPR - *General Data Protection Regulation*

GI - Gestão da Informação

LAI - Lei de Acesso à Informação

LGPD - Lei Geral de Proteção de Dados

PSI - Políticas de Segurança da Informação

SIG - Sistemas de Informações Gerenciais

SI - Sistemas de Informação

TI - Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

Com o fim da segunda guerra e o início da guerra fria, o desenvolvimento da tecnologia se tornou primordial para os países envolvidos na guerra. Devido ao crescimento exponencial e estratégico da tecnologia, houve uma intensa busca pela informação e assim se deu também uma maior importância para quem a detinha. (HAHN; BUCKLAND, 1998; PINHEIRO, 2005; FREIRE; FREIRE, 2009; BAWDEN; ROBINSON, 2012 apud ARAÚJO, 2018). A sequência desses acontecimentos revelou uma necessidade latente de profissionais capazes de recuperar a informação com mais rapidez e assertividade.

Toda essa mudança no cenário do uso da informação e na sua crescente permanente, demanda mais dos profissionais, que hoje em dia ganharam mais um papel no campo da ciência da informação, devido à falta de segurança dos dados pessoais, dados de pequenas e grandes empresas, governos e instituições de todo o mundo. Este papel se configura para um profissional da informação capaz de utilizar seus conhecimentos com objetivo de assegurar a segurança dos dados, através de leis, sistemas e gestão da segurança de dados e informação.

A Lei Geral de Proteção de Dados (LGPD), promulgada no Brasil oficialmente em 14 de agosto de 2018, como um complemento ao Marco Civil da Internet, tem por objetivo regulamentar a coleta, classificação, reprodução, transmissão, compartilhamento, arquivamento, modificação, avaliação ou exclusão dos dados pessoais dos cidadãos feitos por instituições e empresas. Essa lei tornou-se uma realidade com multa aplicável a partir de agosto de 2021.

A LGPD foi criada, usando o modelo da GDPR (*General Data Protection Regulation*) pensando em proteger os usuários que têm seus dados utilizados por empresas, como o Facebook, hoje em dia Meta, que se envolveu em um escândalo de uso de dados pessoais de seus usuários no processo eleitoral dos Estados Unidos em parceria com a Cambridge Analytica no uso de plataformas digitais.

Porém essa lei não afeta apenas grandes empresas, como também pequenas instituições pelo Brasil. Com tais mudanças no cenário legal, a mudança também foi necessária para o cursinho voluntário GALT Vestibulares, que é objeto de estudo deste trabalho, se viu à frente de um verdadeiro desafio de adequação rápida à LGPD, para melhor tratar os dados do seu público alvo, as voluntárias e voluntários e a instituição. Para tal ação, foi feito um processo seletivo para a montagem de uma equipe capaz de realizar a tarefa de

acordo com as exigências que a lei trouxe, dentro da legalidade e com a organização necessária para manter e melhorar o bom funcionamento do cursinho.

2. PROBLEMA DE PESQUISA

Desta forma, o problema de pesquisa que orienta este trabalho é como estruturar os dados institucionais, os processos e informações de alunas e alunos, de voluntárias e voluntários do cursinho preparatório GALT Vestibulares, de acordo com a Lei Geral de Proteção de Dados, a fim evitar a ação da engenharia social?

2.1. Justificativa

Pelo porte do cursinho e pelo status de ser um OSCIP, também tinham obrigatoriedade de aplicar a Lei Geral de Proteção de Dados na organização, a fim de garantir a segurança dos dados das alunas e alunos, das voluntárias e voluntários e do próprio cursinho. Além da implementação da LGPD, também precisavam estruturar os dados já existentes, a fim da informação ter uma recuperação facilitada.

Este trabalho visa apresentar como os dados, as informações e processos das alunas e alunos, das voluntárias e voluntários e os dados institucionais foram estruturados e tratados, a fim de adequar o cursinho GALT Vestibulares a nova lei, utilizando um plano de providências para implementação da lei prevista, com apoio de profissionais da área do direito. Além de recursos teóricos e práticos da biblioteconomia, como classificação e catalogação, e processos de segurança da informação, feitos com apoio de estudantes da biblioteconomia, para o melhor desenvolvimento organizacional no processo de adequação.

Logo, este trabalho traz uma outra perspectiva da biblioteconomia, para alcançar mais espaços e maior interdisciplinaridade, no caso com a área do direito, aplicada na área de gestão da segurança de dados e informações, principalmente no ambiente cibernético, a fim de evitar a ação da engenharia social e suas consequências.

3. OBJETIVOS

3.1. Objetivo geral

Estruturar os dados, informações e processos dos alunos, voluntários e os dados institucionais, conforme a Lei Geral de Proteção de Dados, no cursinho voluntário GALT Vestibulares.

3.2. Objetivos específicos

a) Identificar as diretrizes da Lei Geral de Proteção de Dados para implementação no GALT Vestibulares;
b) Explicar o plano de providências para implementação da LGPD no contexto do GALT Vestibulares;
c) Apresentar as ações tomadas em relação a gestão da segurança da informação;
d) Mensurar o efeito da implementação da LGPD no cursinho;
e) Verificar se o desenvolvimento organizacional relacionado a implementação foi correspondente ao plano de providências.

Este trabalho seguirá uma estrutura que tem início pela revisão de literatura, onde se apresenta os principais conceitos para o desenvolvimento e compreensão da pesquisa, seguido da metodologia utilizada para a execução. Posteriormente será apresentado o estudo de caso propriamente dito, organizado pela apresentação do objeto de estudo e o processo da implementação da LGPD e da estruturação dos dados, informações e processos do cursinho. Processo este feito com base no diagnóstico da situação inicial e as ações tomadas com base no plano de providências. Ainda no estudo de caso, serão apresentados os resultados obtidos a partir da execução do plano de providências para implementação da LGPD e estruturação dos dados, informações e processos. Por fim, o trabalho conta com as considerações finais em relação ao trabalho desenvolvido no cursinho e as percepções em relação ao comportamento do usuário.

4. REVISÃO DE LITERATURA

4.1. Organização da Informação

Segundo Serra (2007) a informação pode ser entendida como o resultado de um processamento, manipulação e organização de dados, ou seja, o tratamento de dados, de maneira que apresente um efeito quantitativo ou qualitativo no conhecimento humano, animal ou em sistemas que o recebe. Taylor (1999) questiona se é a organização é de fato uma necessidade humana primitiva, se os seres humanos necessitam previamente de organizar as informações que são gravadas em suas mentes. Desde muito novos, os seres humanos aprendem a organizar as imagens que o cérebro recebe em algumas categorias, como comidas, pessoas e animais.

Essa atividade de classificação em grupos facilita com que a identificação e a recuperação do significante em conjunto com seu significado, ou seja, seu signo, seja muito mais facilitada. A informação pode ser organizada por setores, classes, em diferentes campos do conhecimento a fim de analisar estruturas e processos, pessoas e lugares, por exemplo. Logo, a junção desses dados, descritos em formato lógico, ordenado e prático, caracteriza ciências que estudam aquilo que já é existente ou que está no campo das ideias. Para este trabalho, considera-se informação a definição dada por McGee e Prusak (1994, p. 25):

> a informação não se limita a dados coletados; na verdade informação são dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto, ou seja, para que os dados se tornem úteis como informação a uma pessoa encarregada do processo decisório é preciso que sejam apresentados de tal forma que essa pessoa possa relacioná-los e atuar sobre eles.

As bibliotecas são consideradas as primeiras instituições da sociedade a realizar a organização da informação de forma ordenada. Segundo Martins (2002), essas primeiras bibliotecas, as Bibliotecas da Antiguidade, tinham como intuito apenas o armazenamento dos milhares de materiais feitos pelo ser humano. Materiais que tinham como objetivo registrar todo o conhecimento que por ele era obtido, mas não com intenção de ser compartilhado com a população da época, a partir de IX a.C., na biblioteca de Nínive. Ela foi considerada a primeira a ter coleção catalogada e indexada na história das bibliotecas (SOUZA, 2005).

Outro modelo de organização amplamente utilizado na ciência da informação é a classificação bibliográfica, a qual tem evidências da sua existência mesmo antes da era cristã.

Logo na década de 1930 nasceu a Teoria da Classificação Facetada, que foi pensada e desenvolvida por Ranganathan (1892-1972), com o objetivo de organizar a Biblioteca da Universidade de Madras, na Índia.

Os pilares teóricos do sistema de classificação facetada feitos por Ranganathan, é utilizado desde então como um modelo para a construção de sistemas de classificação bibliográficos, como uma representação da realidade (GOMES; MOTTA; CAMPOS, 2006). Os sistemas de classificação analítico-sintéticas tem sua proposta de cinco Categorias Fundamentais: Tempo, Espaço, Energia, Matéria (Material e Propriedade) e Personalidade. Essas categorias fundamentais não teriam previamente um conceito, mas o que melhor compreende o que elas seriam é dito na revisão sobre Ranganathan:

> [...] categorias as mais genéricas possíveis e passíveis de se manifestar de diversas formas, capazes de hospedar todos os objetos da natureza até então conhecidos pelo Homem, e de classificá-los de acordo com sua natureza conceitual, cada um numa e somente numa categoria. (GOMES; MOTTA; CAMPOS, 2006)

Essas categorias têm conceitos que são organizados mais uma vez em classes. As classes dos termos ou conceitos podem ser formadas em cadeias ou renques. As cadeias são postas em séries verticais, sendo estas genéricas ou partitivas. Já as classes em renques são organizados em séries horizontais e que da mesma forma que as cadeias verticais, podem ser genéricos ou partitivos. As facetas são manifestações dentro das categorias fundamentais, como termos genéricos usados para determinar um elemento de um assunto composto por vários conceitos ou uma ideia solta.

4.2. Gestão da Segurança da Informação

A informação pode ser vista como algo muito simples quando se pensa apenas em algum conjunto de dados cruzados em que seu resultado pode definir uma pessoa, por exemplo. Porém, o uso da informação para decisões importantes é base para o ser humano desde sua perspectiva individual em situações diárias, até questões relacionadas a grandes empresas e instituições governamentais. O uso e a criação de novas informações no século XX e início do século XXI foram revolucionários pela expansão em larga escala de computadores pessoais, smartphones e a própria internet. As antigas unidades de medida de

informação cresceram em tamanho para *terabytes, petabytes, exabytes* e outras nomenclaturas que expressam o excepcional crescimento do volume de dados, conhecido mundialmente como a era do *big data*. (ARAÚJO, 2018).

Hoje em dia encontra-se uma sociedade na qual a informação deixou de ser apenas pares de dados cruzados, tornou-se ativo com potencial grande de valor, inclusive monetário. Toda essa importância deu à informação um poder, cabendo-lhe assim a necessidade de tratamento e gestão para a segurança da informação em questão, ainda mais com toda essa informação sendo tratada em sistemas. Segundo Robredo (2003), um sistema de informação consiste numa entidade complexa e organizada, onde se capta, armazena, processa, fornece, usa e distribui a informação. Nestes sistemas são incluídos recursos organizacionais e recursos tecnológicos, com objetivo de automatizar pelo menos alguns elementos do sistema. Cabe aqui salientar que nem toda informação, como livros em uma biblioteca pública, exigem um nível de segurança apurado, uma vez que assumem esse caráter público.

Devido a essa preocupação, nasce a Segurança da Informação (SI) com o objetivo de orientar e executar um melhor tratamento da informação enquanto um importante ativo na sociedade. Tornou-se necessário então gerir todos esses dados da maneira mais eficaz possível. Em consequência dessa urgência, surgiram métodos de gestão da segurança da informação para a proteção destes novos ativos de valor, diretamente associados à informação contida nos dados, que consiste em um processo administrativo com objetivo de gerenciar a segurança da informação. A gestão conta com um conjunto de procedimentos, políticas e metodologias para gerir sistematicamente os dados e informações sensíveis de uma organização, visando a proteção dos dados. (BRASIL, 2020).

Alguns objetivos da gestão de segurança da informação são: Planejar e implementar medidas de mitigação e controle dos riscos avaliados; Identificar, analisar e avaliar os riscos relacionados à informação; Divulgar, conscientizar e motivar as boas práticas de segurança; Monitorar e avaliar as medidas de segurança implementadas; Estabelecer e divulgar a Política e Procedimentos de Segurança; Propor medidas preventivas; Gerar condições adequadas para existência da confidencialidade, integridade e disponibilidade da informação. (GOUVEIA, 2016). Para a constituição de uma nova área de pesquisa foram compostos alguns princípios dos quais a SI segue, como o uso de um conjunto de boas práticas na gestão da informação, que tem como base medidas de segurança, prescrita em normas técnicas internacionais, feitas por organizações como a *International Organization for Standardization* e a *International*

Electrotechnical Commission. Uma de suas normas técnicas é um padrão para Sistemas de Gestão de Segurança da Informação, ISO/IEC 27001.

A Segurança da Informação fixada como "[...] ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (BRASIL, Portaria nº 10, 2012) segue as diretrizes, utilizadas como pilares, que tem como premissa a seguridade, sendo esses pilares: a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade, que são comumente representadas pela sigla DICA.

4.2.1. Disponibilidade

Conforme a norma 10/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSI/GSIPR) (2012), a Disponibilidade, referente a Segurança da Informação, é a "propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade". Isso quer dizer que sempre que o titular do dado solicitar acesso a ele ou casos diversos onde a informação for solicitada pelo poder do Estado, deve estar disponibilizada.

4.2.2. Integridade

Ainda dentro da norma 10/IN01/DSIC/GSIPR (2012), a Integridade está descrita como "propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental", ou seja, a entidade responsável por tratar os dados deve assegurar que a informação esteja sempre em sua totalidade, mantendo sua fidedignidade, da forma a qual foi concedida. Isso inclui o encargo de garantir que em caso de acidentes, como uma falha no sistema utilizado, a informação não seja corrompida e/ou perdida, uma vez que a entidade responsável pode agir previamente realizando um *backup* dos dados.

4.2.3. Confidencialidade

A confidencialidade é a "propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado" (BRASIL, Portaria nº 10, 2012). Esse pilar da SI significa que a informação disponibilizada a uma

entidade que tem como objetivo o tratamento do dado, com finalidade previamente informada, deve mantê-la devidamente privada, a fim de evitar o vazamento dessa informação. Ela só deve ser disponibilizada, conforme o primeiro dos pilares da SI, em caso de solicitação da pessoa autorizada a acessá-la, sendo assim o titular de dados, aqueles que o titular deu consentimento ou em caso do uso do poder do Estado.

Um exemplo da importância desse princípio da SI é no mundo empresarial, onde conseguir informações internas de companhias concorrentes pode afetar diretamente no desempenho comercial da empresa que tem os seus dados violados, assim como para a empresa que toma conhecimento dessa informação.

4.2.4. Autenticidade

Autenticidade está relacionada à "propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade"(BRASIL, Portaria nº 10, 2012). Esse princípio da Segurança da Informação existe a fim de garantir que o dado é realmente o que alega ser, ou seja, ele atesta a identidade da informação.

Hoje em dia usa-se muito a biometria como forma de acesso a alguma informação, pois essa medida é teoricamente uma forma irrefutável de confirmar a identidade de quem está a acessar. Outra forma é o certificado digital, que consiste em um documento eletrônico que contém os dados do titular, que é amplamente utilizado na internet para confirmar que a pessoa por trás da ação é realmente quem diz ser.

4.2.5. ISO/IEC 27001

A *International Organization for Standardization* e a *International Electrotechnical Commission* são organizações responsáveis pela criação de normas técnicas em âmbito internacional. Uma de suas normas técnicas é um padrão para Sistemas de Gestão de Segurança da Informação, ISO/IEC 27001 Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação - requisitos, mais conhecido como ISO 27001.

A ISO/IEC 27001 foi publicada em 2005, com objetivo de designar um arquétipo para planejar, implementar, operar, monitorar, avaliar e melhorar um Sistema de Gestão de Segurança da Informação. Ela é a única norma da série 27000 com requisitos de certificação e

com possibilidade de certificação acreditada. A norma é composta por duas partes relativamente diferentes, a primeira delas descreve as regras e requisitos para cumprir a norma dentro de uma organização, como mostra do diagrama a seguir na Figura 1:

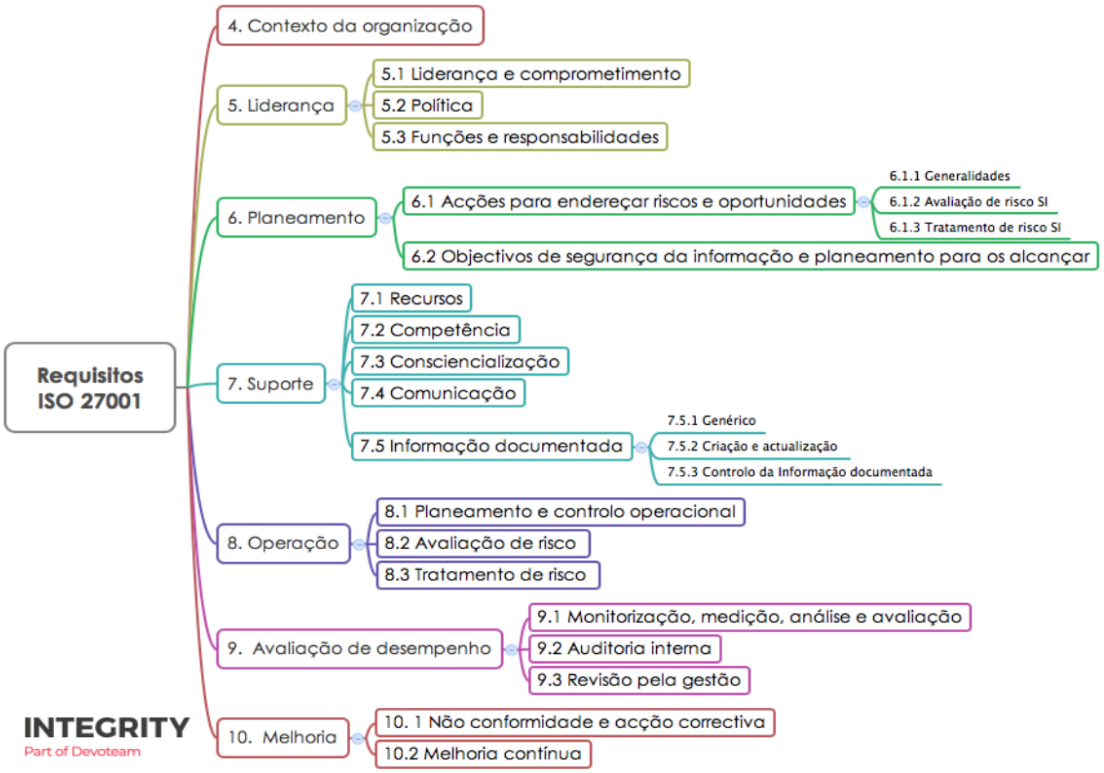

Figura 1: Diagrama de Requisitos da ISO 27001
Fonte: Integrity (2022)

A segunda componente, demonstrada na Figura 2, é um conjunto de controlos da ISO 27001 que a corporação deve adotar para o correto funcionamento da norma. A seguir pode-se analisar os tópicos necessários expostos pela empresa Integrity, especialista em cibersegurança e consultoria em Tecnologia da Informação (2022):

Figura 2: Diagrama de Controlos da ISO 27001
Fonte: Integrity (2022)

A norma ISO/IEC 27001 conta ainda com um esquema de 4 passos chamado ciclo PDCA, que pode ser visualizado na Figura 3, que é uma sigla para *Plan, Do, Check* e *Act.* Ou seja, a primeira parte da sigla significa Planejar, a parte onde se faz o levantamento e análise de problemas, a fim de definir objetivos a serem atingidos, conforme os valores da empresa. Após o processo de observação do problema é escolhido um plano de ação pelo qual a equipe e a empresa irão percorrer para atingir o objetivo estabelecido e por fim, é montada uma equipe para realizar o projeto. A segunda parte da sigla está relacionada a Ação, executar o plano de ação definido e evidenciar tudo o que se obtém êxito e as partes onde houve maior dificuldade ou falha na execução.

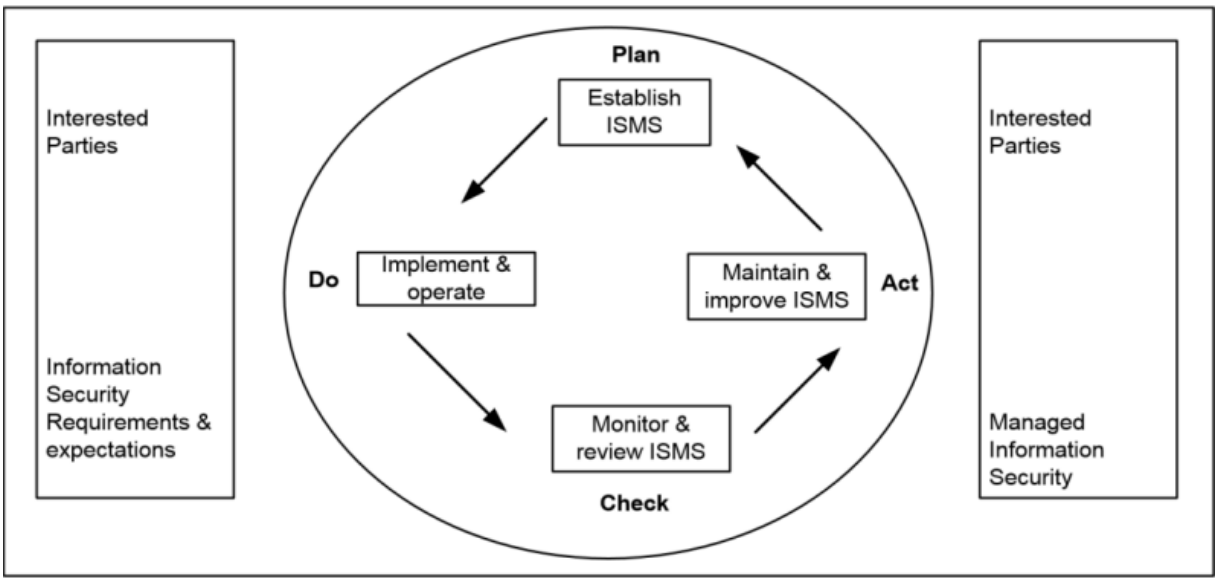

Figura 3: Ciclo PDCA
Fonte: Gouveia (2022)

Na terceira etapa do ciclo PDCA, tem-se o *Check,* onde é o momento de verificar os resultados obtidos com o plano de ação após a execução inicial. Essa fase consiste em comparar aquilo que se pretendia alcançar da proposta inicial com o que realmente foi obtido. Essa parte do ciclo pode ser feita tanto ao fim do planejamento como ser feita ao longo da implementação. Por fim, é a fase da Ação, onde tudo o que teve êxito pode ser padronizado, realizando assim um mapeamento de processo e divulgado como resultado de melhoria da organização. Essa fase também conta com uma gestão do conhecimento da organização, pois gera memória para a empresa, contribuindo desta forma com o compartilhamento de conhecimento adquirido com o processo. Para as partes do processo que não obtiveram êxito, deve-se voltar ao ciclo e recomeçá-lo a partir do planejamento novamente.

A estrutura global da norma ISO/IEC 27001, figura 4, conta com os requisitos apresentados previamente na figura 1, além de conter o Anexo A, representado anteriormente pela figura 2 e vê-se melhor como o ciclo PDCA é utilizado no seu processo de implementação, representado pelas cláusulas 6, 8, 9 e 10 ao centro da figura 4 abaixo:

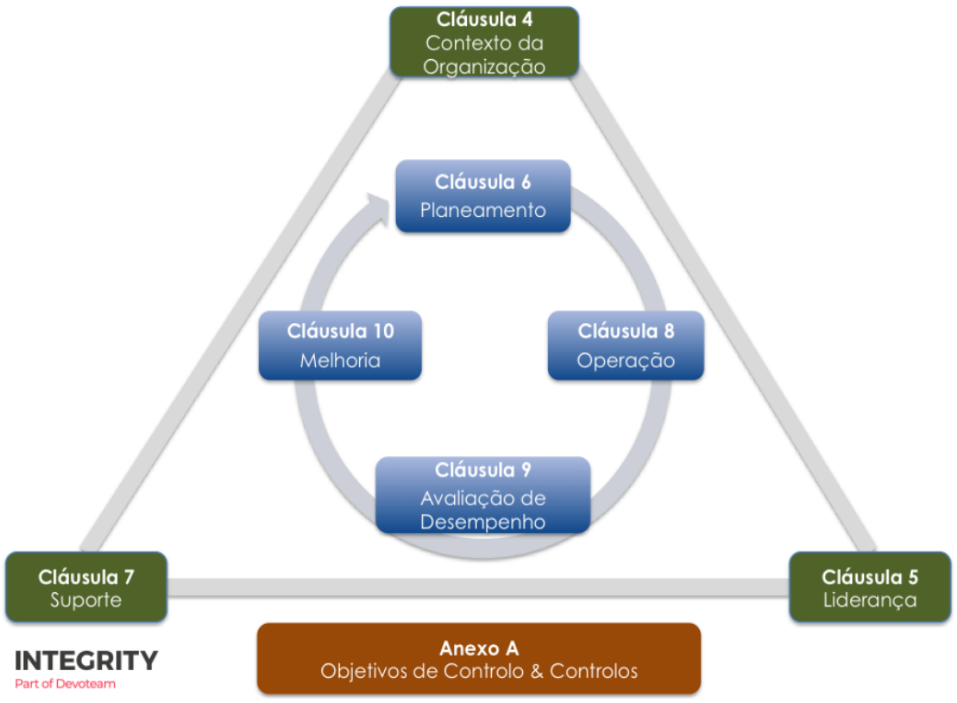

Figura 4: Estrutura Global ISO/IEC 27001
Fonte: Siteware (2022)

4.3. Marcos legais

A) Lei 12.965/2014 - Marco Civil da Internet:

No dia 23 de abril de 2014, o Brasil ganhou uma nova lei que estabelece princípios, garantias, direitos e deveres, para o uso da internet em toda a extensão do país. Essa lei, de número 12.965, foi chamada de Marco Civil da Internet, sancionada pela então presidenta Dilma Rousseff. No artigo 3º da lei 12.965 de 2014, são descritos oito princípios para o uso da internet no Brasil:

> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (BRASIL, 2014).

Esse meio tem como objetivo então mediar as formas como se dão as relações que podem acontecer por meio da rede, e também seu acesso, para manter a organização do espaço, assim alcançando o controle sobre as ações, como os fluxos de navegação.

Assim como muitas leis que são tratadas no âmbito deste trabalho, essa também prevê alguns pilares que compõem a sua base, sendo 3 estes pilares. Nos termos da Constituição Federal, de 1988, o primeiro deles fala sobre a neutralidade da rede, o que gerou muita dificuldade no diálogo para a criação da lei do marco civil da internet. Barreto e César (2007), discorrem na Revista Eletrônica do curso de Direito da UFSM que

> "A paternidade do conceito da Neutralidade da Rede é devida ao professor Tim Wu, da Universidade de Columbia e teve o Chile como primeiro país a trazer para o seu ordenamento jurídico pátrio tal preocupação com a Neutralidade da Rede no ano de 2010. Em 2012 a Holanda foi o segundo país a inserir em seu ordenamento jurídico,

> trazendo que os prestadores e provedores estão proibidos de bloquear ou reduzir a velocidade de serviços ou aplicações na Internet, sendo permitidas práticas que minimizem os efeitos de congestionamento de tráfego, preserve a integridade e segurança da rede, restrinjam envio de spam e deem cumprimento a alguma determinação legal" (BARRETO; CÉSAR, 2007)

A neutralidade da rede está ligada a um princípio da arquitetura de redes, onde os provedores do acesso à internet devem tratar os dados de forma que não haja discrminação no tráfego, em relação ao seu conteúdo ou origem. No artigo 9º, da Lei 12.965, "O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".

Dessa maneira, as empresas de telecomunicações, por exemplo, não podem definir e cobrar valores diferenciados de acordo com o uso da rede. Ou seja, os provedores apenas podem cobrar pela velocidade da conexão e não pelo conteúdo que trafega nos cabos, sua origem ou seu destinatário.

No segundo pilar está a liberdade de expressão, que está previsto no artigo 5º, inciso IV da Constituição Federal do Brasil de 1988, onde é descrito que é livre a manifestação de pensamento, sendo vedado o anonimato. O artigo 8º do Marco Civil da Internet, Lei 12.965, determina que o direito à liberdade de expressão nas redes de comunicação está condicionado ao pleno exercício do direito de acesso à internet.

Isso quer dizer que um eventual excesso no exercício da liberdade de expressão, como em casos de discursos racistas e difamatórios, não isenta o responsável de uma sanção judicial, uma vez que a livre expressão não corresponde à impossibilidade de reprovação. A partir desse pilar, só os conteúdos que poderão ser retirados pelos provedores de internet, são aqueles que sejam ofensivos e criminosos, a partir de uma comprovação feita por uma avaliação imparcial do Judiciário pelo processo legal.

O terceiro, e último, pilar é o da privacidade, que é um direito fundamental previsto no artigo 5º, inciso X, da Constituição Federal do Brasil de 1988, assim como o da liberdade de expressão. A privacidade está descrita como princípio que garante "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2014). Assim

como o sigilo de correspondência e das comunicações por redes, de dados e das comunicações telefônicas, salvo por ordem judicial nos casos estabelecidos em lei.

A Lei nº 12.965/2014, do Marco Civil da Internet, assegura aos usuários da rede o consentimento expresso e informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, servindo as possibilidades em que os dados poderão ter uso e serem utilizados.

B) Lei 12.737/2012 – "Carolina Dieckmann":

Em maio de 2012, houve um episódio sofrido pela atriz global Carolina Dieckmann, onde teve seu computador pessoal invadido por *crackers,* pessoas que burlam os sistemas a fim de obter vantagens ou causar danos, e suas fotos e conversas íntimas foram divulgadas sem a sua autorização. Devido a esse acontecimento repulsivo, foi sancionada a Lei 12.737/12 que ficou conhecida como "Lei Carolina Dieckmann", pela então presidenta Dilma Rousseff, que concerne a alteração no Código Penal Brasileiro, para tipificação de delitos informáticos.

Essa lei foi de suma importância, perante a grande crescente de acontecimentos envolvendo exposição íntima a partir da invasão de *crackers*, que até então não possuíam jurisprudência e meios legais efetivos para seu julgamento. A alteração reforça a necessidade de segurança no meio cibernético, principalmente em relação à privacidade online, que retoma um dos princípios da Lei nº 12.965/2014, do Marco Civil da Internet. Os artigos da Lei 12.737/12, Lei "Carolina Dieckmann", descrevem como devem ser tratados os crimes de invasão digital ou em dispositivos digitais, o impedimento ou dificultar o acesso dos serviços públicos de informação e proibição em casos de cópias não autorizadas ou falsificação de cartões de crédito, débito ou documentos pessoas.

C) Lei 12.527/2011 – Acesso à Informação (LAI):

A Lei nº12.527/11, que entrou em vigor dia 16 de maio de 2012, chamada de Lei de Acesso à Informação (LAI), tem como objetivo principal garantir o direito fundamental do livre acesso à informação. Segundo o do artigo 5º, das disposições gerais, "É dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão." (BRASIL, 2011). Ou seja, o cidadão tem como direito receber as informações de interesse

individual ou coletivo, pelos órgãos públicos, sendo uma exceção aquelas protegidas por sigilo ou preponderantes à segurança do Estado ou da população.

Decorrente da criação dessa lei, foi necessário desenvolver um projeto para facilitar o acesso a essas informações, assim se deu início a cultura da transparência, pelo portal da transparência do governo federal e suas esferas. Inaugurado pela Controladoria-Geral da União (CGU), no ano de 2004, o Portal da Transparência do Governo Federal é um sítio de acesso livre, onde o cidadão tem acesso à informação de como o dinheiro público é utilizado, além de se informar sobre assuntos relacionados à gestão pública do Brasil. (BRASIL, 2022).

Para a melhoria constante e melhor atendimento para a população, o site do portal da transparência foi reestruturado em 2018, pelo governo federal, com novas ferramentas, como mecanismo de busca integrado e intuitivo, mais recursos gráficos, maior e melhor oferta de dados abertos e melhor adequação para utilização nas plataformas móveis.

O portal tem fontes de informações variadas, sendo algumas delas grandes sistemas do Governo Federal, como o Sistema Integrado de Administração de Recursos Humanos (SIAPE), as faturas de Cartão de Pagamentos do Governo Federal e as bases de imóveis funcionais, além de muitas outras. Os órgãos que são responsáveis por prover essas informações encaminham os dados para a CGU, onde são tratados e disponibilizados como ferramentas para a população. Os dados são enviados periodicamente para atualização do portal, sendo cada órgão com a sua periodização definida. Os dados e informações são disponibilizados em diversos formatos, como gráficos, dados abertos ou consultas detalhadas, a fim de apoiar o usuário da melhor forma. Para utilização do portal não é exigido nenhum tipo de senha, cadastro ou identificação, para que o acesso seja o mais democrático e livre possível. (BRASIL, 2022).

4.4. Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados foi promulgada no Brasil como Lei nº 13.709, no dia 14 de agosto de 2018, a fim de garantir a livre formação de personalidade de cada indivíduo, a segurança pessoal, liberdade e privacidade, segundo o artigo 1º:

> Esta Lei 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. (BRASIL, 2018)

A LGPD fala sobre como deve ser realizado o tratamento dos dados pessoais, por meios físicos ou digitais, por pessoa física ou jurídica, do meio público ou privado. Segundo o artigo 5º, inciso X, da lei nº 13.709:

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018)

No âmbito da lei, o tratamento de dados deverá ser realizado pelo Operador e pelo Controlador de Dados, que serão os "Agentes de Tratamento". Segundo o artigo 5º, inciso VII, da lei nº 13.709, compete ao operador de dados o tratamento dos dados em nome do controlador. Já o controlador tem o dever de decidir os meios de tratamento da informação, a finalidade, ou seja, como deverá ser aplicada a lei de acordo com os dados em questão. Existe ainda mais um elemento, responsável por atuar como uma ponte, realizando a comunicação entre o controlador, os titulares dos dados, o operador e a Autoridade Nacional de Proteção de Dados (ANPD), chamado encarregado de dados ou DPO (*Data Protection Officer*).

Os dados que são tratados pelos agentes de tratamento pertencem a uma pessoa ou entidade, chamada de titular de dados, segundo o artigo 5º, inciso V. O artigo 17 da Lei Geral de Proteção de Dados afirma que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (BRASIL, 2018).

Um ponto pertinente a ser apresentado sobre a LGPD, o qual foi necessário de compreender para realização do seguinte estudo de caso, são os tipos de dados que são abordados pela lei, uma vez que não é qualquer tipo de dado que deva ser incluído nas cláusulas da lei. São 4 os tipos de dados: *Dados Pessoais, Dados Sensíveis, Dados Públicos e Dados Anonimizados*. O primeiro tipo é aquele que permite a identificação, direta ou indireta, da pessoa natural, como o nome e sobrenome, Registro Geral (RG), Cadastro de Pessoa Física (CPF), fotografias, endereço de IP (*Internet Protocol Address)* e Testemunhos de conexão (*cookies*).

Já os *Dados Sensíveis* são aqueles, dentre os Dados Pessoais, que caracterizam "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida

sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018).

Em caso do dado estar vinculado a um menor de idade, é necessário um consentimento específico destacado dado por pelo menos um dos responsáveis legais do menor, e neste caso, impossibilitado de dar conhecimento desse dado a terceiros. Ainda sobre os dados sensíveis, é de extrema importância que o tratamento seja consentido de forma explícita pelo titular dos dados e com uma finalidade específica. Sem este consentimento, o uso desse tipo de dado só pode acontecer em casos de uma obrigação legal.

Para abordar os termos que definem os dados públicos é importante salientar que a LGPD tem relação direta com a Lei nº12.527/11, que entrou em vigor dia 16 de maio de 2012, chamada de Lei de Acesso à Informação (LAI), que será tratado no tópico 4.3.1, item C, deste trabalho.

Os *Dados Públicos* serão tratados de forma que a finalidade sempre esteja descrita, considerando ainda a boa-fé e o interesse público ao disponibilizar esses dados. A LGPD determina que as organizações que necessitem tratar de dados tornados públicos, não precisam de consentimento para tal, mas em caso de compartilhamento dos dados coletados publicamente, devem pedir um consentimento com essa finalidade necessariamente.

Por fim, os *Dados Anonimizados*, são tratados a partir de uma técnica de anonimização, onde se remove ou modifica informações com objetivo de desassociar dados que possam identificar o titular. Nesse contexto, a LGPD não poderá ser aplicada, uma vez que não existe o risco de exposição do titular. Porém, um dado só é considerado anonimizado se não for possível de forma alguma a reconstrução de meios que identifiquem o titular. Caso essa identificação suceda, e assim caberá a aplicação da Lei Geral de Proteção de Dados, o dado então será pseudonimizado, que segundo o artigo 13, parágrafo 4 da lei 13.709, é definido como:

> a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. (BRASIL, 2018)

As atividades relacionadas ao tratamento dos dados deverão observar a boa-fé e 10 princípios estabelecidos pela LGPD no artigo 6º.

O primeiro diz sobre a finalidade, ou seja, a informação deve ser utilizada com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento subsequente contrário com as finalidades propostas inicialmente.

O segundo princípio é o da adequação, onde o tratamento deve seguir a finalidade(s) descritas.

O terceiro é referente a necessidade, isto é, o tratamento deve se limitar aquilo que é preciso para realizar as finalidades descritas, sem exceder o que é pertinente para a execução do especificado.

O quarto pilar é sobre o livre acesso, que garante ao titular de dados a consulta livre, facilitada e gratuita dos dados concedidos, enquanto durar o tratamento. Neste quesito, o titular também deve ter seus dados mantidos em sua integralidade, comprometendo o controlador e o operador a manter o dado em seu inteiro teor, da forma que foi concedido, uma vez que a informação coletada pode ser tratada em banco de dados, um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (BRASIL, 2018) e isto implica em vários riscos de ataques cibernéticos ou falhas de Sistemas de Informação.

O quinto princípio fala da qualidade dos dados do titular, que é dar a garantia da exatidão, clareza, relevância e atualização dos dados, sempre condizente com a necessidade e a finalidade estabelecidas previamente.

O sexto pilar estabelecido pela LGPD, dentro do artigo 6º, é referente a transparência, onde os titulares têm como direito receber informações precisas e acessíveis sobre o tratamento dos dados e quem são os agentes de tratamento.

O sétimo diz que devem ser utilizadas medidas técnicas e administrativas qualificadas para a proteção dos dados pessoais. Esse tópico é referente a segurança dos dados, ponto primordial na execução deste trabalho e a fim de garantir a privacidade de acessos não autorizados, acidentes ou destruição, perda, alteração, disseminação ou difusão ilícita.

O oitavo, nono e décimo incisos falam sobre a prevenção, não discriminação, responsabiblidade e prestação de contas, respectivamente.

Segundo o artigo 52 da Lei 13.709/2018, em casos de descumprimento da Lei Geral de Proteção de Dados, algumas sanções administrativas podem ser aplicadas pela autoridade nacional, ANPD. As sanções, que deverão ser aplicadas após um processo administrativo que "possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de

acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios" (BRASIL, 2018), são as seguintes:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> VII - (VETADO);
>
> VIII - (VETADO);
>
> IX - (VETADO).
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018).

4.5. Cenário Mundial

A) *General Data Protection Regulation* (GDPR)

O direito à privacidade faz parte da Convenção Europeia dos Direitos Humanos de 1950, que afirma: "Toda a pessoa tem direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência". A partir desse preceito, a União Européia buscou e busca constantemente garantir a proteção desse direito por meios legais, assim deu-se início ao Regulamento Geral de Proteção de Dados da União Europeia.

Chamado GDPR, *General Data Protection Regulation*, foi criado em 2016 com objetivo de determinar princípios para a Proteção de Dados Pessoais. Este regulamento

contém descrições específicas relacionadas aos meios eletrônicos e à internet. Ele visa controlar o uso de dados dos usuários de rede, os bancos de dados de empresas, prestadores de serviços e órgãos governamentais. (UNIÃO EUROPEIA, 2022).

A GDPR foi uma das precursoras entre as leis de proteção de dados e por isso é utilizada como base para construção de leis em outros países, como a do Brasil, LGDP. Ela orienta pessoas físicas e jurídicas que tratam dados pessoais de cidadãos da União Europeia dentro da Europa e em todo mundo, sendo esses um dos motivos pelo qual a GDPR é considerada uma das leis mais seguras e rígidas do mundo, se tratando de tratamento de dados. O regulamento entrou em vigor em maio de 2018, podendo assim aplicar multas severas a quem violar as regras estabelecidas pelo regulamento, com multas que chegam a milhões de euros. "As multas podem chegar a € 20 milhões de euros ou 4% da receita global, a qual for maior, além dos titulares de dados terem o direito de buscar compensação por danos" (UNIÃO EUROPEIA, 2022).

A norma também reserva o direito ao cidadão de solicitar uma espécie de relatório que mostre os dados que foram recolhidos e para o que serão utilizados, bem como a exclusão total ou parcial dos dados dos bancos de armazenamento. Caso a empresa sofra violação em relação às normas, têm um prazo de 72 horas para informar ao usuário sobre seus dados expostos sem autorização. O cidadão tem direito ainda de negar o processamento dos seus dados e exigir os termos e finalidades específicas que são utilizadas na empresa.

O regulamento em questão define alguns conceitos para termos jurídicos, a fim de melhor compreensão da lei. Pode-se perceber muitas semelhanças com a LGPD, lei de proteção de dados brasileira. Para a GDPR, a *personal data* são informações relacionadas a uma pessoa que pode identificar direta ou indiretamente esta pessoa, os dados pessoais. Sendo assim, como na LGPD, nomes e endereços de e-mail são exemplos desses dados. Informações de etnia, gênero, dados biométricos, opiniões políticas ou crenças religiosas também são consideradas dados pessoais e não dados sensíveis, como na LGPD. Outra semelhança nesse quesito é que os dados pseudônimos podem ser considerados pessoais se de alguma forma eles possam identificar o titular, algo que na lei brasileira é chamada de dado pseudonimizado.

O termo *Data processing* é sobre o processamento de dados, que caracteriza qualquer ação realizada com os dados pessoais, o que chama-se na LGPD de tratamento de dados. No regulamento diz-se que deve haver o consentimento para a coleta dos dados, pois se a finalidade for distinta do que era previsto no termo de consentimento inicial será considerada

como uma transgressão. O titular de dados é chamado de *Data Subject*, que refere-se a pessoa que tem seus dados tratados, quem concede suas informações à empresa.

O *Data Controller*, chamado na LGPD de controlador de dados, é o responsável por decidir por que e como os dados pessoais serão processados, assim como na lei brasileira. Por fim, o operador de dados aqui é definido como *Data Processor*, aquele responsável por tratar os dados, de acordo com as decisões do controlador. "O GDPR tem regras especiais para esses indivíduos e organizações. Eles podem incluir servidores em nuvem como o Tresorit ou provedores de serviços de e-mail como o Proton Mail" (UNIÃO EUROPEIA, 2022).

O regulamento de proteção de dados da União Europeia ainda apresenta mais uma entidade, chamada de DPO (*Data Protection Officer*), que no lei brasileira está em igual cargo que o encarregado de dados, responsável por realizar uma ponte e comunicação entre o *Data Controller* e o *Data Processor*, assegurando que todas as questões relacionadas a proteção de dados passe pelo encarregado de dados. Logo, este cargo é para que uma pessoa especialista na lei, com treinamento referente, faça com que a lei seja aplicada de forma correta, de acordo com todos os termos dispostos, sendo um cargo à parte de possíveis interferências internas da empresa e que responde diretamente e apenas ao mais alto nível de gestão da organização. O artigo 38 da *General Data Protection Regulation* de 2016, diz ainda que nenhuma outra pessoa poderá dar as instruções que um DPO relativas ao correto desenvolvimento da lei.

Apesar de tamanha importância, o DPO só será solicitado pelo controlador ou pelo processador de dados em casos específicos dispostos na lei. Segundo a seção 4, do *Data Protection Officer*, artigo 37 da *General Data Protection Regulation* de 2016:

> *1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.*

A GDPR ainda conta com 7 princípios ao se processar os dados, definidos pelo artigo 5.1-2 do regulamento. Estes preceitos são: Licitude, equidade e transparência, a qual determina que o dado deve ser lícito, fiel ao que foi coletado e transparente para o *Data Subject*; Limitação de finalidade fala sobre a necessidade do *Data Processor* e do *Data Controller* se limitarem ao tratamento do dado conforme o que foi definido nas finalidades

explicitadas ao titular de dados; Minimização de Dados nada mais é que coletar e processar apenas os dados essenciais para a realização do que foi proposto ao *Data Subject*; Precisão é o princípio que trata da atualização e exatidão do dado; Limitação de armazenamento significa que a empresa só poderá armazenar os dados em sua base pelo tempo determinado para a utilização descrita na finalidade; Integridade e Confidencialidade determinam que o processamento deve ser realizado de maneira que a segurança, a integridade e a privacidade do titular de dados sejam garantidas; e por fim, a Responsabilidade, que incumbe ao controlador a execução da GDPR de forma correta na empresa (UNIÃO EUROPEIA, 2022).

B) *California Consumer Privacy Act* (CCPA):

Os Estados Unidos atualmente não tem uma lei geral de proteção de dados como a GDPR ou a LGPD, apenas contam com o *Privacy Act of 1974*, mas contam com algumas leis que tratam de assuntos específicos, como o *Driver's Privacy Protection Act* (DPPA) que trata dos dados pessoais relacionados a veículos a motor, ou a *Children's Online Privacy Protection Act* (COPPA) que regulamenta o tratamento dos dados de crianças menores de treze anos em tipos de empresa.

Apesar disso, alguns estados já possuem leis mais abrangentes e rígidas, como a de Califórnia. Esta lei compreende alguns moldes da GDPR e foi feita em 2018, por ainda não existirem até então leis que protegessem os dados no país. A CCPA tem como objetivo então manter uma maior transparência em relação ao tratamento dos dados, sendo as empresas o maior alvo de implementação da lei.

Os direitos principais conquistados pelos consumidores através dessa lei foram

> *[...]you may ask businesses to disclose what personal information they have about you and what they do with that information, to delete your personal information and not to sell your personal information. You also have the right to be notified, before or at the point businesses collect your personal information, of the types of personal information they are collecting and what they may do with that information. Generally, businesses cannot discriminate against you for exercising your rights under the CCPA. Businesses cannot make you waive these rights, and any contract provision that says you waive these rights is unenforceable. (State of California Department of Justice, 2022).*

Assim como na GDPR, a CCPA considera dados pessoais como informações que podem identificar o indivíduo ou agregados familiares, como nome, correio eletrônico,

impressões digitais, dados de geolocalização ou até mesmo programas ou sistemas que possam criar perfis de características ou escolhas pessoais.

A lei na Califórnia abrange apenas os consumidores residentes do país e define regras para empresas comerciais, as quais têm sede, funcionários ou grande comércio no país. Para se enquadrar em uma empresa comercial passível de cuprir os requisitos da lei, devem ter algumas características, estas são

> *Have a gross annual revenue of over $25 million;*
> *Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or*
> *Derive 50% or more of their annual revenue from selling California residents' personal information. (State of California Department of Justice, 2022)*

A CCPA ainda salienta que a lei não pode ser aplicada em órgãos governamentais ou empresas sem fins lucrativos. Pelas limitações por se tratar de uma lei específica sobre dados pessoais, quando acredita-se que uma empresa possa ter infringido os termos estabelecidos pela CCPA, o cidadão só poderá processar a empresa caso as informações pessoais não criptografadas e tratadas sofrerem violação por falha da empresa em proteger os dados através das práticas de segurança adequadas.

Quando ocorrer essa situação, pode-se processar a empresa em decorrência de violação de dados ou por danos estatutários de até US$750 por incidente sofrido pelo titular de dados. Em caso de processo por danos estatutários, deve-se notificar a empresa por escrito que a mesma violou os termos da CCPA, com o prazo de 30 dias para a resposta da empresa informando que o problema foi corrigido e que não haverá mais nenhum descumprimento à lei. Em casos de danos estatutários, que a empresa possa resolver a violação ocorrida e der uma declaração escrita do ocorrido e a promessa de que não voltará a acontecer, não poderão ser processados, a menos que a empresa prossiga transgredindo a lei. (*State of California Department of Justice*, 2022).

4.6. Vulnerabilidades e ameaças à segurança

De acordo com a ISO 27000, a norma técnica referente a segurança da informação, uma vulnerabilidade é uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças. Uma vulnerabilidade de segurança pode ser vista como qualquer

fator que possa contribuir para gerar incidentes de segurança, como vazamento de dados, invasões de crackers, roubo de dados ou acesso não autorizado aos dados em questão.

4.6.1. Engenharia Social

A engenharia social é a técnica utilizada de forma criminosa para induzir usuários de sistemas e outros meios cibernéticos a enviar dados confidenciais, introduzir malware em seus computadores ou utilizar links em sites sem segurança. Geralmente os golpes acontecem com pessoas que não tem experiência em utilizar esses meios, mas não acontecem apenas com usuários desavisados. Esse crime pode acontecer de várias formas, sendo a online a mais recorrente devido a facilidade de manipular sites que possuem dados pessoais, como sites governamentais, de bancos ou formulários de preenchimento obrigatório para acender algum tipo de serviço. A engenharia social conta principalmente com o comportamento do usuário, sendo esse o próprio provedor da informação para o engenheiro social e que sofre com as consequências, golpes geralmente financeiros.

Barreto (2018) cita que um invasor tem condições de assumir papéis distintos, referentes a sua forma de atuação para invasão. Os crackers, denominação oriunda do idioma inglês, da palavra "*crack*", que pode ser traduzida livremente como "quebra", são os principais responsáveis envolvidos na quebra dos protocolos de segurança e privacidade das informações. Peixoto (2006) aborda o tema evidenciando as possibilidades de atuação dos agentes sociais, salientando ainda que existem milhares de engenheiros trabalhando em prol de seu próprio benefício e de interesses de contratantes.

O autor dá destaque a figuras conhecidas na história dos golpes, que ganharam lugares na mídia através da aplicação de golpes em grandes proporções, que na época gerou prejuízos a milhares de empresas e pessoas. O mais conhecido apontado pelo autor foi Frank Abgnale W. Jr, que teve sua história conhecida por meio do filme "*Catch me if you can*", título traduzido ao português como "Prenda-me se for capaz", estrelado por Leonardo DiCaprio em 2002.

Frank foi responsável pelo prejuízo de milhões de dólares a bancos e empresas, teve sua fama direcionada a dimensão dos golpes que eram aplicados, desde a década de 1960 nos EUA, enquanto ainda era adolescente. O golpista foi capaz de figurar diversos personagens, se passando por médico, advogado, piloto de aeronaves, professor, realizando saques em todos os tipos de ambiente. Até que foi capturado por agentes do FBI – *Federal Bureau*

Investigation, onde passou a ser parte da equipe de inteligência alguns anos depois, sendo responsável pela detecção de golpes e fraudes bancárias, pela sua vasta e longa experiência com procedimentos semelhantes e bem arquitetados.

Outro popular engenheiro social conhecido e citado por Peixoto (2006) foi Kevin Mitnick, um hacker que ganhou grande destaque nos anos de 1990, pela sua habilidade desenvolvida em burlar os sistemas da época. Mitnick desde adolescente aplica pequenos golpes em sua cidade, principalmente na companhia de transportes, falsificando bilhetes rodoviários, por exemplo, o que lhe permitia viajar de graça por todas as rotas disponíveis da companhia. Com o passar dos anos, ele acabou se tornando cada vez mais habilidoso e foi crescendo a dimensão dos golpes realizados, chegando até a atacar o governo norte-americano. Após uma série de fraudes realizadas com sucesso, Mitnick foi detido pelo serviço de inteligência norte-americano e hoje é conhecido por atuar a frente de uma organização de segurança da informação.

O próprio Mitnick (2003) destaca em seu livro a importância de observar o funcionamento dos mecanismos em grandes empresas ou mesmo no dia a dia, buscando encontrar as falhas e brechas existentes que colocam a segurança da informação em risco. O enfoque da engenharia social está em identificar o ponto mais fraco e realizar o ataque sobre este, buscando informações valiosas, que possam dar vantagens para o golpista.

4.6.2. Tipos de Engenharia Social

Algumas ferramentas são utilizadas pelos engenheiros sociais a fim de aplicar o golpe de forma que a vítima não perceba onde está envolvida. A primeira delas é o disfarce, parte indispensável para o ataque da engenharia social, que está relacionada à capacidade do golpista de esconder sua identidade e de assumir a identidade de outra pessoa que tem acesso à informação necessária para o ataque.

As informações descartadas de forma incorreta também são uma fonte de coleta para os golpes. O descarte de informação na forma física ou o simples ato de esvaziar a lixeira de um desktop não garante a segurança da informação descartada, ainda mais em casos de dados sigilosos. Deve-se sempre garantir o descarte seguro da informação, de maneira adequada, como o uso de softwares seguros para apagar informações sigilosas ou o uso de triturador ou da queima segura de folhas em caso de documentos físicos.

As redes sociais são hoje em dia um dos maiores meios de coleta de dados de forma facilitada para golpistas. A rede de amigos e conhecidos, ou não, é uma forma de exposição constante dos dados pessoais de cada indivíduo. Basta apenas uma busca simples para saber onde a pessoa vive, onde trabalha, quais são os locais que mais frequenta, quais os sites que visita, pelo uso de cookies de sites ou pelo banco de dados que não contam com criptografias e segurança de sistemas. Concursos públicos feitos por uma pessoa, seu cadastro de pessoa física, a escola na qual se formou, entre outros dados, podem ser facilmente encontrados com uma busca rápida pela internet.

Outro modo de manipulação da vítima é pelo apelo sentimental. As emoções são a maneira mais fácil de manipular uma pessoa, alguma história que leva a pessoa a crer que algum parente está em risco é o mais famoso golpe com que se depara. Golpes em larga escala levam a vítima a crer que vai se beneficiar, principalmente financeiramente, se realizar uma simples ação como clicar em um link piscando em vermelho que diz “clique aqui”.

A engenharia social conta com um infinidade de relações e técnicas para persuadir a vítima do golpe. No quadro a seguir serão apresentados os tipos mais recorrentes das técnicas e exemplos de como ocorrem:

Quadro 1 - Técnicas da engenharia social

Técnicas Aplicadas	Técnicas Complementares	Exemplos
Spying and Eavesdroping	Hoaxing	A utilização de uma mentira de modo a despertar o interesse da vítima e, dessa forma, estabelecer uma relação de amizade e confiança.
	Dumpster Diving	Métodos de recolha de informação
	Shoulder Surfing	
	Digital Dumpster Diving	
	Tailgating	Obtenção de acesso ao local
	Reverse Social	Criação de uma situação que faça com que a vítima necessite da sua ajuda de modo a obter a sua confiança.
	Impersonation / Pretexting	Fazer-se passar por alguém do interesse da vítima de modo a estabelecer um contacto, uma relação de amizade e obter a sua confiança.
	Baiting	A instalação de um *spyware* para a obtenção de informação
	Smishing	Através do contacto com a vítima por SMS, fazendo-se passar por alguém, tentar obter informação ou fá-la executar algo.
	Vishing	Através do contacto telefónico com a vítima, fazendo-se passar por alguém, tentar obter informação ou persuadir a executar algo.

Reverse Social	Hoaxing	Utilização de uma mentira que faça com a vítima necessite da sua ajuda
	Dumpster Diving	Obtenção de informação sobre os sistemas de informação de modo a identificar as vulnerabilidades da empresa
	Digital Dumpster Diving	
	Spying and Eavesdroping	
	Shoulder Surfing	Obtenção da password de acesso ao sistema
	Impersonation / Pretexting	Fazer-se passar por um especialista ou por alguém com autoridade.
	Baiting	Instalação de um *malware,* através da utilização de uma pen-usb, que crie uma situação em que seja necessário o recurso à sua ajuda.
	Software Interesting	Instalação de um software que crie um problema e seja necessário o recurso à sua ajuda.
	SPAM-mails	Um ataque ao servidor de modo que seja necessário o recurso a um especialista para a resolução do problema
	Footprint	Pesquisa de informação técnica sobre o servidor, de forma a auxiliar o ataque.
	Malware	Instalação de um malware que provoque danos
Impersonation / Pretexting	Hoaxing	Através da utilização de uma mentira, fazer-se passar por alguém com autoridade
	Dumpster Diving	Recolha de informação de forma a credibilizar a sua personificação.
	Digital Dumpster Diving	
	Spying and Eavesdroping	
	Baiting	Instalação de um spyware de forma a obter informação
	Shoulder Surfing	Obtenção dos dados de autenticação, de forma a conseguir fazer-se passar pela vítima.
	Phishing	Através do envio de um email enviado à vitima levá-lo a aceder a um site e a introduzir informação pessoal que depois será utilizada, por exemplo num contacto telefónico com o banco.
	Malware	Propagação de um vírus, por exemplo um *spyware*, com o objectivo de obter informação de forma a ser possível fazer-se passar pela vítima.
Phishing	Hoaxing	Através da utilização de uma mentira que cative o interesse da vítima em aceder a um determinado site "falso".
	Impersonation / Pretexting	No contacto com a vítima fazendo-se passar por alguém ou por instituição induz a vítima a aceder a um determinado site "falso".
	Smishing	Através do envio de uma mensagem SMS solicita a vítima a preencher um formulário alojado num site "falso".
	SPAM-mails	Envio de emails a solicitar que através de um link acedam a um site "falso". e preencha um formulário.
	Vishing	Através de um contacto telefónico solicita à vítima que aceda a um determinado site para actualizar os dados.

Fonte: Castro e Silva, 2013

O *phishing*, apresentado no quadro 1, por exemplo, é uma técnica muito utilizada pelos engenheiros sociais que consiste no envio de mensagens falsas para a vítima, buscando obter, sem o conhecimento desta, informações sigilosas. Essa técnica explora um vínculo de confiança entre a vítima e por quem o atacante está figurando. O ataque pode se dar não só pelo contato de pessoa para pessoa, mas quando o golpista também se utiliza de um *layout* de um site para enviar essas mensagens enganosas.

Como forma de obter essas informações, pode existir um questionário onde a vítima é solicitada para que insira informações confidenciais, como o número da conta, códigos de acessos, cadastro de pessoa física, dados do cartão de crédito, entre outros dados sensíveis.

"*Impersonation* é uma das técnicas mais importantes de engenharia social. Num ataque deste tipo o atacante deve possuir informação necessária para uma melhor personificação da vítima por quem se está a fazer passar" (REDMON, 2005 apud CASTRO E SILVA, 2013).

Em um ataque de engenharia social inversa, *reverse social*, também conhecida como *Quid Pro-Quo,* o atacante age como um especialista ou um funcionário de banco, por exemplo, à qual a vítima pede ajuda. Neste caso, a vítima precisa entrar em contato com o atacante para resolução de um suposto problema. Geralmente o atacante precisa ter um conhecimento prévio de quem é a sua vítima e o que seria um problema para ela a fim de convencer a vítima a iniciar o contato.

"A técnica de *Eavesdropping* consiste na escuta não autorizada de chamadas sendo uma técnica muito eficaz na recolha de informações pessoais e confidenciais" (MANJAK, 2006 apud CASTRO E SILVA, 2013). Já o *Support staff*, é uma técnica utilizada na espionagem, em que o engenheiro social entra na equipe e faz parte enquanto funcionário para coletar informações confidenciais, entrar em computadores de outros colaboradores, utilizar a extensão telefônica para solicitar uma informação, acesso ou ainda escutar outras ligações ou ainda instalar programas de observação ou cópias de informações.

5. METODOLOGIA

Para Fonseca (2002) a metodologia é o estudo da organização, sendo assim o caminho que se percorre para realizar uma pesquisa ou um estudo. Ou seja, a metodologia científica é "[...]o estudo sistemático e lógico dos métodos empregados nas ciências, seus fundamentos, sua validade e sua relação com as teorias científicas." (GERHARDT; SILVEIRA, 2009).

Este trabalho, quanto a abordagem, se caracteriza como uma pesquisa qualitativa e de natureza aplicada, conforme os conceitos estabelecidos por Fonseca (2002) "A pesquisa qualitativa se preocupa com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais". Uma vez que o ponto de vista que será apresentado é interno em relação à organização, com maior importância do contexto da pesquisa e quantidade de fonte de dados ampla.

Segundo Gerhardt e Silveira (2009) esta pesquisa tem seu caráter explicativo, segundo seus objetivos, uma vez que as informações apresentadas permitem compreender conceitos da Lei Geral de Proteção de Dados, porque a lei deve ser aplicada e suas consequências, como será feita a implementação da lei no contexto de um cursinho voluntário e a necessidade do cursinho em implementar a lei, as boas práticas e a organização dos dados. Bem como ocorre o desenvolvimento da lei na realidade, os empecilhos e os facilitadores, a estruturação de dados e informações por métodos utilizados no campo de conhecimento da biblioteconomia e da segurança da informação e como todo o projeto realizado afeta diretamente as ações da engenharia social.

A respeito do procedimento, este trabalho se caracteriza como um estudo de caso, já que "Visa conhecer em profundidade o como e o porquê de uma determinada situação que se supõe ser única em muitos aspectos, procurando descobrir o que há nela de mais essencial e característico" (FONSECA, 2002, p. 33). Sendo assim, o cursinho GALT Vestibulares será objeto de estudo para implementação da LGPD, análise das ações de engenharia social, a efetividade da Lei Geral de Proteção de Dados e para a estruturação de dados, com enfoque na segurança da informação, no contexto organizacional de uma organização educacional.

Foram utilizados passos metodológicos para o planejamento e desenvolvimento do projeto no cursinho no prazo de 1 ano, nos anos de 2021 e 2022, e realização deste trabalho:

1) Apresentação do cursinho GALT Vestibulares, enquanto objeto de estudo;
2) Realização de uma consultoria para um diagnóstico da situação inicial;

   a) Identificação das principais ameaças e vulnerabilidades existentes no GALT Vestibulares;
   b) Identificar os tipos de dados tratados no cursinho através de um mapeamento de dados;
   c) Identificar os acessos aos dados dos titulares e dados institucionais através de um mapeamento de acessos;
3) Gerar um plano de providências, estabelecido em 7 grandes áreas, para implementação da Lei Geral de Proteção de Dados, com base nos requisitos da lei e da situação inicial no cursinho:
   a) Treinamento e Conscientização;
   b) Estrutura de Governança;
   c) Inventário de Dados Pessoais, Fluxos e Acessos;
   d) Privacidade de Dados e Segurança da Informação;
   e) Políticas e avisos de privacidade;
   f) Contato com titulares;
   g) Gestão de incidentes.
4) Criar uma equipe para execução do plano de providências;
5) Criar uma política de privacidade;
6) Criar uma política de segurança da informação interna;
7) Executar o plano de providências, de acordo com os dados, informações e processos identificados no cursinho;
8) Estabelecer um mapeamento de processos da coordenação de compliance, bem como estruturar os dados e informações em pastas classificadas e catalogadas;
9) Revisar a aplicação de cada etapa e reiniciar o ciclo com novas medidas para os tópicos que não obtiveram êxito na execução.

Para este estudo de caso, foi de extrema importância a atuação dentro do cursinho na equipe de Compliance e Proteção de Dados, enquanto assessora e posteriormente diretora. Dessa forma foi possível analisar precisamente o funcionamento da lei na realidade, as dificuldades e facilidades da sua utilização para a instituição e para os usuários, as possíveis ações da engenharia social, o comportamento do usuário perante as mudanças necessárias para o cumprimento da segurança da informação.

6. ESTUDO DE CASO

6.1. O GALT Vestibulares

O GALT Vestibulares é um cursinho voluntário, localizado em Brasília, criado em 2015 por 4 estudantes da Universidade de Brasília. Esse cursinho tem como objetivo ser um local de duplo impacto, uma instituição de empoderamento de jovens de baixa renda até o ensino superior. Desde a equipe organizacional até a equipe institucional, é formada por graduandos ou graduados nas áreas requisitadas. Hoje o cursinho conta com cerca de 110 voluntárias e voluntários, mais de 450 alunos, e é uma organização da sociedade civil de interesse público (OSCIP). Ser uma OSCIP significa ser uma qualificação jurídica atribuída a entidades privadas atuando em áreas típicas do terceiro setor público com interesse social, que podem ser financiadas pelo Estado ou pela iniciativa privada sem fins lucrativos.

Como anteriormente dito, a equipe organizacional até a equipe institucional, é formada por graduandos ou graduados em uma instituição de ensino superior reconhecida pelo Ministério da Educação, nas áreas requisitadas, com objetivo também de gerar lideranças, conhecimentos em temas de empreendedorismo social no terceiro setor, capacitação em planejamento e organização, além da facilitação em relações interpessoais.

A equipe conta com professores, coordenadores pedagógicos, administradores, advogados, bibliotecários, psicólogos e outras graduações a fim capazes de exercer os cargos. O GALT Vestibulares tem como princípio o apoio a comunidade e o Brasil por meio de oportunidades igualitárias e democráticas à educação superior e na promoção do voluntariado. O GALT Vestibulares foi, em 2018, selecionado pelo programa *Young Leaders of the Americas Initiative* (YLAI), organizado pelo governo dos Estados Unidos, que capacita empreendedores sociais da América Latina.

Hoje o cursinho conta com mais de 150 voluntárias e voluntários, mais de 500 alunas e alunos por ano e um total de mais de 1000 aprovados, e é uma organização da sociedade civil de interesse público (OSCIP). Ser uma OSCIP significa ser uma qualificação jurídica atribuída a entidades privadas atuando em áreas típicas do terceiro setor público com interesse social, que podem ser financiadas pelo Estado ou pela iniciativa privada sem fins lucrativos.

Segundo o documento de regimento interno do GALT (2022), o cursinho tem sua estrutura organizacional composta por: I. Assembleia Geral; II. Conselho Administrativo; III. Conselho Fiscal; IV. Comitê Eleitoral; V. Presidência Institucional; VI. Presidência

Organizacional; VII. Diretoria Financeira; VIII. Diretoria de Gente e Gestão; IX. Diretoria de Marketing; X. Diretoria de Captação de Recursos; XI. Diretoria de Dados; XI. Diretoria de Ensino; XII. Coordenação Pedagógica; XIII. Coordenação Jurídica; XIV. Coordenação de Compliance e Proteção de Dados; XV. Coordenação de Psicologia; XVI. Coordenadoria de Área; e XVII. Docentes: Professores, monitores e corretores de redação.

Ainda de acordo com o regimento interno (2022), o art. 26° diz sobre o que compete à Presidência Institucional, sendo assim:

I. Representar o Galt Vestibulares, ativa e passivamente, judicial e extrajudicialmente;

II. Cumprir e fazer cumprir este Estatuto e o Regimento Interno;

III. Convocar e presidir as reuniões da Diretoria;

IV. Gerenciar a publicidade, além de elaborar, produzir e promover campanhas publicitárias,

eventos e anúncios referentes ao Galt Vestibulares; e

V. Estabelecer e promover parcerias com instituições públicas e privadas e/ou pessoas físicas.

Enquanto o art. 27° diz sobre o que compete à Presidência Organizacional:

I. Representar o Galt Vestibulares, ativa e passivamente, judicial e extrajudicialmente;

II. Cumprir e fazer cumprir este Regimento Interno e o Estatuto;

III. Convocar e presidir a Assembleia Geral;

IV. Convocar e presidir as reuniões da Diretoria; e

V. Assinar todos os documentos pertinentes às obrigações financeiras do Galt Vestibulares.

Segue abaixo o organograma completo da organização representado pela figura 5:

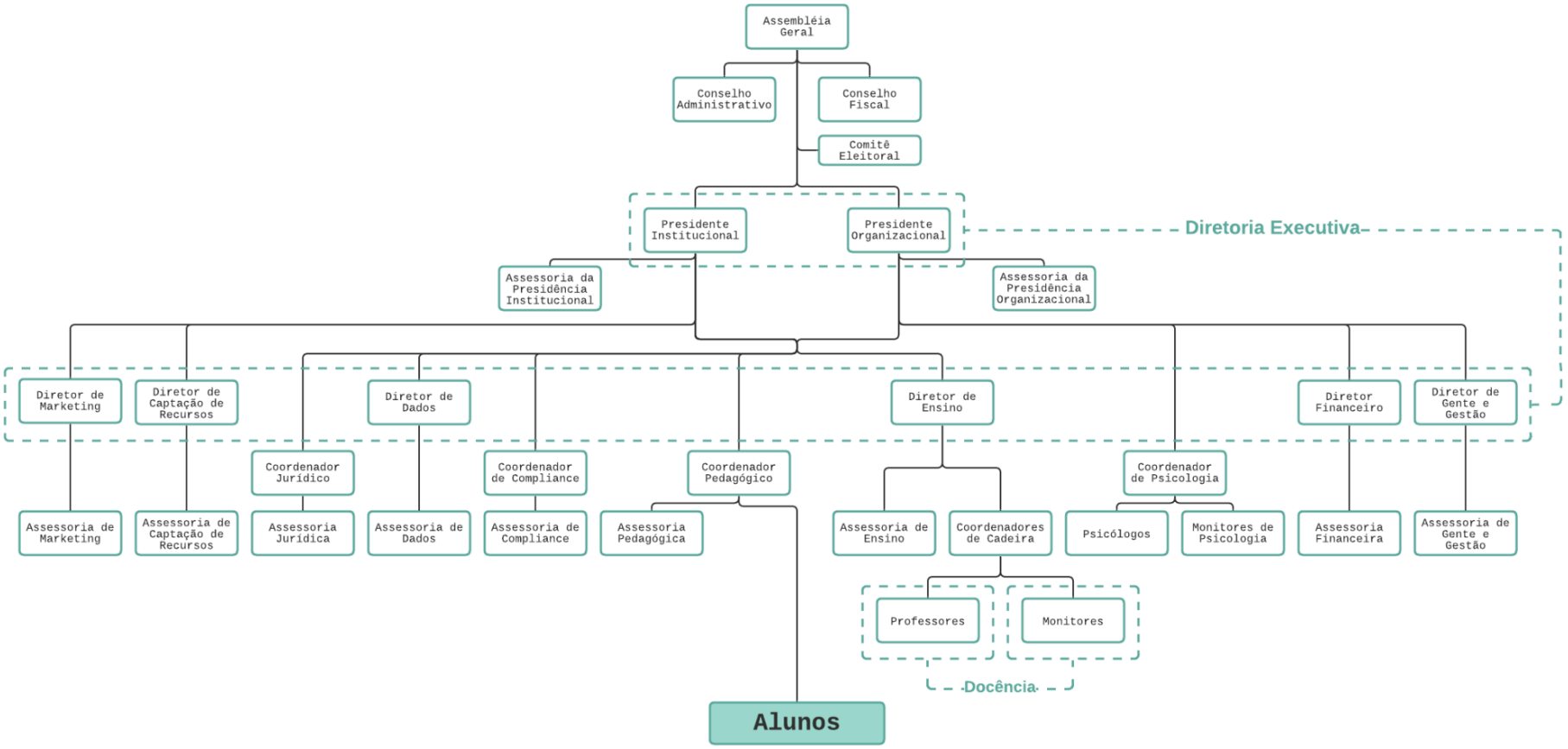

Figura 5: Estrutura Organizacional
Fonte: GALT Vestibulares (2022)

Mesmo com as as áreas separadas e as presidências responsáveis por cada uma delas, além do encargo de tratar de todas as questões externas que também cercam a organização, todas trabalham em conjunto e sincronia, uma vez que muitos dos processos internos dependem do trabalho conjunto das diretorias e presidências.

A diretoria de Gente e Gestão, uma das maiores do GALT, trabalha diretamente a condução de processos seletivos, processos de integração de voluntários, acompanhamento de desempenho, ações de capacitação, descrição de cargos, análise e aprimoramento dos processos de gestão de pessoas e gestão de dados dos colaboradores. Tem-se preferência por pessoas graduadas ou graduandas nos cursos de psicologia, administração ou tecnólogo em Gestão de Recursos Humanos.

A diretoria de Ensino é uma das mais complexas, acompanhada da diretoria de Gente e Gestão, devido ao grande fluxo de dados, processos e demandas, e nela temos algumas atribuições, como coordenar e supervisionar as atividades de docência com base nas demandas institucionais, auxiliar na elaboração do calendário acadêmico, elaborar grades horárias, coordenar a elaboração do material didático, intermediar a relação entre os coordenadores de cada matéria (coordenadores de cadeira) com os membros de suas equipes (professores), bem como monitorar as atividades de docência e gerir o processo seletivos de alunos.

A diretoria de marketing tem como objetivo estabelecer políticas e ações de comunicação interna e externa, definir os canais e estratégias de comunicação, elaborar campanhas para produtos e serviços, cobrir eventos da instituição e desenvolver os conhecimentos em ferramentas de edição de fotos, vídeos e peças. Para atuar nesse cargo, é preciso que a pessoa seja graduada ou esteja na graduação de preferência em cursos como Comunicação Social, Publicidade e Propaganda, Jornalismo e Comunicação Organizacional.

Para a coordenação pedagógica é necessário ter capacidade de controlar a frequência de alunos, elaborar atividades de motivação e engajamento, algo primordial, pois o cursinho não conta com contribuição financeira dos alunos e muitas vezes o interesse do aluno se perde pela falta de compromisso financeiro com o cursinho. Além dessas competências, é necessário também lidar com encaminhamento de alunos para a coordenação de psicologia, devido a toda a carga do contexto de cada aluno, facilitar o acesso aos editais e datas dos principais vestibulares, elaborar relatórios de desempenho individual dos alunos em simulados, em conjunto com a diretoria de dados e receber feedback dos alunos. Para exercer

o cargo de coordenador(a) pedagógico(a), a pessoa deve ser graduada ou estar em uma graduação nas áreas de pedagogia, psicologia ou algum curso de licenciatura.

Para ocupar cargo na coordenação de psicologia, é necessário primeiramente que a pessoa esteja cadastrada no e-Psi, que lista os profissionais capacitados a prestarem serviço psicológico on-line ou já possuírem o número no Conselho Regional de Psicologia (CRP) ativo. Para além da documentação validada, é atribuído ao coordenador psicológico a organização dos serviços de psicologia de acordo com as demandas da instituição, orientar e aprimorar o desenvolvimento da equipe, supervisionar o registro de atividades, e armazenar os documentos gerados nos atendimentos dos alunos, bem como manter o diálogo com a diretoria executiva.

A diretoria de Compliance e Proteção de Dados é responsável, em suma, por orientar, supervisionar e controlar as práticas de segurança da informação no cursinho, elaborar e executar um plano de classificação dos documentos físicos e digitais, organizar e controlar os acessos aos canais de comunicação e aos documentos do cursinho e aplicar em conformidade a Lei Geral de Proteção de Dados a toda a organização durante a gestão dos documentos e das pessoas envolvidas no tratamento de dados. A pessoa que irá trabalhar no cargo de diretora de compliance e proteção de dados deve ser graduada ou estar em graduação nos cursos de arquivologia, biblioteconomia ou direito.

A diretoria de Captação de Recursos tem como principal objetivo o contato com empresas externas a fim de angariar parcerias para o projeto do GALT, uma vez que não há cobrança de mensalidade dos alunos para estudar no cursinho. Essa diretoria apresenta a proposta do cursinho com todos os investimentos detalhados, como o uso de papel, grampeadores, lápis, canetas e borrachas para os dias de simulados presenciais ou os recursos em dias de palestras e eventos motivacionais, além de prêmios nos eventos dos membros da equipe, os quais são todos voluntárias e voluntários.

A área do Jurídico do GALT já tem como requisito, para a diretoria, uma pessoa com graduação no curso de direito e com número válido de cadastro na Ordem dos Advogados do Brasil para atuação no Distrito Federal. As atribuições para essa diretoria é que deve elaborar, analisar e revisar contratos, auxiliar em auditorias legais, auxiliar em questões consultivas, representar o GALT em atividades do judiciário, em meios arbitrais ou em quaisquer meios autocompositivos de solução de conflitos.

Já na diretoria de dados, os requisitos para exercer o cargo é ser graduado ou estar na graduação de cursos capazes de cumprir com a coleta, visualização e análise dos dados do

cursinho, a fim de obter insights e métricas que possam direcionar a tomada de decisões. Além disso, que seja capacitado para desenvolver indicadores e relatórios, os quais avaliem os resultados e impactos gerados pelo cursinho na comunidade que é atendida pelo GALT.

Dessa maneira, pode-se compreender que o cursinho se trata de uma grande rede interna e externa, que trabalha em conjunto com parceiros, como a Universidade de Brasília e a Brasil Cursinhos, que consiste em um movimento dos cursinhos universitários populares a partir da integração e do desenvolvimento de lideranças para transformar a educação no Brasil, como uma forma de apoio e base para o crescimento dos cursinhos em cada estado. Nesta rede de cursinhos são oferecidos cursos, de longo e curto prazo, de forma gratuita para as voluntárias e voluntários, por exemplo, com objetivo de angariar a liderança e conhecimento dos membros dos cursinhos.

6.2. Diagnóstico Inicial

A partir das informações apresentadas no tópico anterior, pode-se reconhecer o tratamento de dados em diversos processos realizados pelas diretorias e presidências do cursinho. Nessa perspectiva, entendeu-se, a partir de um diagnóstico no início do projeto pela diretoria de compliance e proteção de dados, que o cursinho GALT Vestibulares tinha algumas falhas em relação à segurança da informação, principalmente devido a ação despreparada dos usuários das bases de dados do cursinho, ou seja, as voluntárias e voluntários.

A plataforma principal de armazenamento de dados do cursinho é o Google Drive, da empresa Google, a plataforma para aulas e reuniões, *Microsoft Teams*, e um disco rígido (HD) externo para realização de *backups* de todos os materiais. Ações como o *login*, sincronização e *download* de documentos com dados através dos *e-mails* institucionais, providos para o GALT, em parceria com a empresa Google, nos computadores pessoais das voluntárias e voluntários ou em seus celulares, faziam com que documentos com dados pessoais de voluntárias, voluntários, alunas e alunos estivessem em risco de vazamento de dados. Outro exemplo de risco provido pelo desconhecimento dos usuários da plataforma, era o uso de wi-fi público ou desconhecido, tanto para realizar atividades do GALT, quanto para tarefas pessoais, o que coloca em risco os dados, pelo acesso livre de outros utilizadores da rede.

Os dados pessoais e sensíveis que foram identificados na base de dados utilizada pelo cursinho, a partir do mapeamento e inventário dos dados, eram dados capazes de informar a identificação das pessoas, como nome, endereço, situação financeira, escola onde estuda ou

universidade, gravações de aulas com uso de imagem e áudio de alunas, alunos, professoras e professores, fotos dos mesmos utilizados para promoções do cursinho ou cadastro, dados de entrevista, notas e provas dos alunos.

Estes dados ficavam dispostos no drive em pastas de acesso aberto para quaisquer voluntários que possuíssem o e-mail institucional, ou seja, toda e qualquer ação desprovida de cuidado, com ou sem intenção a partir de um membro da equipe, colocava em grande ameaça a segurança dos dados em questão. Mas a partir da criação da Lei Geral de Proteção de Dados e todos os grandes casos que vinham acontecendo em todo o mundo relacionados a vazamento de dados, a presidência organizacional e institucional do cursinho decidiu por criar uma diretoria que realizasse um planejamento estratégico para a implementação da LGPD, executasse esse planejamento e fizesse a organização da informação, visando a segurança dos dados.

6.3. Projeto Compliance e Proteção de Dados

Devido à situação inicial do cursinho, foi identificada a necessidade de realizar uma implementação da Lei Geral de Proteção de Dados, utilizando o método de planejamento PDCA e a ISO 27001 para gerenciamento, visando mitigar incidentes de segurança causados pela própria organização, como apagamento indevido dos dados ou alterações não previstas, a ação de crackers, possíveis sanções administrativas e resguardar os direitos dos titulares de dados.

Resgatando os passos apresentados na metodologia, o projeto seguiu as 7 grandes áreas, definidas no plano de providências (anexo B), para implementação da Lei Geral de Proteção de Dados, com base nos requisitos da lei e da situação inicial no cursinho. Sendo esses passos o Treinamento e Conscientização; Estrutura de Governança; Inventário de Dados Pessoais, Fluxos e Acessos; Privacidade de Dados e Segurança da Informação; Políticas e avisos de privacidade; Contato com titulares; e Gestão de incidentes.

Além da implementação da lei, foi preciso realizar um processo de organização das informações contidas na base de dados. Esse processo se deu através de um mapeamento de processos e dados tratados, estruturando posteriormente os dados e informações em pastas classificadas em cadeias e catalogadas. A catalogação foi realizada conforme os anos referentes aos documentos, suas sub-pastas com palavras-chave que caracterizam a

informação inserida nas pastas e cores que diferem cada ano, com objetivo de gerar uma recuperação facilitada dos dados, mais segurança e controle de acesso por parte dos usuários.

Para alcançar os objetivos, foram apontados no anexo B, de cada parte do plano de providências de adequação à LGPD, foi preciso montar uma equipe e uma diretoria de compliance e proteção de dados, que deu início em agosto de 2021, com apenas uma advogada, DPO.

Posteriormente, em novembro de 2021, com a entrada de uma assessora, graduanda em biblioteconomia, e uma assessora advogada, formou-se uma equipe para execução do planejamento, por meio do processo seletivo para novos voluntários, com regras estabelecidas pelo GALT. Dessa forma, a diretoria contava com três voluntárias durante o período de um ano para adequação do cursinho a LGPD. A autora deste trabalho participou da equipe inicialmente enquanto assessora e posteriormente como diretora.

Primeiramente foi dado início ao processo de implementação da LGPD no cursinho, onde a então diretora realizou a elaboração de uma *política de privacidade*, que pode ser consultada em sua integridade no anexo A, para publicação no site do cursinho, um dos principais documentos que asseguram tanto a instituição, quanto o usuário. Além desse documento, foi produzida uma *política de segurança da informação*, o qual tem como objetivo definir as regras e boas práticas internas que garantam a segurança da informação tratada no GALT Vestibulares.

Ambos os documentos foram constituídos de acordo com o Marco Civil da Internet, Lei Federal no 12.965/2014, e a Lei Geral de Proteção de Dados Pessoais, Lei no 13.709 de 14 de agosto de 2018, e legislações nacionais aplicáveis no âmbito da privacidade, segurança e proteção de dados. A partir dessa política de segurança que foi feito todo o processo de implementação, ela ainda define que

> A presente política define os princípios gerais relativos ao tratamento e proteção de dados pessoais, incluindo a guarda, utilização, disposição, registro documental, armazenamento, preservação, segurança e eliminação dos mesmos. Esta política pode ser complementada por outras políticas, procedimentos, orientações, avisos ou informações de caráter mais específico que sejam considerados necessários para o tratamento de outros dados pessoais. A política de segurança da informação aplica-se a todos os colaboradores internos, parceiros ou colaboradores externos, sobre os quais o GALT realize operações de tratamento de dados pessoais, bem como todas as formas de registo de dados, sejam elas em formato digital ou em papel. (GALT, 2021).

A política de segurança da informação e a política de privacidade ainda seguem os preceitos da gestão de segurança da informação, afirmadas pela ISO 27001 e pela norma

10/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSI/GSIPR) (2012), referentes a disponibilidade, integridade, confidencialidade e autenticidade.

> Integridade: capacidade de manter os dados pessoais inalterados de modo a prevenir, recuperar e reverter alterações dos dados não autorizadas ou acidentais;
> Autenticidade: garantia da integridade, preservação e validade da informação durante todo o processo de tratamento dos dados, desde o momento da recolha até à sua eliminação;
> Disponibilidade - possibilidade de acesso aos dados, sempre que necessário;
> Confidencialidade - capacidade de garantir que os dados serão tratados apenas por pessoal autorizado. (GALT, 2021)

O Marco Civil e a Lei Geral de Proteção de Dados foram implementadas no GALT em etapas, seguindo o plano de providências (anexo B), uma vez que a segurança da informação se dá num conjunto de práticas feitas por toda uma organização. Dessa forma, os próximos tópicos a serem apresentados seguem de acordo com as 7 grandes áreas citadas anteriormente, fazendo referência ao plano de providências.

6.3.1. Treinamento e Conscientização

Para a etapa de treinamento e conscientização, a equipe tem como objetivo garantir que todas as voluntárias e voluntários dentro da organização compreendam as responsabilidades na área da segurança da informação e cumpram com as medidas protetivas em conformidade com as funções e necessidades dentro do GALT.

O objetivo é fazer com que o usuário tenha um comportamento no meio cibernético que evite a ação da engenharia social, o vazamento dos seus próprios dados e da instituição. Além disso, deve-se assegurar que os interesses do cursinho e dos colaboradores, empresas parceiras ou prestadoras de serviço estejam protegidos durante todo o processo de início, mudanças ou cessação das funções relacionadas à instituição.

A conscientização é realizada por meio de templates com informações sobre boas práticas (Figura 6), o que é a LGPD e informações acerca do tema, além de treinamentos online síncronos com cada equipe de cada diretoria, professores e coordenações de cadeira sobre a implementação da lei no cursinho, sua importância para o dia a dia e como cada pessoa poderia colaborar para o bom desenvolvimento da proteção de dados.

A comunicação com todas as equipes é realizada por meio da plataforma Slack, que é um programa de mensagens instantâneas desenvolvido pela Slack Technologies e de propriedade da Salesforce, desenvolvido para comunicações profissionais e organizacionais.

Nessa plataforma também eram postadas as artes de conscientização e documentos pertinentes para visualização de toda a equipe interna.

Figura 6: Guia de boas práticas
Fonte: GALT Vestibulares (2022)

As diretoras são responsáveis por participar das reuniões síncronas quinzenais realizadas pelo *Google Meet*, da DIREX (grupo de diretoras, diretores e presidências do GALT). Nessas reuniões as diretoras tinham, para além de discutir os próximos passos do cursinho e das diretorias em um geral, observar e verificar as atividades que ocorriam no cursinho para manter a conformidade com a LGPD.

6.3.2. Estrutura de Governança

Pensando no melhor monitoramento e avaliação dos processos internos da diretoria e da instituição para conformidade com a LGPD, a equipe de compliance e proteção de dados gerou um manual de boas práticas com 28 itens para auxílio das voluntárias e voluntários do cursinho, que podem ser consultados no apêndice A.

Esse e outros documentos desenvolvidos dentro do GALT, estão armazenados no *Google Drive*, mencionado anteriormente, que é utilizado como base de dados da instituição. Existem pastas que foram organizadas em cadeias para cada diretoria e suas respectivas subpastas, datas conforme os anos das gestões, de acordo com as necessidades de cada equipe, que correspondem ao *framework*. Dentro da pasta da diretoria de compliance e proteção de

dados, existe uma série de documentos internos que garantem as evidências de conformidade da lei, cumprindo o princípio da responsabilização e prestação de contas.

O plano de governança não pode ser elaborado em tempo hábil, mas pode-se dizer que o documento definido para essa finalidade espelha as operações, serviços e modo como a proteção de dados é considerada. Esse documento são os inventários de dados de cada diretoria, com base no inventário de dados disponibilizado pelo governo federal do Brasil e no guia de elaboração de inventário de dados pessoais, sendo o inventário de dados obrigatório segundo o artigo 37 da Lei Geral de Proteção de Dados.

6.3.3. Inventário de dados pessoais, fluxos e acessos

O inventário de dados tem como objetivo identificar as operações de tratamento de dados pessoais realizadas pela instituição no papel de controlador (LGPD, art. 5º, VI). Sendo atualizado regularmente, o inventário dá permissão para que a equipe possa responder ao requisito de manter um registro das operações de tratamento de dados pessoais, conforme estabelecido pela LGPD. Ele consiste em uma lista geral e simples de todos os processos que lidam com tratamento de dados inventariados (Lista Inventário). Depois, pelo menos, um formulário de inventário (Template), contendo a identificação do processo, o encarregado de dados e os agentes responsáveis pelo tratamento, as fases/ciclos de vida do tratamento do dados, ou seja, prazos de conservação de dados, com vista a eliminar periodicamente a informação que não é necessária, de que forma o dado é coletado, armazenado, processado, compartilhado e eliminado, o escopo e a natureza dos dados pessoais, a finalidade do tratamento do dado, a descrição do que são os dados pessoais, a frequência do tratamento do dado pessoal e as instituições com que o dado é compartilhado.

Essa guia do formulário poderá ser replicada e preenchida quantas vezes for necessário para documentar todos os processos que tratam dados pessoais na instituição. Por fim, existe ainda no modelo uma lista que apresenta sugestões de informações para preenchimento do inventário de dados.

Além do inventário, foi realizado o mapeamento do fluxo de dados de cada diretoria, baseado nas informações coletadas nas pastas do drive de cada diretoria e pelos dados inventariados. O mapeamento conta com o fluxo desde a coleta, por onde o dado é recolhido, passando pela retenção, onde o dado é armazenado, o uso, que descreve a finalidade, o compartilhamento, que diz por onde e com quem o dado é partilhado e por fim, a eliminação,

que diz como o dado é descartado. Para uma melhor continuidade do trabalho realizado, foi realizado um mapeamento de processos da compliance e proteção de dados, através da plataforma Bizagi Modeler, representados pelas figuras 7 e 8:

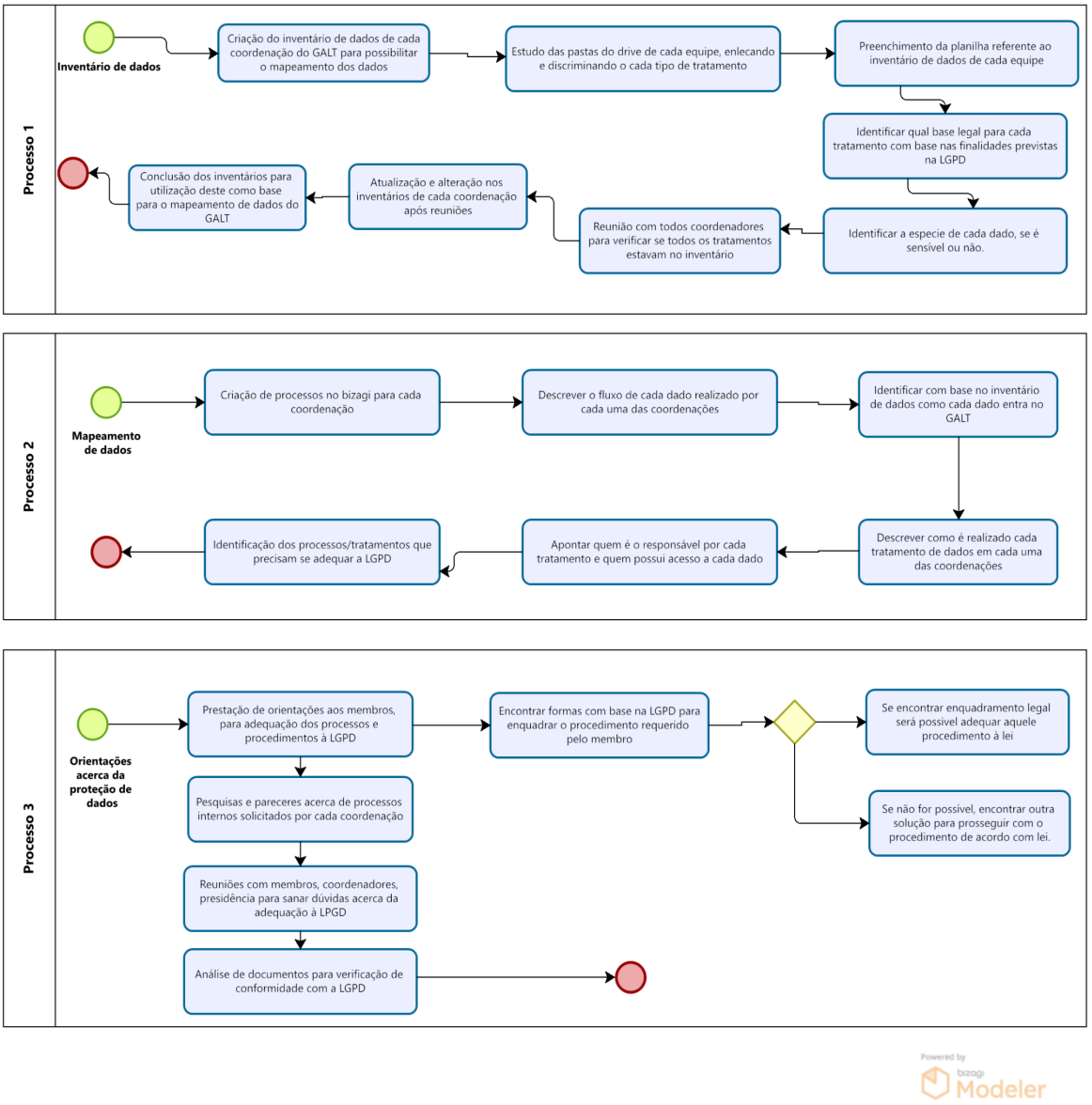

Figura 7: Mapeamento de processos 1
Fonte: GALT Vestibulares (2022)

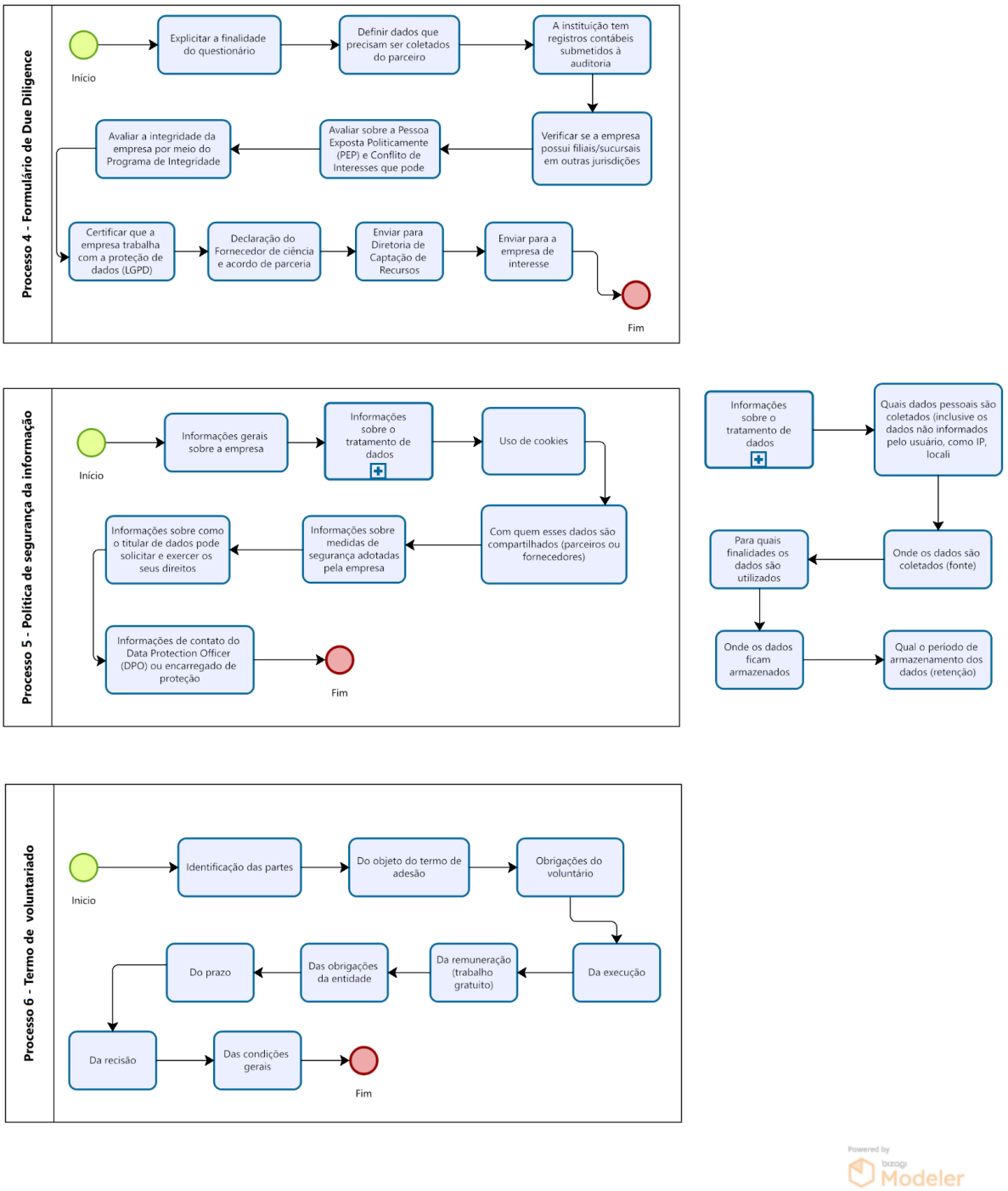

Figura 8: Mapeamento de processos 2
Fonte: GALT Vestibulares (2022)

Houve ainda a tentativa de realização de um mapeamento de acessos das pastas, para segmentação de acesso às pastas, mas que se tornou inviável no período de realização do projeto devido a falta de respostas aos formulários e planilhas enviadas as equipes de cada diretoria e coordenação de cadeira.

6.3.4. Privacidade de Dados e Segurança da Informação

Com objetivo de estabelecer mecanismos de obtenção de consentimentos válidos por parte dos titulares de dados, quando aplicáveis, a equipe foi responsável por gerar documentos de consentimento para alunas, alunos, voluntárias e voluntários do cursinho.

Os documentos feitos foram o termo de consentimento de captação, divulgação e armazenamento de imagens em fotografia ou vídeo, atualização do termo de voluntariado em conformidade a lei geral de proteção de dados, o termo de cessação dos direitos autorais, que pode ser consultado no anexo C, para uso da propriedade intelectual, referente a aulas gravadas e documentos produzidos pelas professoras e professores do cursinho.

Os documentos relacionados aos alunos são de responsabilidade de consentimento dos responsáveis, uma vez que os alunos são em sua maioria menores de idade e os dados tratados são de característica sensível. Neste quesito, poderão ser coletados dados pessoais de menores sem o consentimento, apenas, quando a coleta for necessária para contatar o (a) responsável legal, podendo ser utilizados uma única vez e sem armazenamento, ou para sua proteção, e de forma alguma poderão ser repassados a terceiros sem o consentimento dado por pelo menos um dos pais ou pelo(a) responsável legal. (BRASIL, 2018)

Para além desses documentos, pensando na maior segurança das pessoas envolvidas com o cursinho e os dados tratados, foi produzida um documento capaz de regulamentar o uso dos dispositivos móveis das voluntárias e voluntário, uma vez que o cursinho não detém de um espaço físico para trabalho e dispositivos eletrônicos institucionais para uso do trabalho.

Para isso, a equipe foi responsável por gerar uma política de byod, que consiste em instruções para o uso apropriado de dispositivos móveis no GALT, no intuito de minimizar os riscos envolvidos em sua utilização e atender às legislações, em especial a Lei Geral de Proteção de Dados, normas e boas práticas recomendadas. Esta política, que se encontra no apêndice B, se aplica a todos os colaboradores do GALT. Todos esses colaboradores serão tratados nesta política como usuários.

Se tratando da relação do GALT com parceiros externos, também é de suma importância que os termos da lei geral de proteção de dados também sejam aplicados. Dentro das exigências do Programa de Integridade estabelecido pelo GALT Vestibulares, há a necessidade de melhor conhecer os parceiros de negócios, o checklist de *Due Diligence*, que pode ser consultado no apêndice C, possui o intuito de realizar uma melhor análise dos parceiros.

6.3.5. Políticas e avisos de privacidade

No que se refere às políticas e avisos de privacidade, foi de suma importância a definição e publicação de avisos de utilização de *cookies* válidos no site do cursinho, com intuito de garantir o consentimento do uso dos dados coletados pelo site.

> Os cookies são pequenos arquivos de texto que um site, quando visitado, armazena no computador do usuário ou no seu dispositivo móvel, por meio do navegador de internet (browser). A colocação de cookies ajudará o site a reconhecer o seu dispositivo numa próxima visita, lembrando quem você é e quais seus hábitos de navegação, além de acessar as informações do seu cadastro em nosso website para facilitar e agilizar o preenchimento de formulários. (GALT, 2022).

Assim que o usuário se conecta ao site, recebe um aviso em uma barra inferior descrita "Usamos *cookies* no nosso site para ver como você interage com ele. Ao aceitar, você concorda com o uso de *cookies*", com o link de acesso para a política de privacidade (anexo A) e as opções de configuração ou “aceitar”.

Como opções de configuração, tem-se os cookies essenciais, sempre ativos, referentes às funcionalidades essenciais, tais como segurança, verificação de identidade e gestão de rede. Esses cookies não podem ser desativados; os cookies de marketing, usados para rastrear a eficácia da publicidade, fornecer um serviço mais relevante e anúncios melhores para atender aos seus interesses; os cookies funcionais, que coletam dados para lembrar as escolhas que os usuários fazem e para melhorar e proporcionar uma experiência mais personalizada; e os cookies analíticos, os quais ajudam a entender como os visitantes interagem com o site, descobrir erros e fornecer uma melhor análise geral.

6.3.6. Contato com titulares

Em relação ao contato da diretoria de Compliance e Proteção de Dados com os titulares de dados, foi definido um plano de resposta a possíveis solicitações de acordo com o escopo da LGPD. A instrução detalha as atividades, responsabilidades e documentação associada em relação aos pedidos dos titulares dos dados pessoais nomeadamente o disposto no art. 18º, da lei 13.709, em (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade

com o disposto na LGPD; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) revogação do consentimento, nos termos do § 5º do Art. 18º da LGPD.

Todos os mecanismos para registro, rastreamento, resposta e controlo dos pedidos de resposta aos titulares de dados estão dispostos no plano de resposta, além de definir que o canal oficial para o contato será pelo e-mail da diretoria, compliance@galtvestibulares.com, disponibilizado em todos os documentos disponíveis para os usuários das redes da cursinho.

6.3.7. Gestão de incidentes

Em caso de vazamento de dados, ou seja, um incidente de segurança, deve-se avaliar internamente o incidente, quanto a sua natureza, categoria e quantidade de titulares de dados afetados e consequências concretas; comunicar ao encarregado de dados (art. 5º, VIII da LGPD); Comunicar ao controlador, se for o caso de um operador de dados a lidar com a situação; Comunicar a ANPD e ao titular de dados, em caso de risco relevante aos titulares (art. 48 da LGPD); e elaborar uma documentação com a avaliação interna do incidente, as medidas tomadas e a análise de risco, para comprovativo de cumprimento do princípio de responsabilização e prestação de contas, disposto no artigo 6º, inciso X da LGPD.

Como forma de gerenciar os incidentes em caso de violação de dados pessoais, foi produzido um plano de resposta a incidentes com base no modelo disponibilizado pela Datashield Brasil, como forma de estabelecer os procedimentos necessários em cada tipo de situação e conforme a criticidade identificada. Esse plano de resposta também define as informações que devem ser notificadas aos titulares de dados e Autoridade Nacional de Proteção de Dados (ANPD) em caso de vazamento de dados pessoais.

7. CONSIDERAÇÕES FINAIS

Neste trabalho foi possível estruturar os dados e as informações das alunas e alunos, das voluntárias e voluntários e os dados institucionais, além de apresentar como foram tratados, adequando o cursinho GALT Vestibulares à nova Lei Geral de Proteção de Dados. Executou-se um plano de providências para implementação da lei prevista, com apoio de profissionais da área do direito. Foram utilizados recursos teóricos e práticos da biblioteconomia, como classificação das pastas e documentos em cadeia, a catalogação dos documentos na base de dados, e processos da gestão de segurança da informação, feitos com apoio de estudantes da área, para o melhor desenvolvimento organizacional no processo de adequação e facilitação da recuperação dos dados e documentos.

Este estudo de caso apresentou informações que permitem compreender conceitos da Lei Geral de Proteção de Dados, como foi feita a implementação da lei no contexto de um cursinho voluntário e a necessidade do cursinho em implementar a lei, as boas práticas e a organização dos dados. A partir do trabalho preventivo da equipe de Compliance e Proteção de Dados, o cursinho voluntário se adequou às normas previstas pela LGDP. Dessa forma não houve nenhum incidente de segurança, durante o período de um ano, caracterizado principalmente pelo vazamento de dados dos titulares.

Contudo, apresentou o desenvolvimento da lei na realidade, sendo assim um dos empecilhos maiores foi a falta de engajamento e resposta dos voluntários em formulários de coleta de informações necessárias para a implementação da LGPD. Isso dificultou a elaboração do inventário de dados e do mapeamento do fluxo de dados de cada diretoria e coordenação.

Um trabalho de implementação de um novo sistema ou padrão de procedimentos conta com a colaboração dos envolvidos e a mudança da cultura organizacional de uma instituição ou empresa, e essa foi uma das maiores dificuldades enfrentadas neste trabalho. Devido a resistência das voluntárias e voluntários em compreender a importância da segurança da informação e engajar nos procedimentos necessários para alcançar os objetivos do projeto, houve um atraso na execução de alguns documentos cruciais para a implementação.

Em um contraponto, as diretorias estavam em geral preocupadas em consultar as normas com as coordenadoras de proteção de dados em relação à exposição de dados pessoais e sensíveis dos titulares de dados. Apesar da resistência, pode ser observado que em relação às medidas mais necessárias em função de mitigar o vazamento de dados, as voluntárias e

voluntários estavam preocupados em seguir as regras com mais afinco. Neste caso, o comportamento do usuário em relação às medidas protetivas foi uma dificuldade driblada aos poucos com treinamentos e conscientização em relação a ação da engenharia social, a exposição de dados pessoais e as normas previstas na LGPD.

Portanto, ao realizar este estudo foi possível considerar o quanto a biblioteconomia tem uma larga área de estudo em relação a gestão de segurança da informação e de dados. Como os conhecimentos da tecnologia da informação, do direito e da ciência da informação podem ser amplamente discutidos e interligados. Logo, o conhecimento adquirido na ciência da informação sobre a importância do dado, da informação e dos padrões de organização, recuperação, armazenamento, gestão, redes de dados e segurança foram de suma importância para o desenvolvimento do projeto.

Durante a realização deste trabalho, não foi possível mensurar com profundidade como o comportamento do usuário pode afetar de forma positiva ou negativa a ação da engenharia social e como a LGPD pode atuar diretamente no comportamento do usuário, não apenas na área legal administrativa. Em continuidade a esta pesquisa sugere-se o tema citado anteriormente para trabalhos futuros a fim de enriquecer a compreensão das considerações finais deste trabalho.

REFERÊNCIAS

ARAMUNI, João Paulo C.; MAIA, Luiz Cláudio. O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. **AtoZ: novas práticas em informação e conhecimento**, [S.l.], v. 7, n. 1, p. 31-37, jan. 2020. ISSN 2237-826X. Disponível em: https://revistas.ufpr.br/atoz/article/view/64640. Acesso em: 03 jan. 2023. DOI: http://dx.doi.org/10.5380/atoz.v7i2.64640.

ARAÚJO, Carlos A. A. **O que é Ciência da Informação**. Belo Horizonte: KMA, 2018. 126 p. ISBN 978-85-92728-06-9.

BARRETO, Jeanine dos Santos; ZANIN, Aline; MORAIS, Izabelly Soares; VETTORAZZO, Adriana. **Fundamentos de Segurança da Informação**. Editora Grupo A, 2018.

BARRETO JUNIOR, Irineu; CÉSAR, Daniel. Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos. **Revista Eletrônica Do Curso De Direito Da UFSM**, vol. 12, n. 1, p. 65-88, 2017. DOI: 10.5902/1981369423288.

BRASIL. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 dez. 2022.

_____. Controladoria-Geral da União. **Serviço de Informações ao Cidadão da Controladoria-Geral da União (SIC/CGU)**. Brasília: CGU, [2022?]. Disponível em: https://www.portaldatransparencia.gov.br/sobre/o-que-e-e-como-funciona Acesso em: 20 dez. 2022.

_____. **Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal**. 2012. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-10IN01DSICGSIPR.pdf . Acesso em: 08 dez. 2022.

_____. **Lei nº 12527, de 18 de novembro de 2011**. Institui a Lei de Acesso à Informação. Brasília, DF: Presidência da República, [2011?]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 dez. 2022.

_____. **Lei nº 12737, de 30 de novembro de 2012**. Institui a lei sobre tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, [2012?]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 dez. 2022.

_____. **Lei nº 12965, de 23 de abril de 2014**. Institui a Lei do Marco Civil da Internet. Brasília, DF: Presidência da República, [2014?]. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 dez. 2022.

_____. **Lei nº 13709, de 14 de agosto de 2018**. Institui a Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, [2018?]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2022.

_____. Ministério do Desenvolvimento e Assistência Social, Família e combate à fome. **Lei Geral de Proteção de Dados**. Brasília, [2022?]. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em: 16 dez. 2022

_____. Ministério do Desenvolvimento e Assistência Social, Família e combate à fome. **Glossário de Termos Técnicos da LGPD**. Brasília, [2022?]. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/glossario-de-termos-tecnicos-da-lgpd. Acesso em: 16 dez. 2022

_____. Ministério do Desenvolvimento e Assistência Social, Família e combate à fome. **Guia de Boas Práticas da Lei Geral de Proteção de Dados**. Brasília, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 18 dez. 2022

CAMPOS, M. L. de A.; DE SOUZA, R. F.; CAMPOS, M. L. M. Organização de unidades de conhecimento em hiperdocumentos: o modelo conceitual como espaço comunicacional para a realização da autoria. **Ciência da Informação**, Brasília, v. 32, n. 2, maio/ago. 2003. DOI: 10.18225/ci.inf.v32i2.1001. Disponível em: https://revista.ibict.br/ciinf/article/view/1001. Acesso em: 26 dez. 2022.

CAPURRO, Rafael e HJORLAND, Birger. O conceito de informação. **Perspectivas em Ciência da Informação [online]**. 2007, v. 12, n. 1, pp. 148-207. Disponível em: https://doi.org/10.1590/S1413-99362007000100012. Acesso em: 09 nov. 2022**.**

CASTRO E SILVA, Francisco J. A. F. **Classificação taxonómica dos ataques de engenharia social**: caracterização da problemática da segurança de informação em Portugal relativamente à engenharia social. 2013. Dissertação (Mestrado em Segurança dos Sistemas de Informação) - Faculdade de Engenharia, Universidade Católica Portuguesa, Lisboa, 2013. Disponível em: http://hdl.handle.net/10400.14/15690. Acesso em: 16 jan. 2023.

CONCEIÇÃO, J. P. A arte da fraude no campo da informação: engenharia social, big data e a manipulação do usuário na rede. **Bibliotecas Universitárias**: pesquisas, experiências e perspectivas, v. 4, n. 1, 2017. Disponível em: http://hdl.handle.net/20.500.11959/brapci/17089. Acesso em: 02 jan. 2023.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Disponível em: https://blogdageografia.com/wp-content/uploads/2021/01/apostila_-_metodologia_da_pesquisa1.pdf. Acesso em: 03 dez. 2022.

GALT VESTIBULARES. **Plano de providências de adequação à Lei Geral de Proteção de Dados**. Brasília: [s.n.], 2021.

_____. **Políticas de Privacidade**. Brasília: [s.n.], 2022.

_____. **Política de Segurança da Informação**. Brasília: [s.n.], 2021.

_____. **Quem somos?**. Brasília, 2022. Disponível em: https://www.galtvestibulares.com.br/quemsomos**.** Acesso em: 06 dez. 2022.

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

GOMES, H. E.; MOTTA, D. F.; CAMPOS, M. L. A. **Revisitando Ranganathan**: A Classificação na Rede. 2006. Disponível em: http://www.conexaorio.com/biti/revisitando/revisitando.htm#categorias . Acesso em: 04 dez. 2022.

GOUVEIA, Luis**. Gestão da Segurança da Informação.** Disponível em: https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 14 dez. 2022.

INTEGRITY. **ISO 27001**. 2023. Disponível em: https://www.27001.pt/iso27001_3.html. Acesso em: 10 jan. 2023.

ISO, International Standards Organization. **ISO/IEC 27001:2022**. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 3. ed. 2022. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en. Acesso em: 10 dez. 2022.

ISO, International Standards Organization. **ISO/IEC 27000:2018**. Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2018. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Acesso em: 23 fev. 2023.

MAIA, R. M. C. S.; ALVARENGA, L. Teoria da classificação facetada e contribuições para o modelo entidade relacionamento. **Prisma.com**, Portugal, n. 25, p. 91-125, 2014. Disponível em: http://hdl.handle.net/20.500.11959/brapci/69895. Acesso em: 10 dez. 2022.

MARTINS, Wilson. **A palavra escrita**: história do livro, da imprensa e da biblioteca. 3. ed. São Paulo: Ática, 2002.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação**: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

PEIXOTO, Mário C. P. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Editora Brasport, 2006.

PONTIERI, Alexandre. Marco civil da internet: Neutralidade de rede e liberdade de expressão. **Revista jurídica luso-brasileira**, Lisboa, v. 5, n. 1, p. 79-98. 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0079_0098.pdf. Acesso em: 14 dez. 2022.

ROBREDO, Jaime. **Da Ciência da Informação Revisitada aos Sistemas Humanos de Informação**. Brasília: Thesaurus, 2003. 245 p.

SALOMÃO, Mariana. **Marco Civil da Internet: Perspectivas de Aplicação e seus Desafios.** 2016. 19 f. Artigo Científico (Curso de Pós-Graduação *Lato Sensu*) - Escola da Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

SANTANA, F. J. Clarinda de. **A segurança da informação na ciência da informação no Brasil**. 2021. Tese (Doutorado em Ciência da Informação) - Instituto de Ciência da Informação, Universidade Federal da Bahia, Bahia, 2021. Disponível em: https://repositorio.ufba.br/handle/ri/34280. Acesso em: 15 dez. 2022.

SERRA, João Paulo. **Manual de Teoria da Comunicação.** Covilhã: Livros Labcom. 2007. Disponível em: http://www.labcom-ifp.ubi.pt/ficheiros/serra-paulo-manual-teoria-comunicacao.pdf. Acesso em 05 dez. 2022.

SOUZA, Clarice Muhlethaler de. **Biblioteca**: uma trajetória. In: III CONGRESSO INTERNACIONAL DE BIBLIOTECONOMIA, Rio de Janeiro, 2005.

SOUZA, R. C. de; FERNANDES, J. H. C. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Science: research trends**, [S. l.], v. 10, n. 1, 2016. DOI: 10.36311/1981-1640. Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/view/5088. Acesso em: 05 jan. 2023.

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE. ***California Consumer Privacy Act (CCPA)***. 2023. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 04 jan. 2023.

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE. ***The California Consumer Privacy Act of 2018***. 2018. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 04 jan. 2023.

TAYLOR, Arlene G. **The organization of information**. Englewood: Libraries Unlimited, 1999. ISBN 1-56308-498-8.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Luxemburgo, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31995L0046. Acesso em: 28 dez. 2022.

_____. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva

95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 28 dez. 2022

APÊNDICE A - MANUAL DE BOAS PRÁTICAS

MANUAL DE BOAS PRÁTICAS

1. Não baixar os arquivos da nuvem no seu computador pessoal;
2. Não clicar em links estranhos;
3. Não conectar em Wi-fi público ou desconhecido;
4. Não compartilhar arquivos com pessoas desconhecidas;
5. Ler políticas de privacidade/ termos de consentimento de sites e aplicativos;
6. Fazer backup das informações/dados;
7. Uso de antivírus;
8. O colaborador deve possuir uma senha e utilizador pessoal e intransmissível como forma de autenticação no seu computador;
9. Bloqueio de computador: Sempre que o colaborador se afastar do PC deverá bloqueá-lo;
10. Segurança dos dados: Sempre que alguém que não deve ter acesso aos dados se aproximar do ambiente de trabalho, o colaborador deverá minimizar as janelas com dados sensíveis;
11. Armazenamento de informação: Os utilizadores devem guardar a informação e os documentos gerados e transferidos no servidor (local de armazenamento definido) da empresa ou pasta com password;
12. Manter confidencialidade;
13. Não escrever em papéis ou locais visíveis;
14. Modificar regularmente a senha;
15. Não gravar de forma automática nos sistemas;
16. Não utilizar as mesmas passwords para os sistemas profissionais e sistemas pessoais;
17. Utilizar senhas seguras mas fáceis de memorizar;
18. Descartar adequadamente os dados que não são mais necessários, como por exemplo: currículos de processos seletivos devem ser triturados, mídias devem ser destruídas e backups devem ser verificados para eliminar completamente uma informação desnecessária, dados físicos devem ser rasgados ou triturados, não reaproveite-os para fazer rascunho;
19. Instalar somente aplicativos de fontes e lojas oficiais;

20. Antes de instalar aplicativos, verifique as telas e o nome do aplicativo, pois muitos falsos aplicativos se assemelham aos oficiais;

21. Limitar quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização;

22. Apagar os aplicativos que você não usa mais;

23. Limitar a divulgação ou fornecimento de dados pessoais na internet, inclusive para redes sociais, ou para empresas parceiras, aos casos estritamente necessários;

24. Ativar a criptografia nos discos e mídias externas, como pendrives;

25. Tenha certeza de sair de suas contas (*logout*) ao usar equipamentos compartilhados;

26. Habilitar, quando disponíveis, notificações de login, para ser mais fácil perceber se outras pessoas estiverem usando suas contas;

27. Seja cuidadoso ao abrir arquivos enviados por terceiros;

28. Ao acessar sites, procure limitar a coleta de dados por cookies. Preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão e limpe frequentemente o histórico de navegação;

APÊNDICE B - DIRETRIZES DE USO DOS DISPOSITIVOS MÓVEIS

DIRETRIZES DE USO DOS DISPOSITIVOS MÓVEIS

Usuário com dispositivos móveis particulares (*BYOD - bring your own device* – traga seu próprio dispositivo): Todo dispositivo móvel *BYOD* que utilizam o banco de dados do GALT deve ter os mesmos padrões de configuração e segurança estabelecidos nesta política;

Medidas de segurança e boas práticas:

A. Evitar o uso de redes públicas;
B. Recomenda-se manter as conexões de comunicação, como bluetooth, desabilitadas e somente habilitar quando for necessário;
C. Ao trafegar com dispositivos móveis, sugere-se que estes sejam devidamente protegidos, guardados em locais seguros ou não expostos, como, por exemplo, na mala do carro;
D. Proteger o dispositivo com senha de acordo com a política de segurança da informação;
E. Atualizar software regularmente;
F. Instalar antivirus e firewall;
G. Realizar cópias de segurança dos dados;
H. Não baixar aplicativos desconhecidos ou que não forneçam níveis adequados de segurança;
I. Não permitir que outras pessoas tenham acesso ao dispositivo;
J. Não compartilhar dados pessoais indevidamente;
K. Atualização automática dos aplicativos do telefone móvel;
L. Não permitir instalação de de aplicativos de fontes desconhecidas;
M. Não permitir o preenchimento automático dos códigos recebidos por SMS a partir das opções de desenvolvedor do Android, ou pelas configurações da conta Google;
N. Ativar o bloqueio instantâneo de tela, no botão liga/desliga;
O. Ative a autenticação de dois fatores para aplicativos ou sites que a suportam;

P. Desative as lojas de aplicativos de terceiros, que podem ser vetores para a propagação de malwares;
Q. Exclua periodicamente os aplicativos que não são usados ou não são mais necessários;
R. Limite as informações de identificação pessoal armazenadas em aplicativos;
S. Defina privilégios mínimos nos aplicativos instalados;
T. Permita que um aplicativo acesse sua localização apenas durante seu uso;
U. Apenas ative Bluetooth, NFC, Wi-Fi, ou GPS quando for necessário;
V. Use apenas carregadores e cabos confiáveis, evitando a utilização de carregadores do tipo USB públicos;
W. Habilite a função de localização de dispositivo perdido; e
X. Verifique a legitimidade de um e-mail antes de abrir um anexo ou clicar em links.

Em caso de desligamento do voluntário que possua dispositivo móvel *BYOD* incorporado ao banco de dados do GALT, coordenador ou diretor deve comunicar à Coordenação de Compliance e Proteção de Dados, que solicitará que toda informação do GALT no dispositivo seja salva em ativos físicos corporativos e removida do referido dispositivo.

Para mais informações entre em contato com a coordenação compliance@galtvestibulares.com

APÊNDICE C - CHECKLIST *DUE DILIGENCE*

CHECKLIST *DUE DILIGENCE*

1. Identificação do Parceiro de Negócio/ Fornecedor/ Prestador de Serviços:
Razão Social:
Nome Fantasia:
CNPJ/MF:
Endereço:
Principais contatos:
E-mails:
Site: Telefones:
Porte da Empresa: ( ) Microempresa ( ) Pequena Empresa ( ) Média Empresa ( ) Grande Empresa ( ) Administração Pública
Número de Empregados:

Introdução:

Descreva sobre a história da empresa, o que faz, como trabalha, cultura da organização, como foi fundada, missão visão e valores da empresa:
Ética:

1.1 A Empresa tem seus registros contábeis submetidos à auditoria independente? ( )
Sim ( ) Não

1.2 A empresa possui filiais/sucursais em outras jurisdições, participação em coligadas, controladas ou consorciadas?
( ) Sim ( ) Não. Se sim, quais? (caso o espaço não seja suficiente, anexar lista).

Nome	**CNPJ**	**Endereço/Contato**

2 Pessoa Exposta Politicamente (PEP) e Conflito de Interesses:

2.1 A empresa participa de licitações públicas? ( ) Sim ( ) Não

2.2 Algum proprietário, sócio, acionista majoritário, membro do Conselho de Administração, Diretor e/ou representante da empresa enquadra-se na condição de PEP (Pessoa Exposta Politicamente)? ( ) Sim ( ) Não

2.3 Os sócios da empresa são ou possuem relacionamento* próximo com funcionários públicos, agentes do governo, ex-funcionários públicos e ex-agentes do governo, políticos ou ex-políticos?

**Obs. Por relacionamento próximo, entenda-se: pais e padrastos, filhos e enteados, irmãos, cônjuges e companheiros e pessoas que coabitam na mesma residência. 12 - empresa ou sócios já foram acusados ou condenados por crimes de (i) corrupção, (ii) contra o patrimônio, (iii) contra o sistema financeiro nacional ou qualquer outro crime?*

2.4 A empresa presta serviços a órgãos públicos, partidos políticos ou a candidatos?

2.5 A empresa ou sócios já foram proibidos ou suspensos temporariamente de operar/contratar com o poder público?

2.6 A empresa irá interagir com agentes/funcionários públicos e órgãos do poder público, em nome do Galt Vestibulares?

( ) Sim ( ) Não

3 Programa de Integridade:

3.1. A empresa possui Política Anticorrupção e Código de Ética e Conduta? Se sim, anexar cópia.

3.3. A empresa possui políticas específicas para prevenção e combate à corrupção implementadas? (Política Anticorrupção). ( ) Sim ( ) Não. Em caso afirmativo, favor fornecer uma cópia da política ou documento similar.

3.4. Os funcionários recebem treinamento sobre o código de ética e/ou outros temas relacionados com ética e integridade e legislação anticorrupção? ( ) Sim ( ) Não

3.5. De que forma a empresa possibilita a realização de denúncias de irregularidades por parte de funcionários, intermediários, fornecedores, prestadores de serviço e público externo? ( ) Sim ( ) Não

3.6. A Empresa (Parceiro/ Fornecedor/ Prestador de Serviços), algum dos sócios, conselheiros, dirigentes ou proprietários têm qualquer condenação, ainda que não transitada em julgado, por crimes ou ilicitudes de corrupção, lavagem de dinheiro, improbidade administrativa, relacionados à legislação de combate à lavagem de dinheiro, de defesa da concorrência ou de licitações? ( ) Sim ( ) Não

3.7. A Empresa (Parceiro/ Fornecedor/ Prestador de Serviços), algum dos sócios, conselheiros, dirigentes ou proprietários, nos últimos 5 anos, foi ou está sendo formalmente acusada ou investigada por parte de autoridade governamental competente por qualquer crime, nos termos da Lei nº 12.846/13 (Lei Anticorrupção) ou sob os crimes previstos no Código Penal (capítulos II-Crimes praticados por particular contra a administração pública e II-A-dos crimes praticados por particular contra a administração pública estrangeira) ou ainda nos termos da Lei 12.529/11? ( ) Sim ( ) Não

3.8. A Empresa (Parceiro/ Fornecedor/ Prestador de Serviços), algum dos sócios, conselheiros, dirigentes ou proprietários, nos últimos 5 anos, está sujeita a qualquer mandado

ou sentença de bloqueio, confisco ou perda de direito baseada em qualquer violação alegada de quaisquer leis de corrupção, lavagem de dinheiro ou de terrorismo, ou por violar quaisquer leis antilavagem de dinheiro ou antiterrorismo?

4 Proteção de dados:

4.1. A empresa trata dados pessoais de acordo com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) ( ) Sim ( ) Não

4.2 A empresa possui política de privacidade ou política de segurança da informação? Se sim, anexar cópia.

4.3.A empresa aplica medidas de segurança para tratamento de dados pessoais? ( ) Sim ( ) Não

4.4. Os funcionários recebem treinamento a respeito da proteção de dados? ( ) Sim ( ) Não

4.5. A empresa possui um canal adequado de comunicação para exercício dos direitos dos titulares de dados ( ) Sim Informar: _____ ( ) Não

ANEXO A - POLÍTICA DE PRIVACIDADE DO GALT VESTIBULARES

POLÍTICAS DE PRIVACIDADE

Atualizada pela última vez em 20 de julho de 2022

O GALT vestibulares em consonância com a Lei Geral de Proteção de Dados, considera fundamental assegurar a privacidade e a proteção de dados pessoais de seus usuários. Por essa razão, a presente Política de Privacidade tem por objetivo dar transparência às atividades de tratamento de dados pessoais que realizamos.

Esta Política de Privacidade define a maneira como o GALT Vestibulares coleta, usa, mantém e divulga informações dos usuários, candidatos, alunos e membros, titulares dos dados pessoais (denominado os “usuários”) pelos sites, aplicativos e sistemas de informação e de gestão escolar utilizados pela Instituição. Esta política se aplica ao site, redes sociais e a todos os serviços oferecidos pelo GALT Vestibulares.

Coleta dos dados

Nós podemos coletar dados pessoais tanto virtualmente quanto fisicamente. Os dados pessoais podem ser coletados:

- Quando você preenche um formulário;
- Quando você realiza seu cadastro conosco;
- Quando você acessa ou interage em nossas redes sociais;
- Quando você posta uma mensagem nos fóruns, nos grupos, no nosso sistema de mensagens ou entra em contato conosco;
- Quando você faz sua matrícula para nosso cursinho;
- Quando você assiste às aulas, faz as atividades e avaliações do curso;

Quais dados pessoais coletamos e tratamos

- Dados cadastrais: nome completo, nome social, CPF, RG, CNH, data de nascimento, endereço e/ou, telefone, e-mail, nacionalidade, naturalidade, gênero, formação;

- Dados familiares: nome, telefone, e-mail do responsável legal, nome, CPF;

- Dados sensíveis: origem racial, étnica e imagem, características físicas (tatuagens, peso, altura), preferências de atividade de lazer, fotos;
- Dados de navegação: acesso, endereço IP, provedor de internet, sistema, operacional utilizado, geolocalização;
- Dados socioeconômicos: renda das pessoas que residem com o candidato, ocupação do mantenedor, situação de trabalho, situação de renda per capita, situação de moradia;
- Os dados podem ser coletados mediante preenchimento de formulários, navegação em websites ou plataformas digitais.

Como utilizamos seus dados (finalidade)

Relação comercial: participação em processo seletivo para ingresso no cursinho, emissão de declarações acadêmicas, atendimento das solicitações dos alunos, controle de vínculo.
Marketing direto: para manter nossos alunos e usuários atualizados sobre as melhorias propostas, utilizamos dados pessoais para o envio de materiais publicitários e divulgações em redes sociais.
Obrigações Legais e Regulatórias: seus dados pessoais também poderão ser utilizados para o atendimento de obrigações dispostas em lei, regulamentações de órgãos governamentais, autoridades fiscais, Poder Judiciário e/ou qualquer outra autoridade competente. Este tratamento poderá incluir seus dados de identificação e documentos pessoais. Seus dados pessoais ainda poderão ser utilizados para resguardo dos nossos direitos e atuações em processos judiciais, administrativos e arbitrais.
Melhorar nossos serviços: usando as críticas, sugestões e opiniões dos membros e alunos, para melhorar e aprimorar o curso; entendendo como utilizam para trazer informações e conteúdos cada vez mais relevantes.
Contato, ajuda e suporte: seus dados também poderão ser utilizados para notificação, para respostas às mensagens e contato, assim como, para prestar suporte e fornecer ajuda técnica relacionada às aulas e/ou eventos, sempre que necessário.
Segurança: os dados também poderão ser utilizados nos procedimentos para implementação e manutenção das medidas de segurança, inclusive para evitar instabilidades; investigar e

prevenir práticas fraudulentas, evitar acessos não autorizados e outras atividades ilegais dentro da instituição.

Armazenamento internacional e compartilhamento de dados pessoais

Segunda a legislação vigente, os dados pessoais podem vir a ser armazenados em bancos de dados de terceiros, inclusive no exterior, desde que respeitem a privacidade e a proteção de dados dos usuários em nível condizente com aquele oferecido pela legislação brasileira e por esta Política de Privacidade, além de apresentarem condições adequadas de segurança no armazenamento e processamento desses dados.

Nós armazenamos os dados pessoais em cloud (nuvem) da plataforma internacional com a segurança adequada, utilizada somente para este fim específico nos termos do art. 33, inciso I da Lei Geral de Proteção de Dados, pelo período necessário para cumprir as finalidades informadas, para cumprir nossas obrigações legais, regulatórias ou para preservação de direitos. Terminado o prazo de armazenamento, os dados pessoais serão anonimizados ou excluídos, utilizando método seguro de descarte.

O GALT possui empresas parceiras ou apoiadoras, para o desenvolvimento de atividades e serviços educacionais ou comerciais, com quem poderá compartilhar as informações coletadas automaticamente ou deliberadamente fornecidas por você. O GALT Vestibulares não vende ou aluga as informações pessoais coletadas, sob nenhuma hipótese.

Além disso, nós poderemos compartilhar os dados pessoais nas circunstâncias abaixo, mediante processos seguros e respeitando ao máximo a confidencialidade e privacidade:

- Com as áreas internas do GALT;
- Com prestadores de serviço, empresas e instituições de ensino parceiras, para facilitar, fornecer ou executar atividades relacionadas aos nossos serviços;
- Com autoridades públicas, sempre que houver determinação legal, requerimento, requisição ou ordem judicial/administrativa nesse sentido;
- Para cumprir os termos de uso do site e redes sociais, inclusive para apuração de violações;
- Para proteger os direitos dos usuários, do GALT ou do público em geral, nos termos da legislação aplicável;

Não compartilharemos os dados pessoais para qualquer finalidade que esteja em desacordo com a legislação vigente ou com esta Política de Privacidade.

Direitos dos titulares

Conforme elencado no art. 18 da Lei Geral de Proteção de Dados, o titular de dados pessoais possui os seguintes direitos relativos às suas informações pessoais:

1. Saber se a Instituição realiza algum tratamento com seus dados pessoais e quais dados são tratados;
2. Corrigir ou solicitar a correção de dados incompletos, inexatos ou desatualizados;
3. Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação;
4. Solicitar a portabilidade dos dados a outro fornecedor de produtos ou serviços similares;
5. Solicitar a eliminação dos dados coletados e utilizados com base no consentimento do titular de dados;
6. Obter informações completas sobre as entidades públicas ou privadas com as quais compartilhamos os seus dados;
7. Quando a atividade de tratamento necessitar de consentimento, o titular dos dados pessoais pode se negar a consentir. Nesse caso, lhe informaremos sobre as consequências da negativa do titular dos dados pessoais consentimento;
8. Quando a atividade de tratamento necessitar do consentimento do titular dos dados pessoais, a qualquer momento você poderá revogá-lo.

Uso de cookies

Os cookies são pequenos arquivos de texto que um site, quando visitado, armazena no computador do usuário ou no seu dispositivo móvel, por meio do navegador de internet (browser). A colocação de cookies ajudará o site a reconhecer o seu dispositivo numa próxima visita, lembrando quem você é e quais seus hábitos de navegação, além de acessar as informações do seu cadastro em nosso website para facilitar e agilizar o preenchimento de formulários.

Caso você não deseje receber cookies ou queira ajustar o seu navegador para alertá-lo cada vez que um cookie estiver sendo enviado, ou ainda se você desejar desativar todos os cookies, use as opções existentes em seu navegador para assisti-lo. A opção “Ajuda” em seu navegador poderá orientá-lo sobre como modificar suas preferências com relação à coleta de cookies. Tenha em mente, contudo, que, ao desativar os cookies, você não terá acesso a muitos dos itens disponíveis em nosso Website

Segurança dos dados

Os dados pessoais que nos transmitir serão mantidos pelo GALT em registro informatizado, que está devidamente salvaguardado no que respeita a acessos e suportado em plataformas de empresas líderes de mercado do setor de tecnologia de informação. Aos seus dados pessoais, apenas terão acesso a membros nossos devidamente autorizados a processá-los.

Término de tratamento e exclusão dos dados

O GALT Vestibulares garante que retém dados pessoais apenas pelo tempo necessário para responder às solicitações do Titular dos dados, para cumprir com obrigações legais ou judiciais, ou contratuais, para resolver eventuais disputas, para evitar fraudes e abusos e para proteger os legítimos interesses do GALT. Quando extintas estas obrigações ou interesses legítimos, o GALT eliminará os seus dados pessoais num prazo máximo de 12 meses.

Determinadas informações são necessárias para prestar os serviços, assim só podemos deletar essas informações após excluirmos o seu cadastro. Ao excluir seu cadastro da Instituição, ele será apagado permanentemente do GALT dentro de um prazo de 30 (trinta) dias a partir da solicitação, ressalvadas as hipóteses de guarda obrigatória de registros previstas em lei ou regulamento.

O titular pode solicitar a exclusão de sua conta através do e-mail: **segurancadainformacao@galtvestibulares.com.br.**

Condições Gerais

Ao utilizar nosso site, redes sociais, assim como ao se cadastrar para ser membro ou aluno do GALT, você está sujeito às regras de coleta, armazenamento e uso detalhadamente descritas nesta Política de Privacidade.

A fim de proporcionar maior segurança e transparência, o GALT reserva-se o direito de alterar esta Política de Privacidade, o que será informado aos usuários por meios razoáveis, inclusive através de publicação em nosso site e redes sociais da política alterada.

A Política de Privacidade do GALT se aplica unicamente às informações coletadas pela Instituição.

Caso algum ponto desta Política seja considerado inaplicável pela Autoridade Nacional de Proteção de Dados ou por alguma autoridade judicial, as demais condições permanecerão em pleno vigor.

Esta Política será interpretada segundo a legislação brasileira, no idioma português, sendo eleito o foro da Circunscrição de Brasília - DF, para resolver qualquer controvérsia que envolva este documento, salvo ressalva específica de competência pessoal, territorial ou funcional pela legislação aplicável.

Contato

Quaisquer questões, reclamações, comentários ou pedidos relacionados com este Aviso de Privacidade, ou com seus direitos, deverão ser enviados por e-mail para o nosso e-mail de contato **segurancadainformacao@galtvestibulares.com.br.**

ANEXO B - PLANO DE PROVIDÊNCIAS DE ADEQUAÇÃO A LEI GERAL DE PROTEÇÃO DE DADOS

Plano de providências de adequação à Lei Geral de Proteção de Dados: coordenadoria de Segurança da Informação do GALT Vestibulares

Treinamento e Conscientização

- Ampliação da realização de ações de conscientização e treinamento a toda a organização, sobre a LGPD e práticas de operação relativas ao tratamento de dados;
- Preparação de um plano de formação contínua, particularmente focado nos intervenientes direitos à privacidade e proteção de dados;
- Elaboração de comunicações, dinâmicas e cartazes de sensibilização;
- Abordagem regular e sistemática do tema “LGPD/ Proteção de dados” (internamente e com parceiros de negócio).

Estrutura de Governança

- Elaboração de um *framework* e de um repositório de evidências que permita demonstrar conformidade com cada um dos artigos da LGPD;
- Preparação de um plano de comunicação para o projeto e para o pós projeto;
- Definição de documento que evidencie o processo de Gestão de Mudanças (inclui operações, serviços e de que modo a proteção de dados e segurança da informação é considerada);
- Elaboração de um documento de boas práticas.

Inventário de dados pessoais, fluxos e acessos

- Preparação de um inventário de dados pessoais de todas as operações de tratamento de dados pessoais e suas respectivas avaliações, sob a ótica dos princípios da LGPD, desde a sua coleta até a sua exclusão, com indicação de base legal, finalidades, tempo de retenção e as práticas de segurança;

- Definição de prazos de conservação de dados, com vista a eliminar periodicamente a informação que não é necessária;
- Elaboração de comunicações, dinâmicas e cartazes de sensibilização;
- Abordagem regular e sistemática do tema "LGPD/ Proteção de dados" (internamente e com parceiros de negócio).
- Implementação de processos de eliminação de dados.

Privacidade de Dados e Segurança da Informação

- Estabelecimento de mecanismos de obtenção de consentimentos válidos por parte dos titulares de dados, quando aplicáveis;
- Aplicação e documentação de medidas organizacionais e técnicas de segurança em processos de contato com titulares;
- Revisão de contratos e termos para inclusão de cláusulas relativas à Lei Geral de Proteção de Dados.

Políticas e avisos de privacidade

- Definição e publicação de avisos de utilização de cookies válidos;
- Criação de avisos de privacidade e devida comunicação com os titulares de dados;
- Definição e comunicação interna de uma Política de Privacidade e Proteção de Dados, onde constem os mecanismos de segurança adotados.

Contato com titulares

- Definição de procedimentos de resposta a titulares dos dados de acordo com o escopo da LGPD;
- Implementação de mecanismos para registro, rastreamento, resposta e controlo dos pedidos de resposta aos titulares de dados;
- Adoção de canal para resposta aos titulares de dados (email).

Gestão de incidentes

- Definição de plano de gerenciamento de incidentes para ser seguido em caso de violação de dados pessoais, de forma a estabelecer os procedimentos necessários com base na criticidade identificada em cada situação;
- Definição de templates de resposta a aplicar na notificação de vazamento de dados pessoais (aos titulares de dados e a Autoridade Nacional de Proteção de Dados - ANPD);
- Realização de avaliações periódicas da ocorrência de incidentes, com relação à sua gravidade, adoção de ações corretivas, entre outros aspectos (ex.: documento de comprovação de registro de eventos e incidentes).

A ideia inicial é iniciar o agendamento de capacitações em primeiro para os integrantes da DIREX. Em simultâneo, iniciar as entrevistas com os gestores para preencher o inventário e mapeamento de dados, assim possibilitando investigar o grau de risco das operações de dados e definindo a prioridade de outras ações de adequação.

Sigo à disposição,

Mariana Cavalcante
Coordenadora de Segurança da Informação

ANEXO C - TERMO DE CESSÃO DE DIREITOS AUTORAIS

TERMO DE CESSÃO DE DIREITOS AUTORAIS

CEDENTE: (COLOCAR NOME COMPLETO DO MEMBRO CEDENTE)

CESSIONÁRIA: GALT Vestibulares

OBJETO: Cessão de Direitos Autorais sobre a OBRA (DISCIPLINA)

Pelo presente instrumento particular NOME COMPLETO DO CEDENTE de nacionalidade COLOCAR A NACIONALIDADE, inscrito no CPF sob o nº. COLOCAR NÚMERO, residente e domiciliado COLOCAR ENDEREÇO, doravante denominado (s) CEDENTE (s) e o GALT VESTIBULARES, pessoa jurídica de direito privado, inscrita no CNPJ sob n° 21.840.133/0001-46 com sede no SGAS I St. de Grandes Áreas Sul 907 - Asa Sul, Brasília - DF, doravante designada CESSIONÁRIA, contratam, sob a regência da Lei nº. 9.610/1998, de 19 de fevereiro de 1998, por esta e na melhor forma de direito, a CESSÃO GRATUITA DE DIREITOS AUTORAIS sobre obra produzida na Instituição Cessionária mediante as cláusulas e condições adiante estipuladas que, voluntariamente, aceitam e outorgam:

CLÁUSULA PRIMEIRA - Da Caracterização do objeto da Cessão

1.1. Será designada “OBRA”, no âmbito do presente contrato, o (LIVRO/MATERIAL PEDAGÓGICO/VIDEOAULA/AMBIENTE VIRTUAL) da disciplina COLOCAR NOME DA DISCIPLINA do Curso COLOCAR NOME DO CURSO de titularidade do (s) CEDENTE (S), produzida com o apoio e dentro da Instituição CESSIONÁRIA

CLÁUSULA SEGUNDA – Do objeto da Cessão

2.1. O (s) CEDENTE (S), titular (es) dos direitos autorais sobre a OBRA, cede (m) e transfere (m) à CESSIONÁRIA, os direitos autorais patrimoniais referentes à OBRA em questão, nos termos da Lei nº. 9.610/1998, de 19 de fevereiro de 1998.

2.2. O (s) CEDENTE (S) transfere (m) à CESSIONÁRIA, para todos os fins e efeitos e na melhor forma de direito, em caráter gratuito, parcial, irrevogável, irretratável e não exclusivo, os direitos autorais relativos à OBRA.

2.3. Reservam-se ao (s) CEDENTE (S) os direitos de utilização da OBRA, sob qualquer forma, inclusive, a exploração comercial, mesmo na vigência da presente cessão, cujo objeto deverá, em qualquer hipótese, ser preservado.

2.4. A cessão objeto deste termo abrange o direito de a CESSIONÁRIA usar a OBRA, como lhe aprouver sob qualquer modalidade prevista em Lei, inclusive reprodução, divulgação, produção de mídia ou qualquer outro meio.

2.5. Da mesma forma, fica a CESSIONÁRIA autorizada a promover quantas edições, totais ou parciais, se fizerem necessárias e em qualquer número de exemplares, bem como a sua distribuição, inclusive no que se refere à circulação nacional ou estrangeira, ao meio ou material utilizado no armazenamento ou veiculação da OBRA.

2.6. O material cedido ficará disponível nos sítios institucionais do GALT VESTIBULARES (incluindo na plataforma ADICIONAR PLATAFORMA DE ARMAZENAMENTO), para quando material audiovisual.

2.7. Os materiais estarão sob licença Creative Commons 4.0.

CLÁUSULA TERCEIRA – Da Remuneração

3.1. O (s) CEDENTE (S) declara (m) ter cedido a OBRA para a CESSIONÁRIA a título gratuito, sem que disso seja devida ao (s) CEDENTE (S) qualquer remuneração, reembolso ou compensação de qualquer natureza.

CLÁUSULA QUARTA – Das Obrigações

4.1. CEDENTE (S) e CESSIONÁRIO se comprometem com as cláusulas e obrigações constantes deste instrumento particular de contrato de cessão de direitos autorais.

CLÁUSULA QUINTA – Da Titularidade

5.1. O (s) CEDENTE (S) declara (m) ser o (s) titular (es) e detentor (es) dos direitos autorais referentes à OBRA, cedendo, neste ato, a CESSIONÁRIA, em caráter gratuito, parcial, irrevogável, irretratável e não exclusivo, os direitos autorais patrimoniais que sobre ela recaem.

Assume (m), portanto, o (s) CEDENTE (S) a responsabilidade de manter a CESSIONÁRIA imune aos efeitos de qualquer eventual reivindicação fundada na autoria da OBRA.

CLÁUSULA SEXTA – Da Responsabilidade

6.1. O (s) CEDENTE (S) assume (m) ampla e total responsabilidade civil e penal, quanto ao conteúdo, citações, referências e outros elementos que fazem parte da OBRA.

6.2. Responsabiliza (m) -se o (s) CEDENTE (S) por eventuais questionamentos judiciais ou extrajudiciais em decorrência de sua divulgação, declarando que o conteúdo da obra cedida é de sua exclusiva autoria.

CLÁUSULA SÉTIMA – Do Registro

7.1. É facultado a CESSIONÁRIA promover o registro da OBRA previsto no artigo 19 da Lei nº. 9.610/1998, não estando a OBRA registrada, bem como o registro em Cartório de Títulos e Documentos ou, ainda, junto a outros órgãos especializados.

7.2. A CESSIONÁRIA poderá, ainda, averbar a presente CESSÃO à margem do registro a que se refere o artigo 19 da Lei nº. 9.610/1998, ou não estando a obra registrada, poderá o instrumento de cessão ser registrado em Cartório de Títulos e Documentos.

E por estarem assim justos e de acordo, firmam este Termo, CEDENTE (S) e CESSIONÁRIA, em 2 (duas) vias de igual teor e forma, na presença das testemunhas abaixo nomeadas e indicadas, para que surta seus jurídicos e legais efeitos.

_____, ____ de _____ de 20___.

Local e Data

_____

ASSINATURA (S)

CEDENTE (S)

_____

GALT Vestibulares

CESSIONÁRIA

TESTEMUNHAS:

1) _____

Nome:

CPF:

2) _____

Nome:

CPF: