UNIVERSIDADE DO SUL DE SANTA CATARINA
EDSON VICENTE SIVIERI

ESTRUTURAÇÃO DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO PARA ATENDER A GESTÃO DE DADOS EM CONFORMIDADE À LEI GERAL DE PRIVACIDADE DE DADOS (LGPD)

São Paulo
2021

AGRADECIMENTOS

Agradeço primeiramente a Deus onipotente e a Maria Santíssima, que me carregam, todos os dias, em seus braços carinhosos e providentes.

Agradeço a minha esposa, Marcia, por tamanha paciência comigo nestes tempos tão difíceis. Atravessamos juntos dificuldades, Pandemias e responsabilidades e ela, com sua dedicação e simplicidade, me trouxe até aqui.

Agradeço ao meu grupo de Canto Gregoriano, especial ao meu mestre Luiz França, por me permitir usar o tempo dos ensaios para concluir este importante passo de minha vida.

Agradeço a minha mãe, por nunca desistir de querer bem seus filhos: de em sua humildade, implorar para que estudemos.

“Senhor, dá-me forças para executar aquilo que ordenas. Depois ordena o que quiseres”.
(Santo Agostinho)

“Bendito seja o Senhor, meu rochedo, que adestra minhas mãos para o combate, meus dedos para a guerra; meu benfeitor e meu refúgio, minha cidadela e meu libertador, meu escudo e meu asilo, que submete a mim os povos." (Salmos, 143)

LISTA DE FIGURAS

SUMÁRIO

1 RESUMO

Manter a privacidade dos dados pessoais vem se tornando cada vez mais um grande desafio para os gestores de Departamentos de Segurança da Informação de empresas de diversos tamanhos e nichos de negócio.

Não limitada ao tamanho da empresa ou a sua natureza, a responsabilidade sobre a gestão (ou utilização) de dados e informações dos colaboradores, clientes fornecedores e instituições de regulação (Poder Público), havia tempos que estava sob análise das autoridades governamentais, em especial, as brasileiras. Para isto, aqui mencionamos as principais ações do governo brasileiro com foco na contenção dos riscos em de Segurança da Informação e da Privacidade dos dados dos cidadãos naturais como o Marco Civil da Internet[1], a Política Cibernética de Defesa[2] e a implantação dos Normativos e Frameworks de Proteção de Dados Pessoais[3].

Este projeto tem como objetivo principal se tornar uma fonte de referência para o gestor do departamento de segurança da Informação, determinar mudanças necessárias para preparar a área para suportar de maneira eficaz e eficiente, o DPO (*Data Privacy Officer*) de empresas em sua missão de zeladoria pela privacidade dos dados.

A metodologia adotada para este Projeto foi a de pesquisa exploratória, com coleta de dados por meio de pesquisa bibliográfica não somente focada na literatura disponível. A pesquisa bibliográfica foi focada nas publicações da ABNT (Associação Brasileira de Normas Técnicas), em respeito aos Segmentos de Segurança da Informação e Privacidade da Informação, assim como em literatura técnica utilizada por profissionais da área de Segurança da Informação e de Riscos/*Compliance*.

---

[1] MARCO CIVIL DA INTERNET. *Disponível em*: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 07/10/2021.

[2] ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA. *Disponível em:* http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm#:~:text=A%20presente%20Estrat%C3%A9gia%20Nacional%20de,validade%20no%20quadri%C3%AAnio%202020%2D2023. Acesso em 06/10/2021.

[3] NORMATIVOS E FRAMEWORKS DE PROTEÇÃO DE DADOS PESSOAIS. *Disponível em* : https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/normativos-e-frameworks-de-protecao-de-dados-pessoais. Acesso em 06/10/2021.

1.1 RESULTADO

O Resultado da pesquisa nos apresenta que a preparação do Departamento de Segurança da Informação para suportar a nova realidade imposta pela Lei Geral de Privacidade de Dados (LGPD), é chave de sucesso para que a empresa, representada pelas áreas de *Compliance*, Tecnologia ou Governança Corporativa, possa responder prontamente e com qualidade às demandas de controle impostas pela autoridade (ANPD – Agência Nacional de Privacidade de Dados) de forma a mitigar riscos de perda financeira e de sanções mais graves pela autoridade.

Para atingir este objetivo, a pesquisa evidencia, através de informações coletadas em diversas fontes que é necessária a adoção de metodologia e ferramental capazes de fornecer informações precisas sobre o ciclo de vida dos dados.

No segmento de Metodologia, o trabalho recomenda a adoção das normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e a ABNT NBR ISO/IEC 27701:2019, todas como fontes de balizamento para a implantação de Governança Corporativa em Segurança da Informação.

A primeira define os requisitos a serem atendidos pelo Programa de Segurança da Informação estabelecido pela entidade para que possa obter certificação por meio de auditoria. A segunda é desenhada para ser um guia (ou código) de boas práticas para a gestão da Segurança da Informação. A terceira, complementa as Normas Técnicas anteriores, estabelecendo requisitos e diretrizes para um Programa de Governança relacionado à Privacidade.

Como suporte a gestão, recomendamos a adoção de ferramental costumeiramente utilizado em países onde a Privacidade dos dados já é tratada com a criticidade que lhe é devida. Para tal, aqui recomendamos a adoção de ferramentas do NIST (*National Institute of Standards and Technology*): como o NIST *Framework for improving Critical Infrastructure Cybersecurity*[4], e o NIST *Privacy Framework: A tool for improving Privacy through Enterprise Risk Management*[5].

A partir dos resultados obtidos pela pesquisa, é possível chegar à conclusão de que, para que as empresas consigam sobreviver ao desafio imposto pelas autoridades e pelo

---

[4] Disponível em https://www.nist.gov/cyberframework/framework. Acessado em 09/10/2021

[5] Disponível em https://www.nist.gov/privacy-framework/privacy-framework. Acessado em 09/10/2021

ecossistema de negócio (Mercado, concorrência) no qual elas estão inseridas, é mandatório ter aplicada governança de forma eficaz e eficiente quanto a privacidade de seus dados e, para tal, o Departamento de Segurança de Informação (DSI) assume protagonismo decisivo para que esta governança seja suportada e confiável.

Pela pesquisa é possível enxergar de forma conclusiva que o suporte do Departamento de segurança da Informação (DSI) é fundamental para a construção e adoção de Políticas, metodologia e de seleção de ferramental, com o objetivo de se garantir o sucesso da gestão da Privacidade dos dados, dada a sua experiência na gestão do Sistema Gestor de Segurança da Informação (SGSI) e sua visão abrangente da dimensão de uso de recursos de gestão dos dados (sistemas operacionais, armazenamento, transmissão).

Palavras-chave: LGPD. Riscos de Informação. DSI. Privacidade de Dados. ABNT.

1.2 ABSTRACT

Keeping the privacy of personal data is becoming more and more a great challenge for managers of Information Security Departments of companies of different sizes and business niches.

Not limited to the size of the company or its nature, the responsibility for the management (or use) of data and information of employees, supplier customers and regulatory institutions (Public Authorities), had been under analysis by government authorities, in particular, the Brazilian authorities. For this, we mention here the main actions of the Brazilian government with a focus on containing the risks in Information Security and Privacy of data of natural citizens, such as the Civil Rights Framework for the Internet, the Cyber Defense Policy and the implementation of Regulations and Frameworks of Protection of Personal Data.

This project's main objective is to become a reference source for the manager of the Information security department, to determine necessary changes to prepare the area to support the DPO (Data Privacy Officer) of companies effectively and efficiently in their mission of taking care for the privacy of data.

The methodology adopted for this Project was exploratory research, with data collection through bibliographical research not only focused on the available literature. The bibliographic research was focused on ABNT (Brazilian Association of Technical Standards) publications, in respect to the Information Security and Information Privacy Segments, as well as on technical literature used by professionals in the Information Security and Risks/Compliance areas.

2 INTRODUÇÃO

A privacidade do ser humano, em especial do cidadão consumidor de produtos e serviços disponíveis no imenso mercado que, hoje, não possui fronteiras, vem sendo objeto de estudo e de grande preocupação.

Cabe, primeiramente, classificar o que significa a palavra "Privacidade". Segundo o Dicionário Escolar da Língua Portuguesa, editado pela Academia Brasileira de Letras, a palavra PRIVACIDADE significa: "*Condição de privado, do que diz respeito unicamente ao indivíduo*[6]. Da Universidade de Coimbra, em texto publicado em seu sítio na Internet intitulado: "Da Privacidade à Proteção de Dados"[7], obtemos o seguinte, sobre o conceito de Privacidade**:**

> "Na verdade a ideia de privacidade tem a sua origem no reconhecimento de uma manifestação de interesse individual de "ser deixado só", que remonta a 1834, nos Estados Unidos, e que mais tarde, em 1890, com a publicação do artigo de Samuel D. Warren e Louis D. Brandeis intitulado *The right to Privacy*, na *Harvard Law Review*, é difundida e posta em prática, enquanto direito à privacidade (um direito à "não-intrusão", ou seja, o direito a não ser perturbado ou o direito a ser deixado só – *the right to be let alone*, ou ainda, o direito do indivíduo de estar livre de intrusões públicas não autorizadas), designadamente para os países que adotam o sistema da *common law*. Neste artigo, os autores fundamentavam o direito à **privacidade**, no direito à vida, já enunciado na declaração de independência das treze colónias, a Declaração de Independência dos EUA: "todos os homens são criados iguais, que são dotados pelo Criador de certos direitos inalienáveis, que entre estes são vida, liberdade e busca da felicidade".

Na Declaração dos Direitos Humanos (DUDH), promulgada em 1948, já estava configurado o direito do ser humano à privacidade:

> "Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" [8]

---

[6] PRIVACIDADE. *In*: Dicionário Escolar da Língua Portuguesa, 2ª ed.—São Paulo: Companhia editora Nacional, 2008. Pag 1029

[7] "*Da Privacidade à Proteção de Dados"* – disponível em: https://www.uc.pt/protecao-de-dados/da_privacidade_a_protecao_de_dados, acesso em 08/10/2021

[8] DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS - disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos Acesso em 19/10/2021.

2.1 DEFINIÇÃO DO PROBLEMA

Não é raro lermos ou ouvirmos em diversos tipos de mídias que um enorme volume de dados (pessoais, financeiros) foram indevidamente expostos na rede mundial de computadores devido a uma falha sistêmica ou até humana. Esta preocupação tomou mais importância nos últimos tempos pelo impacto causado pela notícia veiculada nos periódicos *The Guardian* e *The New York Times*[9] quanto ao vazamento de informações de mais de 50 milhões de pessoas ativas na plataforma *Facebook*®, (à época, a maior rede social virtual existente no planeta) para a *Cambridge Analytica* ®, empresa especializada na análise de dados e que fornece consultoria a políticos, empresas, governos e muitos interessados nas informações de costumes que internautas demonstram livremente nas redes sociais. A princípio, como investigado pelo congresso Americano e pela mídia especializada, a *Cambridge Analytica*® haveria comprado o acesso a dados pessoais de usuários da rede social e utilizado esses dados para criar um sistema suficiente capaz de predizer e influenciar as escolhas dos eleitores nas urnas (especialmente na campanha da eleição Americana de seu novo presidente, em 2016) assim como para a aprovação do BREXIT (a saída do reino unido da união europeia), Este vazamento de informações rendeu ao Facebook uma multa de USD 5 bilhões nos EUA[10] e 500 mil libras ao Reino Unido[11]. Já à Cambridge Analytica, sua falência.

Segundo a Revista especializada em grandes fortunas e negócios, a FORBES, 2,3 bilhões de arquivos foram expostos na Internet em 2018[12], dentre eles dados de cartões de crédito, informações de pacientes (fichas médicas) e patentes de propriedade intelectual.

Falando em território nacional, a conceituada empresa desenvolvedora de produtos com foco na segurança digital na Internet, a *Kaspersky Labs*®, recentemente divulgou

---

[9] "*Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades"* – disponível em: https://www.bbc.com/portuguese/internacional-43461751, acesso em 20/10/2021.

[10] "EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários"- disponível em: https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html#:~:text=O%20Facebook%20%C3%A9%20reincidente%2C%20e,usu%C3%A1rios%20no%20caso%20Cambridge%20Analytica. Acesso em 20/10/2020.

[11] "Facebook paga multa simbólica por caso Cambridge Analytica no Reino Unido" – disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/10/facebook-paga-multa-simbolica-por-caso-cambridge-analytica-no-reino-unido.html, acesso em 20/10/2021

[12] "2,3 bilhões de arquivos vazam na internet em 2018" - disponível em: https://forbes.com.br/colunas/2019/06/23-bilhoes-de-arquivos-vazam-na-internet-em-2018/ acesso em 20/10/2021

estatística[13] que traz a informação de que, 50% das PMEs (pequenas e médias empresas) brasileiras já sofreu vazamento de dados expondo informações sensíveis de funcionários, clientes e negócios correndo o risco de extorsão por parte de criminosos atuantes na rede mundial.

2.2 OBJETIVO GERAL

O objetivo geral deste Projeto é realizar uma pesquisa (e recomendações de melhorias) na preparação e missão do Departamento de Segurança da Informação (DSI) de uma empresa de médio a grande porte (faturamento acima de R$ 4.8 Milhões/Ano)[14] frente ao grande desafio da entrada em vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) com foco nas metodologias para gestão e privacidade dos dados armazenados/trafegados em meios eletrônicos.

Como escopo do Projeto, o trabalho foca em uma estrutura existente de Segurança da Informação (SI), esta já implantada dentro do contexto anterior à aprovação da LGPD e que deve ser reorientada para suportar, de maneira eficaz e eficiente, a demanda da efetiva gestão de dados em todas as suas dimensões.

Como objetivo restritivo, cabe informar que este trabalho foca a gestão de dados em sua natureza DIGITAL, e não será abordada aqui, dada a extensão do contexto a ser explorado, a privacidade de dados disponíveis em meios não-eletrônicos (ex.: documentação em papel).

2.3 OBJETIVOS ESPECÍFICOS

Partindo do Objetivo geral, foram estabelecidos os seguintes objetivos específicos:

---

[13] "Metade das PMEs já sofreu vazamento de dados" - disponível em: https://forbes.com.br/colunas/2019/06/23-bilhoes-de-arquivos-vazam-na-internet-em-2018/ acesso em 20/10/2021

[14] BNDES, Classificação de Porte de empresa, disponível em: https://www.bndes.gov.br/wps/portal/site/home/financiamento/guia/porte-de-empresa. Acesso em 21/10/2020.

- Descrever a missão do DSI, anterior a LGPD.
- Analisar as necessidades de adequação do DSI frente a nova realidade.
- Propor ações para que o DSI possa responder pronta e proativamente à esta nova realidade e apoie a empresa de forma ampliada quanto a mitigação de riscos.

3 JUSTIFICATIVA

A aceleração da utilização das plataformas digitais para a realização de negócios vem acontecendo de forma exponencial no Brasil, a exemplo do que já ocorre no resto do mundo. Segundo o veículo de informações de mercado MEIO&MENSAGEM, o e-commerce brasileiro cresceu mais de 47% no ano de 2020 em comparação ao mesmo período do ano anterior, representando a maior alta em 20 anos[15]. Ainda segundo o mesmo veículo, das tecnologias para "se ficar de olho em 2020" está em sétimo lugar, na sua classificação, a Fusão das mídias sociais com o e-commerce[16]. A utilização das mídias sociais para e-commerce oferece um desafio ainda maior aos DSI quanto à governança de dados e na prevenção de vazamentos acidentais ou propositais (onde há um ataque ou exploração de vulnerabilidades sistêmicas).

Analogamente, na mesma plataforma de informação, a Cibersegurança está classificada como a quinta tecnologia a estarmos atentos para 2020[17], justamente pela preocupação dos consumidores com a exposição de seus dados: "Transparência e rastreabilidade são elementos críticos para apoiar essas necessidades de ética e de privacidade digitais.

O dilema do Departamento de Segurança de Informação (DSI) é o de oferecer conhecimento e proteção suficientes para que os negócios da empresa possam continuar a crescer de maneira virtuosa e, para isto, é necessário conhecer em profundidade as fragilidades (e atuar nelas) que podem quebrar a relação de confiança entre a empresa, consumidor e seus parceiros de negócio [18]

Como progressão do impacto do risco, há ainda de se considerar as penalidades a serem aplicadas em caso do descumprimento das obrigações para com a privacidade dos dados classificados como alcançáveis pela lei, que vão desde a advertência, multas até a proibição

---

[15] *Meio & Mensagem - E-commerce cresce 47%, maior alta em 20 anos*. Disponível em: https://www.meioemensagem.com.br/home/marketing/2020/08/27/e-commerce-cresce-47-maior-alta-em-20-anos.html. Acesso em 22/10/2020.

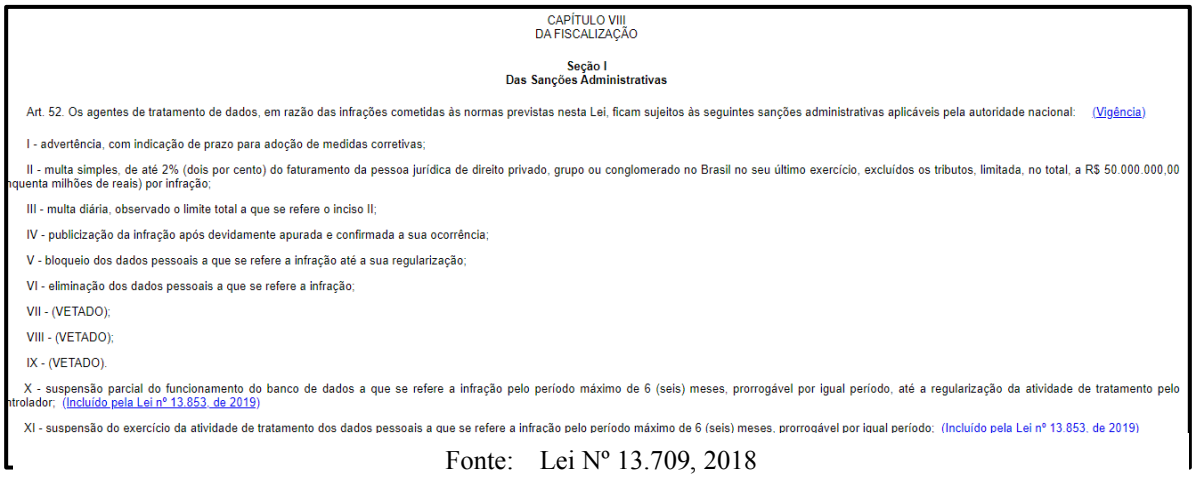
[16] *Meio & Mensagem - Tecnologias para ficar de olho em 2020 - 10. Fusão das mídias sociais com o e-commerce.* Disponível em: https://www.meioemensagem.com.br/home/opiniao/2020/01/27/tecnologias-para-ficar-de-olho-em-2020.html. Acesso em 22/10/2020.

[17] *Meio & Mensagem - Tecnologias para ficar de olho em 2020 – 5. CiberSegurança.* Disponível em: https://www.meioemensagem.com.br/home/opiniao/2020/01/27/tecnologias-para-ficar-de-olho-em-2020.html. Acesso em 22/10/2020.

[18] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. CAPÍTULO VIII - DA FISCALIZAÇÃO-Seção I - Das Sanções Administrativas. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em 22/10/2020.

parcial ou total do exercício de atividades relacionadas a tratamento de dados, estas previstas na LGPD e que podem inviabilizar a continuidade da operação da empresa. Para melhor elucidação, abaixo apresentamos quadro resumo das sanções administrativas previstas na lei.

Figura 1 – Das Penalidades e Sanções Previstas na LGPD



CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

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 nquenta 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 ntrolador; (Incluído pela Lei nº 13.853, de 2019)

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; (Incluído pela Lei nº 13.853, de 2019)

Fonte: Lei Nº 13.709, 2018

Assim, dados os riscos de continuidade do negócio da empresa em função da responsabilidade para com os dados que mantem e/ou administra, a responsabilidade do DSI para a correta orientação à empresa quanto à tratativa dos dados por ela utilizados torna-se crucial para a sua sobrevivência no mercado em que atua.

4 PROCEDIMENTOS TEÓRICO-METODOLÓGICOS

A metodologia adotada para este Projeto será de pesquisa exploratória, com coleta de dados por meio de pesquisa bibliográfica e relato de experiência. A pesquisa bibliográfica estará focada nas publicações da ABNT (Associação Brasileira de Normas Técnicas), em respeito aos Segmentos de SEGURANÇA DA INFORMAÇÃO (NBR ISO/IEC 27000), PRIVACIDADE DA INFORMAÇÃO (NBR ISO/IEC 27701, 29000 e 29143) e em literatura pertinente e amplamente utilizada por profissionais da área de Segurança da Informação e de Riscos/*Compliance.*

Atendendo aos Objetivos propostos, detalha-se abaixo a metodologia a ser utilizada, para melhor entendimento do trabalho:

- Descrever a missão do DSI, anterior a LGPD.
    - A partir da Bibliografia disponível e da experiência do autor, far-se-á a conceituação geral da estrutura de um Departamento de Segurança de Informações costumeiramente implantado em empresas de pequeno e médio porte (também é possível identificar as mesmas características em empresas de grande porte).
- Analisar as necessidades de adequação do DSI frente a nova realidade.
    - Com base ainda na bibliografia disponível, em especial em sítios na Internet assim como por literatura digital (e-books), demonstraremos e analisaremos as demandas de mudanças necessárias a serem aplicadas ao DSI corrente, para atendimento a nova realidade.
- Propor ações para que o DSI possa responder pronta e proativamente à esta nova realidade e apoie a empresa quanto a mitigação de riscos de privacidade.
    - Por fim, trazendo para o trabalho a experiência prática adquirida durante a carreira do autor e alicerçada na Bibliografia indicada, serão propostas medidas (ações) práticas para que o DSI possa atender de maneira eficaz e eficiente as estruturas da empresa para suporte à Implantação e gestão da Privacidade de Dados em atendimento a LGPD.

4.1 REFERENCIAL TEÓRICO

O referencial teórico utilizado para a presente pesquisa foi definido em quatro tópicos, a saber: a estrutura usual de um Departamento (ou área) responsável pela Segurança da informação, a responsabilidade aumentada sobre a gestão de dados para todos os participantes do processo, as teorias de ferramental para mapeamento e perseverar o sistema, a estrutura necessária do novo Departamento de Segurança da Informação, agora com foco na LGPD.

Para a correta estruturação deste projeto, o autor se utilizou de metodologia de Pesquisa Exploratória-descritiva. Estará exposto, no mesmo, os levantamentos biográficos que auxiliam na definição do problema em si assim como para a base da solução proposta, daí a menção à pesquisa exploratória.

Para o desenvolvimento do tema de forma mais aprofundada, o autor disporá da análise observatória e, para a explicação coerente dos resultados, será utilizada uma soma das análises qualitativa e quantitativa.

4.1.1 COMUNIDADE EUROPEIA: A GDPR - *GENERAL DATA PROTECTION REGULATION*.

Como uma resposta direta da comunidade europeia em relação a preocupação quanto a privacidade dos dados de seus cidadãos (anterior ao caso Facebook®), resposta esta acelerada pelos escândalos de vazamento de dados, notadamente protagonizados por empresas do continente americano, em 25 de maio de 2018, entra em vigor a GDPR (*General Data Protection Regulation n. 679* ou "Regulamento Geral de Proteção de Dados")[19], em discussão no União Europeia desde 2012 e aprovada pela mesma em 28 de Abril de 2016. Trata-se de lei que determina regras para o gerenciamento de informações as quais de alguma forma, possam identificar dados de clientes, colaboradores, parceiros de negócio e fornecedores, sem que exista o consentimento prévio destes últimos para que seus dados sejam compartilhados com quer que seja. As penalidades aplicadas às empresas vão desde multas até a decretação de

[19] "*EU data protection rules - Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field."*- disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en. Acesso em 20/10/2021

fechamento da empresa e consequente detenção de gestores que não forem diligentes quanto ao cuidado com os dados [20].

4.1.2 BRASIL: A LGPD - LEI GERAL DE PRIVACIDADE DE DADOS PESSOAIS.

No Brasil, não diferentemente do que se verifica em outros países, a preocupação com a privacidade dos dados dos seus cidadãos também veio, ao longo do tempo, tomando forma e importância. O crescer da economia digital e o apetite das novas gerações pelo uso das mídias sociais e interativas aceleraram as iniciativas governamentais para que a promulgação de uma lei que tornasse claras as regras para a utilização de dados pessoais. A própria União Europeia, com base no artigo 45 de sua lei regulatório número 2016/679[21], classifica se um país está ou não adequado quanto ao seu nível de proteção de dados[22].

O fato de um país estar na lista daqueles onde há regulação quando as tratativas (efetivas) dos dados, o diferencia dos demais em oportunidades de investimentos e comercio por parte dos países da União Europeia.

Com isto o governo brasileiro, em 14 de agosto de 2018, promulga a lei de número 13.709/18, denominada "LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)"[23] com o objetivo de normatizar o uso de dados dos cidadãos, empresas e entidades públicas brasileiras. Segundo MENDES & DONEDA (2016, p. 35-48, apud KLEE e NETO, 2019, p.30.) há uma clara proximidade com a *GDPR*:

> "A LGPD é bastante inspirada na regulamentação europeia. Adota um modelo *ex ante*[24] de proteção de dados, baseado no conceito de que não existem mais dados

---

[20] "*EU data protection rules - Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field.*"- disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en acesso em 20/10/2021

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC. Acesso em 20/10/2020.

[22] European Comission, *Adequacy Decisions*, disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents. Acesso em 21/10/2020.

[23] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em 21/10/2020.

[24] *EX ANTE* – "Para diante", (SARAIVA, 2019, p.81).

> irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação".

Para que a dimensão da LGPD possa ser corretamente compreendida principalmente no contexto deste trabalho que objetiva a definição da missão do Departamento de Segurança de Informação frente a Lei, é importante ter em mente conceitos por ela definidos.

De acordo com MENDES & DONEDA (2016, p. 35-48, apud KLEE e NETO, 2019, p.18.), temos o seguinte, sobre os conceitos legais abordados na lei:

> "A LGPD define alguns conceitos que nortearão a sua interpretação e aplicação. É um ponto bastante positivo da Lei. Entre os conceitos trazidos no texto legal, destaque deve ser dado às definições de dado pessoal, de dado pessoal sensível, dado anonimizado, banco de dados, tratamento e consentimento. Mas a LGPD não se restringe a apenas esses conceitos, trazendo outros." (vide Figura 2)

Figura 2 – Conceitos estabelecidos pela lei 13.709/18

Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
Agentes de tratamento	O controlador e o operador
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
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
Transferência internacional de dados	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
Uso compartilhado de dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados
Relatório de impacto à proteção de dados pessoais	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco
Órgão de pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. A importância na definição desses conceitos no texto legal está no fato de servirá de guia para a correta interpretação e aplicação da lei, bem como da fiscalização com relação ao seu fiel cumprimento

Fonte: MENDES&DONEDA (apud KLEE e NETO, 2019, p.18.)

É notório que o texto da Lei identifica, de forma clara, o objeto necessário de proteção que é o dado em sua essência elementar, quando este de alguma forma possa identificar a pessoa natural, de maneira direta ou indireta. Assim, a qualificação e o controle sobre o dado desde o seu nascedouro, sua coleta até a forma como que ele é disponibilizado, torna-se uma missão importantíssima e estratégica para as empresas, como nos diz BRAZ (2020, p.650):

> "Igualmente preocupante é como efetivamente as empresas têm garantido a Segurança da Informação no manuseio desses dados. Por fim, a ausência de maior transparência quanto ao tratamento bem como a impossibilidade de os titulares poderem efetivamente exercer maior controle sobre seus dados, representam mais desafios a serem superados para assegurar respeito/observância a direitos e a garantias dos cidadãos pelos agentes de tratamento. A Lei Geral de Proteção de Dados chega para empoderar o cidadão, impondo aos agentes de tratamento obrigações para endereçar e sanar os desafios elencados."

É neste contexto que o Departamento de Segurança da Informação assume um protagonismo importante e decisivo para o efetivo controle e proteção deste ativo tão caro para as empresas, frente ao desafio a necessidade mandatória de se garantir a privacidade dos dados, regulada a partir da LGPD, como nos alerta MARINHO (2020, p.85):

> "Proteção de dados = privacidade. E não se obtém proteção de dados seguindo a Lei. É necessário um forte trabalho de divulgação, conscientização e implementação de SI, para que seus objetivos consolidem a privacidade de dados e informações".

Seguiremos, agora, com o desenvolvimento do tema dentro das expectativas de explanar, da melhor maneira possível, o objetivo e os caminhos para atingimento dele.

4.1.3 A ESTRUTURA CONTEMPORÂNEA DE UM DEPARTAMENTO DE SEGURANÇA DE INFORMAÇÕES

Geralmente, nas empresas Brasileiras de pequeno e médio porte (algumas vezes até de grande porte), o DSI fica estruturalmente alocado dentro da área de Tecnologia da Informação (TI) a qual, por sua vez, responde ao CFO (*Chief Finance Officer* – Executivo principal da área Financeira). Isto se dá desta forma, quer seja pelo entendimento muitas vezes

equivocado que estrutura organizacional da Empresa possui sobre as missões das áreas de TI e do DSI ou pela dificuldade em deliberar o plano orçamentário para estas áreas[25].

SÊMOLA (2014, 2.6 *Posicionamento Hierárquico*. n.p.) nos alerta quanto a este entendimento:

> "Diante da abrangência dos desafios associados à segurança da informação, torna-se fundamental reorganizar a estrutura hierárquica da empresa a fim de suprir as novas demandas. É comum haver imediata confusão ao associar as atividades e a responsabilidade da gestão de segurança à área tecnológica. Muitas empresas insistem em relacionar, e muitas vezes encapsular, o orçamento e as ações de segurança ao plano diretor de informática ou plano estratégico de TI."

Não limitado ao nome ou ao posicionamento hierárquico ao qual o DSI esteja vinculado na empresa, sua missão é a de ser responsável pelo suporte à definição, implantação e operacionalização do SISTEMA DE GESTÃO DA SEGURANÇA DE INFORMAÇÕES (SGSI).

A ABNT NBR ISO27701 (Privacidade de dados) nos traz, em sua introdução, a referência a conceituação do SGSI [26]:

> "O Sistema de Gestão de Segurança da Informação (SGSI), definido na ABNT NBR ISO/IEC 27001, é projetado para permitir a adição de requisitos específicos setoriais, sem a necessidade de desenvolver um novo Sistema de Gestão. As Normas de Sistemas de Gestão ISO, incluindo as específicas por setor, são projetadas para poderem ser implementadas separadamente ou como um Sistema de Gestão combinado."

Mais do que um sistema computadorizado, o SGSI é um processo definido para que a empresa tenha visão ampliada e controlada de sua segurança da Informação.

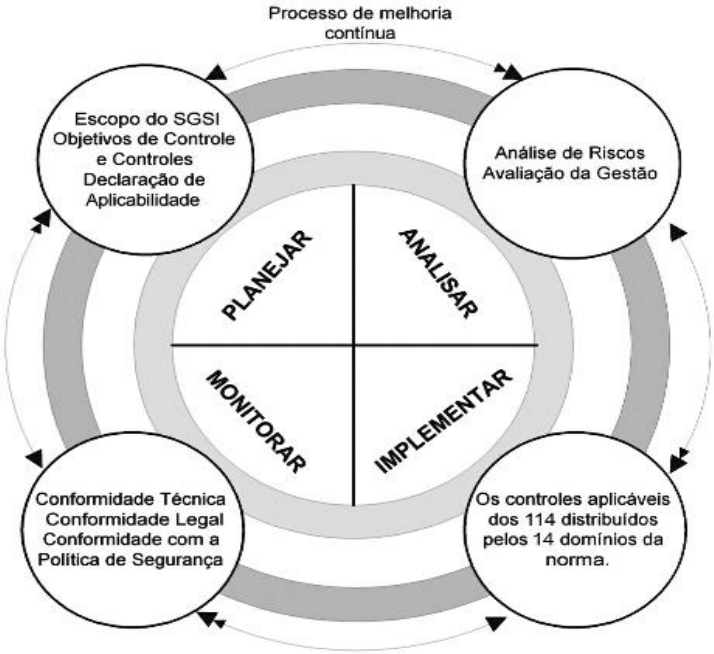
---

[25] SÊMOLA, Marcos. Gestão da segurança da informação. GEN LTC. Edição do Kindle, 2014.

[26] ABNT, 2020 –ABNT NBR ISO/IEC 27701 - *Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação-Requisitos e diretrizes.* Pg ix.

Abaixo, segue a representação do Framework de SGSI, segundo SEMOLA(2014):

Figura 3 – Modelo de Framework SGSI



Fonte: SEMOLA (2014)

Especial atenção se deve atribuir ao quadrante da análise de riscos e Avaliação da Gestão, onde inclui-se a previsão para a gestão de dados e de Privacidade.

As premissas básicas que atendem o SGSI, por si próprias suportam a governança da privacidade de dados em suas dimensões. Estas Premissas, as quais e podemos denominar como CONTROLES são, conforme SÊMOLA (2014), as seguintes:

> "Domínios/controles:
> Políticas de segurança da informação
> Organização da segurança da informação
> Segurança em recursos humanos
> Gestão de ativos
> Controle de acesso
> Criptografia
> Segurança física e do ambiente
> Segurança nas operações
> Segurança nas comunicações
> Aquisição, desenvolvimento e manutenção de sistemas
> Relacionamento na cadeia de suprimento
> Gestão de incidentes de segurança da informação
> Aspectos da segurança da informação na gestão da continuidade do negócio

Conformidade.”

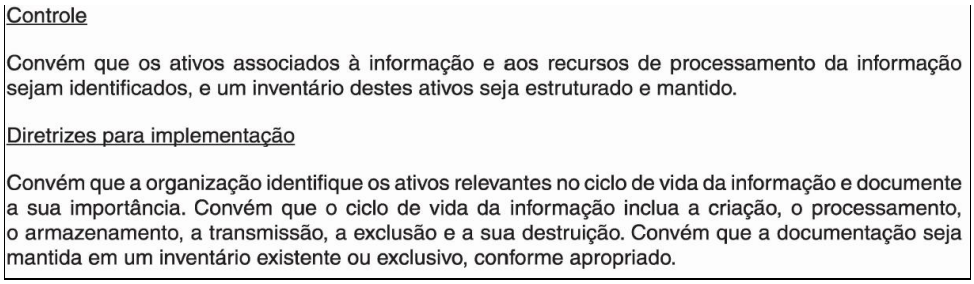
Dentro destes controles, há particular importância a ser dedicada a disciplina de CLASSIFICAÇÃO DE INFORMAÇÕES, esta que deve estar presente na POLÍTICA DE SEGURANÇA DE INFORMAÇÕES, conforme nos traz novamente SÊMOLA (2014):

> “... e classificação da informação são bons exemplos de normas de uma típica política de segurança. Em especial, a norma de classificação da informação é fator crítico de sucesso, pois assume a responsabilidade por descrever os critérios necessários a fim de sinalizar a importância e o valor das informações, premissa importante para a elaboração de praticamente todas as demais normas. Não há regra preconcebida para estabelecer essa classificação, mas é preciso entender o perfil do negócio e as características das informações que alimentam os processos e circulam no ambiente corporativo para que os critérios sejam personalizados.

De forma análoga, para que seja efetiva a gestão de riscos e de privacidade, é vital que a empresa possua uma compreensiva e extensiva gestão de seus ativos de Tecnologia (Computadores, dispositivos de armazenamento de dados, telefones móveis etc.) ou seja, todos os meios eletrônicos ativos e passivos que tenham capacidade de armazenar dados em sua estrutura física.

A norma ABNT NBR ISO 27002, em seu capítulo 8 – GESTÃO DE ATIVOS, conceitua a importância do que está colocado acima:

Figura 4 – Gestão de ATIVOS - ABNT



Controle

Convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estruturado e mantido.

Diretrizes para implementação

Convém que a organização identifique os ativos relevantes no ciclo de vida da informação e documente a sua importância. Convém que o ciclo de vida da informação inclua a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição. Convém que a documentação seja mantida em um inventário existente ou exclusivo, conforme apropriado.

Fonte: ABNT NBR ISSO/IEC 27002:2013 – (2013, Gestão de ativos. pg.16)

Igualmente crítico é o controle efetivo que se deve possuir quanto ao mapeamento de dados da organização, o qual deve reunir meios automatizados, ou manuais, para suporte a esta disciplina, como nos diz BRAZ (2020, p. 660):

> “O processo de mapeamento de dados pessoais tratados pela organização é uma etapa fundamental no projeto de implementação da LGPD. Através dele, com a análise de todos os processos de negócio que envolvam dados pessoais, observando todo ciclo de vida dos dados tratados (que envolve coleta, armazenamento, utilização,

> compartilhamento, reutilização elou destruição deles), é possível identificar as ações a serem adotadas para garantir a Segurança da Informação bem como outros elementos relevantes para etapas posteriores da adequação."

4.1.4 A ADEQUAÇAO DO DSI EM RELAÇÃO À LGPD (GESTÃO DE DADOS).

A responsabilidade do DSI, gestor dos mecanismos de Segurança da Informação, ganha especial protagonismo quanto a gestão da privacidade dos dados, como nos diz CUEVA (2020, p.540),

> "Embora a garantia da segurança da informação não se confunda com o direito à proteção de dados pessoais, como muitas vezes se acredita, há inequívoca relação de pertinência entre eles."

Ainda acrescenta, em seguida, quando a associação entre a Segurança da Informação e a privacidade de dados:

> "A segurança da informação é indissociável da proteção de dados pessoais. E um pré-requisito, uma condição de possibilidade para que se tutelem efetivamente os direitos dos titulares dos dados pessoais."

Adicionalmente, propõe CUEVA (2020, p.540), quanto ao entendimento que se deve ter quanto ao que é a Segurança da Informação sob a ótica da Associação Brasileira de Normas técnicas:

> "A Segurança da informação, tal como definida na norma técnica ISO/IEC 27002, é "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".
>
> A segurança da informação, portanto, deve resguardar a confidencialidade, a integridade e a disponibilidade dos sistemas e dos serviços de tratamento.

Como resultado, mas não limitado a este, responsabilidade pelo inventário de dados, este proposto como legado importante do SGSI, assume vital importância para a sobrevivência da organização.

Nos diz FONTES (2020, pg.6), sobre a relação entre o SGSI e a LGPD:

> "Sem um Programa Organizacional de Segurança da Informação efetivo, a organização não tem sustentabilidade para a conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD. Evidentemente esta lei tem outros controles legais que não diz respeito diretamente com a segurança da informação."

Pode-se assim dizer que o DSI, para atender às determinações da LGPD, essencialmente necessitará ter o SGSI sedimentado na organização para que o departamento possa atuar atendendo as expectativas de apoio ao DPO (em inglês *Data Privacy Officer*), pois é este (SGSI) que fornecerá as premissas e diretrizes para a Gestão efetiva da Segurança da Informação. Caberá ao DSI apoiar a estrutura de governança da companhia, em especial o DPO, quanto a selecionar ferramental para apoio a disciplina de Gestão de Privacidade de tal forma que a resposta a incidentes (ou suspeita) seja ágil, consistente e determinante ao ponto de mitigar riscos de vazamento de dados ou/e, detectar o "ponto de fuga" pós-evento. O CISO *(Chief Information Security Officer*), responsável pelo DSI, examina questões de segurança do ponto de vista de negócios e operações. Ao reforçar a postura de proteção cibernética de uma organização, esse profissional trabalha para garantir que todas as informações da empresa sejam processadas de maneira segura.[27]

Ao contrário do exemplo acima, que está focado em proteger os interesses de segurança da organização, "o DPO se preocupa principalmente com a forma em que a organização lida com dados pessoais. Suas preocupações incluem comunicação com os titulares dos dados, gerenciamento de direitos, minimização de armazenamento, coleta, processamento e minimização de dados"[28].

4.1.5 MISSÃO DO DSI NA GESTÃO DA SEGURANÇA DE DADOS.

A fluidez dos dados e informações da empresa, dada a sua volatilidade, devem ser gerenciados de forma perene com particular importância a ser conferida a constante atualização

---

[27] Privacidade de dados demanda trabalho em conjunto entre DPOs e CISOs. Disponível em: https://www.securityreport.com.br/overview/privacidade-de-dados-demanda-trabalho-em-conjunto-entre-dpos-e-cisos/#.YZBYaFPQ9QI. Acesso em 10/11/2021.

[28] Privacidade de dados demanda trabalho em conjunto entre DPOs e CISOs. Disponível em: https://www.securityreport.com.br/overview/privacidade-de-dados-demanda-trabalho-em-conjunto-entre-dpos-e-cisos/#.YZBYaFPQ9QI. Acesso em 10/11/2021.

do inventário de ativos e de dados, de forma a identificar pontos de vulnerabilidade de maneira antecipada.

SILVA (2020, p.93), traz à luz do conhecimento da importância do inventario e Mapeamento de dados:

> "O inventário e o mapeamento de dados são componentes-chave de um programa de governança em privacidade. As organizações precisam saber o tipo de dados que coletam e como eles são compartilhados, processados e armazenados para que possam atender aos requisitos das normas de privacidade e gerenciar riscos em toda a organização. Conforme ensina Renato Opice Blum1: Com o mapeamento dos dados, pode-se identificar se há excessos nos tratamentos, ou se somente os dados necessários foram coletados para a finalidade proposta. É possível conferir se as bases legais usadas são condizentes para determinadas finalidades, ou se não há base que justifique o tratamento do dado coletado. Finalmente, o mapeamento permite identificar os principais focos de riscos no tratamento de dados de cada organização e que demandam mais cuidados e ações."

A adoção de ferramental para que este inventário seja atualizado de forma constante e sólida, é fator de sucesso (Maturidade) para que a gestão dos dados seja eficaz, visto o dinamismo, do ciclo de vida da informação nas empresas. Já existem diversas ferramentas de mercado que suportam a demanda, mas considerando o alto custo hoje aplicado pelos fornecedores das soluções, há possibilidade de serem adotadas ferramentas de automação de departamento como base para que seja elaborado inventário suficientemente capaz de fornecer apoio para a avaliação de situações de risco. Claramente, para grandes instituições, onde o volume e a complexidade da estrutura de informações tratadas pela companhia, são altos e com alto grau de volatilidade e fluidez, necessária será a contratação de ferramental mais evoluído (sistema de gestão de dados) que ofereça possibilidades de automação, alarmes em desvios de propósito e controle de obsolescência.

SILVA (2020, p.94) justifica o paragrafo anterior, conceituando a importância da maturidade na seleção de ferramental para suporte a governança da LGPD, caracterizando as funcionalidades que devem estar presentes:

> "Nesse aspecto, as plataformas de gestão de privacidade têm apresentado soluções para mapeamento de dados com as seguintes funcionalidades: Interface fácil de usar para incluir e atualizar dados. Possibilidade de inclusão em massa de dados sobre ativos e atividades de processamento de dados pessoais, bem como atribuição de riscos. Portal com questionários prontos ou customizáveis para envio automatizado para obtenção de informação sobre ativos e atividades de processamento. Gestão do

> fluxo de trabalho e automação de processos de mapeamento de dados. Painel visual da localização dos ativos de TI e do fluxo de dados para outros países. Painel de controle com os indicadores mais relevantes."

4.1.5.1 METODOLOGIAS E FERRAMENTAL PARA APOIO A GESTÃO DA PRIVACIDADE

A princípio, as normas/metodologias que nos parecem as mais adequadas para a gestão da Segurança da Informação (em apoio a Gestão de Privacidade de dados) são aquelas compiladas pela ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Aqui ressaltamos as normas de gestão da *Cybersecurity*, como as ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos e de gestão da Privacidade e a ABNT NBR ISO/IEC 16167:2013 - Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.

Já para a gestão efetiva da Privacidade a ABNT NBR ISO/IEC 27701:2019 Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes, apresenta-se como eficaz para a orientação da gestão da Privacidade de dados.

Ambos os parágrafos acima são justificados por BLUM (2020):

> "No Brasil, há um contunde normativo acerca de gestão de segurança da informação constante principalmente nas normas da Associação Brasileira de Normas Técnicas (ABNT), notadamente: (i) a ABNT NBR ISO/IEC 27001, de 2013, acerca de sistemas de gestão de segurança da informação; (ii) a ISO/IEC 27002, também de 2013, sobre código de prática para controles de segurança da informação, que, se internalizadas e adotadas pelas organizações, já poderiam identificar o valor e a criticidade de dados pessoais e mitigar os riscos do seu tratamento; bem como, recentemente, (iii) a ABNT NBR ISO/ IEC 27701, de 2019, que trata da extensão das citadas normas, mas justamente para a gestão da "privacidade da informação", com diretrizes e requisitos, havendo um item dedicado à "Avaliação de impacto de privacidade"

Por sua vez, o ferramental técnico disponível no mercado para atender a gestão de dados estruturados e desestruturados (sem uma organização formal) já existe há algum tempo, porém, encontrar uma ferramenta que cubra na totalidade o que a LGPD exige ainda é um

grande desafio dada a complexidade dos ambientes de TI das empresas e seu nível de profissionalismo e experiência. A melhor ferramenta ainda é a gestão processos.[29]

Para que as ferramentas possam oferecer um bom nível de confiabilidade, as áreas de TI (Tecnologia da Informação) e de Segurança da Informação necessitam estar alinhadas com os gestores de negócio em toda a dimensão da empresa, como nos diz FONTES (2016):

> "A Sustentabilidade do processo de segurança da informação é o conjunto de ações e decisões que devem existir para que este processo:
> - Seja contínuo ao longo do tempo,
> - Permita que este processo se retroalimente,
> - Permita que a organização aprenda,
> - Possibilite que as perdas e impactos que o processo de segurança impediu que a organização sofresse, tornem-se os geradores de recursos para o patrocínio deste processo.
>
> Sem dúvida alguma o apoio da alta direção da Organização e o alinhamento aos objetivos de negócio são críticos para que haja esta sustentabilidade."

Assim, o Departamento de Segurança de Informação, como já citado neste documento, assume vital importância para manter alinhadas as estratégias de Governança de Segurança da Informação e de Governança Corporativa, como nos coloca FONTES (2016):

> "Considere a Governança da Segurança da Informação alinhada à Governança Corporativa. Apresente no planejamento estratégico como acontecerá a Governança de Segurança e como será garantida este alinhamento. Inclusive a validação, pela Direção, do planejamento estratégico é uma das ações deste alinhamento."

Para enfrentar este desafio, entidades do mundo inteiro, destacadamente aquelas que já tiveram de se adequar à GDPR, desenvolveram *frameworks*, que apoiam as áreas de segurança de informações, assim como de Tecnologia de Informação e *Compliance*, na missão da gestão de segurança, não limitado somente na gestão de dados.

---

[29] Qual a melhor ferramenta de adequação à LGPD?, disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/qual-melhor-ferramenta-adequacao-lgpd-protecao-dados. Acesso em 10/11/2021.

Em esclarecimento, um *framework* diz respeito a um conjunto de ferramentas, processos e disciplinas que buscam a simplificar a gestão sobre algo ou alguma coisa, como esclarecem FABRETTI&LOPEZ (2020, p.75):

> "Apesar de ser um termo normalmente distante da prática jurídica, frameworks são nada mais do que uma forma de organizar um determinado assunto de maneira didática, que possibilite um melhor controle e mensuração e são comumente utilizados nas áreas de governança corporativa e segurança da informação. Em outras palavras, criando, adaptando e utilizando um framework de privacidade já existente, é possível organizar as obrigações, requerimentos e direitos previstos, por exemplo, na Lei Geral de Proteção de Dados Pessoais, deforma que se possa instituir controles que, caso presentes, demonstrem que determinada organização está em conformidade"

Neste foco, o NIST (em inglês: *National Institute of Standards and Technology*), órgão vinculado ao Departamento de Comércio do governo dos estados Unidos da América e que oferece referencias de padrões de tecnologia para todo o Globo, em atendimento as crescentes demandas por gestão eficiente da segurança de dados, desenvolveu alguns frameworks de suporte para o DSI e a área de TI.

O NIST apresentou seu NIST *Framework for improving Critical Infrastructure Cybersecurity*[30], que contempla diversas disciplinas e processos que tratam amplamente da metodologia de gestão de riscos da Segurança da Informação com especial atenção dada a gestão de segurança de dados.

Ainda para sermos mais específicos quanto ao tratamento de Privacidade de dados, o NIST disponibilizou um outro *framework* que aprofunda nas técnicas de gestão de segurança e privacidade de dados, o NIST *Privacy Framework: A tool for improving Privacy through Enterprise Risk Management*[31].

Este *framework* atinge seus objetivos de ser um ferramental de suporte para que empresas e entidades públicas realizem um tratamento adequado e otimizado de dados pessoais geridos e armazenados em suas estruturas.

Os *frameworks* propostos são compostos de um documento de metodologia e uma ferramenta de classificação de ações.

As ferramentas estão desenvolvidas em planilhas de computador a partir do Software de Automação de escritório, Microsoft Excel, de ampla utilização por empresas de

---

[30] Disponível em https://www.nist.gov/cyberframework/framework. Acessado em 09/10/2021

[31] Disponível em https://www.nist.gov/privacy-framework/privacy-framework. Acessado em 09/10/2021

diferentes tamanhos dada a sua popularidade. Sua utilização como base ferramental para apoio a gestão de *Cybersecurity* e de Privacidade de dados é detalhada nos documentos de metodologia.

4.1.5.2 CASO PARTICULAR: A MISSÃO DO DSI EM APOIO A DESTRUIÇÃO DOS DADOS.

Cabe ainda uma particular atenção quanto ao papel do DSI no atendimento a uma das regras (bases legais) das mais importantes e que está contemplada na LGPD diz respeito quanto a destruição dos dados, quando estes não se fazem mais de legítimo interesse por parte da empresa que detém o dado de outrem.

O artigo 16, Seção IV da LGPD[32] determina que dados pessoais devem ser eliminados após o término de seu tratamento:

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

Levando-se em conta que a declaração de legitimo interesse deve ser justificada formalmente pela empresa a qualquer momento quando requisitado pela ANPD, também deve-se ter em mente que não somente os aspectos de segurança da gestão da manutenção daqueles dados em suas bases de dados devem ser suportados pelas justificativas, mas como também a destruição dos mesmos deve ser igualmente considerada como crítica.

CUEVA (2021, pg.544) nos diz sobre o apagamento dos dados pessoais e a responsabilidade da empresa (aqui denominado controlador) que pode ser questionada

---

[32] LEI 13.709 DE 14 DE AGOSTO DE 2018 (LGPD). *Disponível em*: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 07/10/2021.

legalmente pela falta de controle na gestão e destruição dos dados, o que implica diretamente na qualidade com que a Segurança de Informação é mantida pela empresa:

> "A destruição de dados aponta para a aniquilação do dado pessoal, enquanto a alteração indica uma corrupção de sua forma ou de sua completude. Já a perda de dados pessoais pode significar um obstáculo de acesso pelo controlador, a exemplo do que se tem recorrentemente verificado nos ataques de hackers, que por vezes exigem o pagamento de resgate para que os dados sejam novamente acessíveis (ransomware), mas pode também ser resultado de apagamento acidental das informações ou, ainda, quando os dados estiverem criptografados, da perda da chave criptográfica. Obviamente, a perda pode ser meramente temporária, situação que exige análise de seus riscos e efeitos sobre os direitos dos titulares dos dados. A cláusula final do caput do art. 46 da LGPD, que remete a "qualquer forma de tratamento inadequado ou ilícito", abrange todos os incidentes de segurança, sejam eles causados por terceiros, sejam causados por desídia dos agentes de tratamento. De todo modo, os incidentes de segurança podem ser classificados como incidentes de confidencialidade (acesso elou divulgação não autorizados), de integridade (alteração não autorizada de dados) e de disponibilidade (perda de acesso ou destruição de dados pessoais). Para cada uma dessas três modalidades de incidente de segurança há recomendações específicas, em linha com a norma ISO/IEC 17799:2005"

A responsabilidade do DSI quanto as medidas de segurança suficientes para garantir a privacidade e gestão efetiva dos dados não é nenhuma novidade para o DSI, inclusive a mesma estando disposta nas normas da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS que regem a disciplina de Segurança e privacidade de dados como as ABNT NBR ISO/IEC 16167:2013[33], ABNT NBR ISO/IEC 27001:2013[34], ABNT NBR ISO/IEC 27002:2013[35], ABNT NBR ISO/IEC 27701:2019[36] e assegurar que o dado foi definitivamente destruído para que o mesmo não possa ser recuperado de forma a atestar o encerramento do relacionamento entre o cliente e a empresa, é ação mandatória e prevista na lei, como confere CARDOSO (2021):

---

[33] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 16167:2013 - Segurança da Informação - *Diretrizes para classificação, rotulação e tratamento da informação*

[34] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISSO/IEC 27001:2013 - Tecnologia da informação - *Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos*

[35] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISSO/IEC 27002:2013 - Tecnologia da informação -*Técnicas de segurança - Código de prática para controles de segurança da informação*

[36] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27701:2019 - Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

> "A partir do exercício do direito ao conhecimento da existência de tratamento de dados pessoais, o titular pode exercer diversos direitos, previstos especialmente no art. 18 e em outros dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
>
> Entre eles está o direito à eliminação dos dados pessoais, que leva ao fim de qualquer operação de tratamento pelo controlador ou pelo operador.
>
> O inciso IV do art. 18 da LGPD contém três direitos, que podem ser exercidos quando o controlador tratar dados desnecessários, excessivos ou realizar operações de forma contrária às normas da LGPD: a anonimização, o bloqueio e a eliminação.
>
> O direito à eliminação consiste na paralisação total das operações de tratamento e o consequente descarte dos dados pessoais ou do banco de dados, o que não permite a posterior retomada do tratamento.
>
> Além de um direito do titular, a eliminação dos dados pessoais também é uma sanção administrativa (art. 52, VI, da LGPD) e uma consequência direta do término do tratamento de dados pessoais, ressalvadas as exceções legais (arts. 15 e 16 da LGPD)."

A importância aqui dada a metodologia em detrimento ao ferramental é justificada pela complexidade de se ter ferramental único que tenha a capacidade de consolidar de maneira automática o inventário de dados em sua totalidade. Assim a metodologia ganha um protagonismo importante para que os diferentes mecanismos de armazenamento de dados sejam considerados em tempo de necessidade de ações de recuperação e/ou apagamento de dados.

Sem a utilização de metodologia adequada para garantir que o dado foi efetivamente retirado de circulação nas bases de informação da empresa, o risco de exposição destes dados passa a ser crítico assim como é elevado (e agravado) o risco de punição monetária por exposição indevida ou descumprimento da requisição de destruição do dado dentro do prazo determinado.

5 CONCLUSÃO

Como procuramos demonstrar no decorrer do presente projeto pela pesquisa efetuada, a entrada da LGPD veio trazer a necessidade de ser tratada com definitivas maturidade e responsabilidade, a gestão dos dados de clientes, fornecedores, funcionários e todo ecossistema que participa da vida das empresas (e setores públicos, aqui não abordados). A responsabilidade da segurança aplicada por uma empresa sobre a gestão dos dados que armazena, sai do campo de "melhores esforços" e é elevada à categoria de altíssimo risco para a continuidade de negócios e conseguinte sobrevivência da empresa.

Constatamos pela pesquisa que, desde a implantação da Lei geral de Privacidades dos Dados Pessoais (LGPD) e a efetiva entrada em vigor das punições monetárias ocorrida em agosto de 2021, a corrida pela adequação dos controles da gestão dos dados vem acontecendo de maneira acelerada e consumindo tempo e recursos financeiros das empresas que não desejam ter sua marca atrelada a escândalos nas mídias por descuido no tratamento dos dados a elas confiados. Adicionalmente, segue a penalização financeira que afetará de forma significativa o fluxo de caixa da empresa que, em casos extremos, pode determinar a extinção dela junto ao mercado.

Diante deste contexto, o papel desempenhado pelo Departamento de Segurança da Informação (DSI), como suporte operacional e tecnológico às áreas de sustentação da empresa (Jurídico, *Compliance*, Recursos Humanos, Financeiro) passa a ser caminho crítico para manutenção da continuidade dos negócios dada a sua relação direta com o SGSI (Sistema de Gestão da Segurança da Informação) em todas as suas disciplinas, especialmente quanto a análise e gestão de riscos de Tecnologia da Informação, invariavelmente gestora dos mecanismos de controle de dados da empresa.

Pela pesquisa é possível constatar que, apesar dos Departamentos de Segurança da Informação (quando bem estruturados), terem condições de atender à maioria das regras e determinações impostas pela LGPD assim como responder (diretamente ou indiretamente, em suporte ao DPO) às questões formuladas pela autoridade de fiscalização (ANPD) em tempo de auditoria, dado ao exíguo tempo de resposta exigido e a rigidez das sanções a serem aplicadas em caso da constatação da falta de assertividade e de controles dedicados à Privacidade de dados, é mister estar aplicada (e em regime de uso), metodologia de gestão de Privacidade de dados baseada em pilares consolidados na gestão da segurança da informação, comprováveis e de conhecimento da autoridade.

Também como resultado da referida Pesquisa, evidenciamos a importância da adoção de ferramental tecnológico disponível no mercado. Para compor a oferta de solução tecnológica, recomendamos a utilização de *frameworks* do NIST (em Inglês: *National Institute of Standards and Technology*) como o NIST *Framework for improving Critical Infrastructure Cybersecurity*, e o NIST *Privacy Framework: A tool for improving Privacy through Enterprise Risk Management* para que a área de Segurança da Informação atue de maneira mais efetiva e eficiente no apoio que deve ser dado às áreas de negócio e, principalmente, ao DPO que deverá assumir a função de ponto focal da empresa para os assuntos de Privacidade, como rege a LGPD.

6 CONSIDERAÇÕES FINAIS

Todos os conceitos que aqui foram expostos visam trazer a visão do autor sobre a nada nova definição de que os Departamentos de Segurança da Informação (DSI) devem desde sempre estarem preparados e estruturados de forma a atender de forma efetiva as disciplinas que regem a proteção da informação em seu estado mais natural: o dado.

Como colocado no desenvolvimento do tema, não é de hoje que temos normas que, pelo menos desde 2003, regem os princípios de aplicação da segurança tecnológica em todo o ecossistema de tecnologia da informação, como as normas internacionais ISO e as nacionais (e muito bem estruturadas) ABNT NBR ISO/IEC. Mais do que orientar, estas normas são básicas para que a empresa enfrente diversos tipos de contestações e auditorias focadas em como a empresa está gerindo sua governança de Informações.

O fato de a LGPD ter entrado em vigor confere uma escalada no risco de continuidade das empresas em seus meios de atuação, ainda mais para aquelas que não possuem práticas adequadas para a gestão da Privacidade dos dados. Desta forma, a necessidade de prevenção ao risco vem agregar mais celeridade às premissas de se ter Departamentos de Segurança da Informação mais estruturados, atuantes e, antes de tudo, preparados para responder de maneira efetiva e consistente às demandas que serão colocadas para sua atuação.

Espera-se que as empresas, nesta nova fase global de se ter um olhar mais aguçado sobre a Privacidade dos dados, empenhem-se de maneira responsável e contínua em disponibilizar recursos financeiros suficientes para que as estruturas de Segurança da Informação, Tecnologia da Informação e de *Compliance*, possam atuar na importante e determinante missão de preservar o novo “ouro” da vida moderna: A informação.

7 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 16167:2013 - Segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.**

_____. **NBR ISO/IEC 27001:2013 - Tecnologia da informação - *Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos***

_____. **NBR ISO/IEC 27002:2013 - Tecnologia da informação -Técnicas de segurança - Código de prática para controles de segurança da informação**

_____. **NBR ISO/IEC 27701:2019- Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**.

Brasil, **Estratégia nacional de segurança cibernética**. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica. Acesso em 06/10/2021.

Brasil, **LEI 13.709 de 14 de agosto de 2018 (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 07/10/2021.

Brasil, M**arco civil da internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 07/10/2021.

Brasil, **Normativos e frameworks de proteção de dados pessoais**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/normativos-e-frameworks-de-protecao-de-dados-pessoais. Acesso em 06/10/2021.

BRAZ, Marcilio Jr. et al. **A Lei Geral de Proteção de Dados Pessoais LGPD:** aspectos práticos e teóricos relevantes no setor público e privado / - coordenação. -- 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021.

Cardoso, Oscar Valente. **Direito à eliminação dos dados pessoais na lei geral de proteção de dados pessoais**. Disponível em: https://jus.com.br/artigos/90814/direito-a-eliminacao-dos-dados-pessoais-na-lei-geral-de-protecao-de-dados-pessoais. Acesso em 10/11/2021.

CUEVA, Ricardo Villas Boas, **Segurança de Informações e proteção de dados pessoais. A Lei Geral de Proteção de Dados Pessoais LGPD:** aspectos práticos e teóricos relevantes no setor público e privado / Denise de Souza Luiz Francoski, Fernando Antônio Tasso - coordenação. -- 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021.

Et Al., BLUM, Renato Opice. **Proteção de Dados** Forense. Kindle Edition.

FABRETTI, Henrique; LOPEZ, Nuria. **Frameworks de Privacidade na Construção de Programas de Conformidade em Data Protection Officer:** Teoria e Prática de Acordo com

a LGPD e o GDPR**.** Coordenadores: BLUM, Renato Opice; VAZINOF, Rony e FABRETTI, Henrique. Ed. Revista dos Tribunais, 2020, p. 74.

FONTES, Edison. S**egurança da Informação: Gestão e Governança: (Conformidade para a LGPD)** (p. 6). 2020. Edição do Kindle.

FONTES, Edison. S**egurança da Informação: Orientações Práticas.** 2016. Editora Profissional. Edição do Kindle.

FRANCOSKI, Denise de Souza Luiz, TASSO, Fernando Antônio. **A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado /** - coordenação. -- 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021.

KLEE, Antônia Espindola Longoni, NETO, Alexandre Pereira Nogueira. **Proteção de dados Pessoais: Privacidade versus Avanço Tecnológico.** Caderno Adenauer 3 Schutz von persönlichen Daten (2019). PDF disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em 21/10/2020.

MARINHO, Fernando. **Os 10 mandamentos da LGPD**. 1. ed. – São Paulo, SP: Atlas, Edição do Kindle,2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018**. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em 07/10/2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. Version 1.0. 2020**. Disponível em: https://www.nist.gov/privacy-framework/privacy-framework. Acesso em 07/10/2021.

SARAIVA, F.R. dos Santos. **Dicionário Latino-português. 13 ed**. - Belo Horizonte, MG: Garnier, 2019.

SÊMOLA, Marcos. **Gestão da segurança da informação**. GEN LTC. Editora Elsevier. Edição do Kindle, 2014.

Et Al., SILVA, Laercio. **Proteção de dados: desafios e soluções na adequação à lei. – Rio de Janeiro: Forense, 2020.** Edição do Kindle.