LGPD: MEDIDAS ESSENCIAS DE SEGURANÇA DA INFORMAÇÃO

LGPD: ESSENTIALS INFORMATION SECURITY

Elton Pereira Duarte, Fatec Araraquara, elton.duarte@fatec.sp.gov.br
Romeu Domeniconi Junior, Fatec Araraquara, romeu.domeniconi@fatec.sp.gov.br
Daisy Eboli, Fatec Araraquara, daisy.eboli@fatec.sp.gov.br

Resumo

O presente artigo, de caráter bibliográfico, pretender averiguar as medidas de segurança da informação essenciais em relação aos dados, no ambiente computacional, que as empresas devem aderir, para garantir a proteção e a segurança de seus ativos, bem como iniciarem o processo de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Para tal, é necessário demonstrar a importância da lei e da conformidade, relação com a segurança da informação, ademais os riscos e sanções pela não conformidade

Palavras-chave: lgpd; dados pessoais; proteção de dados; segurança da informação.

Abstract

This article, of a bibliographic nature, intends to investigate the essential information security measures, which companies must adhere to, to start the process of compliance with the General Law for the Protection of Personal Data (LGPD). To this end, it is necessary to demonstrate the importance of the law and compliance, its relationship with information security, in addition to the risks and sanctions for non-compliance.

Keywords: *lgpd; personal data; data protection; information security.*

1. Introdução

O presente artigo, de caráter bibliográfico, pretender averiguar as medidas de segurança da informação essenciais, no ambiente computacional, que as empresas devem aderir, para garantir a proteção e a segurança de seus ativos, bem como iniciarem o processo de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Para tal, é necessário demonstrar a importância da lei e da conformidade, relação com a segurança da informação, ademais os riscos e sanções pela não conformidade.

A Lei Geral de Proteção de Dados Pessoais (LGPD), é a regulamentação brasileira sobre os dados pessoais, aprovada em 2018, passando a vigorar a partir de 3 de maio de 2021. A LGPD veio para garantir a obrigatoriedade de boas práticas de segurança e privacidade que as empresas devem aplicar sobre os dados pessoais. Para isso, é necessário passar por uma série de adequações envolvendo pessoas, processos e investimentos em segurança da informação.

Conforme Pohlmann (2020) boas práticas de segurança de dados são recomendadas há mais de vinte anos, no entanto como não era uma obrigação legal, apenas uma recomendação, poucas empresas faziam uso dessas recomendações, afinal isso envolve custos com pessoas, tecnologia e treinamento. Agora todas as empresas terão que implementar independentemente do tamanho e custo que isso irá gerar, caso contrário, podem sofrer multas, sanções administrativas ou problemas contratuais.

No contexto tecnológico, a segurança da informação desempenha um papel fundamental para os processos de conformidade, pois fornece boas práticas e controles técnicos essenciais que irão proteger os dados em todo seu ciclo de vida, bem como resguardar as empresas em relação ao tratamento.

Por tanto, explica Baars et. al. (2019) é natural que as organizações estejam empenhadas em proteger melhor as informações, em particular aquelas classificadas como sensíveis, seja fornecendo treinamento adequado a seus colaboradores ou captando profissionais que já possuem treinamento e conscientização no que se refere à Segurança da Informação, bem como, adotar medidas de segurança para protegê-las.

Em relação às teorias abordadas, pretende-se demonstrar os conceitos de segurança da informação, assim como uma breve explicação sobre a lei geral de proteção de dados, e por fim expor controles essenciais para uma boa gestão de segurança da informação.

2. Fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD) e Segurança da Informação

LGPD é a sigla para Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, entrou em vigor em 3 de maio de 2021. Devido à crise mundial causada pela pandemia do novo coronavírus (COVID-19), que impôs diversas restrições, as sanções administrativas passaram a vigorar a partir de agosto de 2021 nos termos da Lei 14.010/2020 (Prescrição e Decadência na Pandemia) (DONDA, 2020). A LGPD é um conjunto de novas diretrizes que visa regulamentar o uso de informações no Brasil, principalmente dados pessoais.

A LGPD é um marco jurídico inédito, atingindo todas as organizações que agora serão obrigadas a adaptar-se a essa nova lei, que tem como objetivo principal, proteger os diretos de liberdade e privacidade dos brasileiros (DONDA, 2020).

de acordo com Art. 1 da Lei nº 13.709 (BRASIL, 2018), “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”.

A legislação é relevante para todas as organizações, públicas ou privadas, pessoa física ou jurídica, que realizam algum tipo de tratamento de dados pessoais, sendo como coleta, armazenamento, tratamento ou processamento (PINHEIRO, 2018 apud CHAGAS; BIAZOTTO, 2022).

Conforme Donda (2020), a lei traz consigo, desafios e oportunidades na área de segurança da informação, pois todas as empresas, independente do porte, precisam buscar entendimento para a conformidade, e conforme Pinheiro (2018, apud CHAGAS E BIAZOTTO), a lei terá um grande impacto para as organizações, principalmente para as pequenas e medias empresas, startups, setor público em especial as que tratam de dados pessoais sensíveis.

2.1. Dados Pessoais

De acordo com Art. 5 da Lei nº 13.709 (BRASIL, 2018) “O dado pessoal é definido como a “informação relacionada a pessoa identificada ou identificável.”

> Dado pessoal é qualquer informação relacionada a um indivíduo, exemplos: nome, sobrenome, data de nascimento, CPF, RG, CNH, carteira de trabalho, passaporte, título de eleitor, sexo, endereço, e-mail, telefone. O nome é um exemplo, de dado de pessoal natural identificada, o e-mail, número de cartão de crédito, endereço IP, cookies, podem ser considerados dados identificáveis, pois permitem de alguma forma identificar o titular (DONDA, 2020).

2.2. Dado pessoal sensível

De acordo com Art. 5 da Lei nº 13.709 (BRASIL, 2018)

> “dado pessoal sensível, é aquele que se refere à 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.”

Conforme Donda (2020), esses dados devem ter uma atenção maior, pois podem gerar atos discriminatórios e lesivos.

2.3. Dado pessoal anonimizado

De acordo com Art. 5 da Lei º 13.709 (BRASIL, 2018), “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.”

Conforme complementa Chagas e Biazotto (2022) dado anonimizado é aquele que não identifica de forma direta ou indireta uma pessoa.

Por fim, Donda (2020) explica que é qualquer dado relativo a um indivíduo e que não o identifica, isso acontece por meio de recursos técnicos que permitem embaralhar as informações, perdendo a possibilidade de associação.

2.4. Tratamento de dados pessoais

O tratamento de dados, conforme o Art. 5 da Lei nº 13.709 (BRASIL, 2018)

> "é 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."

2.5. Sanções administrativas

A lei prevê sanções administrativas em razão da sua infração que, de acordo com Art. 52 da Lei nº 13.709 (BRASIL, 2018)

> "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 – publicação 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;"

2.6. Segurança da Informação

De acordo com a norma ISO 27001 (2013), a segurança da informação é a proteção das informações de uma grande variedade de ameaças com o objetivo de assegurar a continuidade do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio. Conforme explicam Baars et. al. (2021) antes de iniciar uma estratégia de segurança, precisamos saber o que estamos protegendo, e, doque estamos protegendo, a segurança da informação é alcançada por meio da implementação de um conjunto adequado e controles, políticas, processos, procedimentos, estruturas organizacionais, e tais controles devem ser estabelecidos, implementados, monitorados, revisados e melhorados, conforme for necessário, para garantir que os objetivos de segurança da organização sejam atendidos.

2.7. Confidencialidade

De acordo com a norma ISO 27000 (2018), a confidencialidade é a propriedade de que as informações não sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos

sem autorização, complementam Baars et. al. (2021) que a confidencialidade, está relacionada aos limites de quem pode obter acesso à informação, assegurando os níveis necessário de sigilo, evitando a divulgação não autorizada. Uma das formas de garantir esse pilar, é por meio da criptografia de dados, durante o armazenamento e transmissão.

2.8. Integridade

De acordo com a norma ISO 27000 (2018), "a integridade é a propriedade da informação que garante a precisão e completude."

Conforme explicam Baars, et.al. (2021), a integridade refere-se à informação ser correta e consistente com o estado pretendido, e qualquer modificação não autorizada, considera-se uma violação a essa propriedade.

2.9. Disponibilidade

Conforme a norma ISO 27000 (2018), a disponibilidade é a propriedade da informação de ser acessível e utilizável sob demanda por uma entidade autorizada.

> A disponibilidade possui três características: Oportunidade, que diz respeito a informação estar disponível quando necessário. Continuidade: a equipe consegue continuar trabalhando em caso de falha e a Robustez, garantindo que existe a capacidade suficiente para permitir que toda a equipe trabalhe no sistema (BAARS et. al, 2021).

2.10. Controles de segurança

> Controles de segurança são salvaguardas, contramedidas técnicas, administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidades, devido a ameaças agindo sobre a vulnerabilidade. Controles são referenciados o tempo todo na segurança, mas são raramente definidos, tais controles podem ser, controles técnicos, administrativos, de pessoal, preventivos, de detecção e de compensação corretiva, bem como os controles gerais (BAARS et. al, 2021),

De acordo com a norma ISO 27000 (2018), "os controles podem ser definidos como as medidas que estão modificando o risco."

3. Medidas essenciais sobre os dados

3.1. Mapeamento de dados

Na etapa de mapeamento de dados é imprescindível saber onde estão os dados, a tarefa de mapear os dados é feita para ajudar a identificar quais controles de segurança devem ser adotados na proteção dessas informações, e conforme Donda (2022) esse é o mais importante e complexo processo de adequação da LGPD, pois os dados são o ativo-alvo para

o tratamento correto e deve-se saber onde estão localizados, para definir quais mecanismos de proteção no tratamento vamos aplicar, algumas ferramentas de descobrimento e prevenção de perda de dados são recomendadas para auxiliar nesta tarefa, como o *Data Discovery* que permite descobrir dados com determinadas informações, softwares para essa finalidade, identifica, analisa e classifica automaticamente dados contendo informações pessoais como, nomes, endereços, números de telefone, números de contas bancárias etc.

Outra solução bastante adotada pelas empresas explica Donda (2020) é o *Data Loss Prevention (DLP)*, que assim como as ferramentas de *Data Discovery*, ajuda a encontrar os dados com determinadas informações e classificá-las como informações sensíveis.

"Um bom software de *DLP* irá detectar e impedir violações de dados, exfiltração (transferência não autorizada de dados) ou destruição indesejada de dados confidenciais; e deve proteger dados em movimento, em repouso e até mesmo em estações de trabalho de usuários e na nuvem." (DONDA, 2020).

.

3.2. Classificação dos dados

A classificação dos dados, é utilizada para a definição de diferentes níveis de sensibilidade na qual a informação deve ser organizada. Classificar é o ato de atribuir a classificação apropriada, como secreto, confidencial ou público, a uma informação específica (BAARS et. al, 2021).

Conforme explica Donda (2020), a classificação de arquivos pode ser implementada nativamente em ambientes de plataforma Microsoft ou adquirida como software de diversos fabricantes. Geralmente, a classificação vem antes de softwares como o *DLP*, pois a classificação dos dados auxilia na tomada de decisão.

Data Classification é uma importante ferramenta auxiliar na proteção e no rastreamento de informações. Enquanto algumas soluções de *DLP* e *Data Discovery* podem classificar dados, outras podem depender da classificação para a tomada de decisão.

> A classificação pode ser automática (baseada no conteúdo dos arquivos), manual e/ou obrigatória. A classificação usa um label, e tenho certeza de que você já se deparou com dados classificados como *"Confidencial"* ou *"Top Secret",* mas você pode escolher o nome que achar mais interessante (DONDA, 2020).

3.3. Definição da finalidade para o tratamento

Conforme determina o Art. 7 da Lei nº 13.709 (BRASIL, 2018), "o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: seja qual for o método, todos devem respeitar o propósito legítimo da coleta seguindo as bases legais."

3.4. Definição de operadores

Conforme determina o Art. 5 da Lei nº 13.709 (BRASIL, 2018) "operador é a pessoa natural ou jurídica, público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador, já o controlador é a pessoa natural ou jurídica que tomam as decisões sobre

o tratamento de dados pessoais, denominados agentes de tratamento."

Donda (2020) acrescenta que o controlador é a empresa que decide qual provedor de serviços usar, enquanto o operador é o provedor de serviços.

3.5. Definição do ciclo de vida dos dados

Entender e documentar o ciclo de vida dos dados nas empresas é vital para o desenvolvimento do processo de adequação. É acompanhar e entender tudo o que acontece com os dados desde a criação, recebimento, exclusão. Envolvendo, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão distribuição, processamento, arquivamento, armazenamento, eliminação, modificação etc. Identificar o fluxo de tratamento de dados.

Conforme Donda (2020), uma das principais e mais complexas tarefas para a conformidade com a LGPD é a identificação inicial da coleta dos dados para a definição de um plano de gerenciamento de seu ciclo de vida.

3.6. Relatório de impacto a proteção de dados pessoais (RIPD)

Conforme determina o Art. 38 da Lei nº 13.709 (BRASIL, 2018)

> "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

O RIPD é um documento de valor legal e deve detalhar todos os processos de tratamento pelos quais os dados pessoais passam durante o seu ciclo de vida, deve conter os riscos e controles de segurança aplicados.

4. Considerações Finais

Este artigo visou investigar ações relevantes em relação aos dados pessoais, e para tanto, foi necessário demonstrar a importância, relação com a segurança da informação. Em relação às teorias envolvidas, conclui-se que a LGPD trouxe diversas dúvidas para as empresas, principalmente em relação as implementações necessárias sobre os dados, no entanto a lei veio para obrigar boas práticas de segurança, organização e proteção dos dados, que antes eram apenas recomendações e na visão dos gestores, um gasto. Conclui-se finalmente que algumas ações iniciais são de caráter obrigatório, como o mapeamento, classificação, definição da finalidade, operadores, ciclo de vida e por fim gerar um relatório de impacto a proteção de dados são passos essenciais para iniciar o processo de conformidade.

Referências

27001, ABNT/CB-21 PROJETO ABNT NBR ISO/IEC. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão**. [S.l.]: [s.n.], 2013.

27002, ABNT/CB-21 PROJETO ABNT NBR ISO/IEC. **Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação**. [S.l.]: [s.n.], 2013.

27000, ABNT/CB-21 PROJETO ABNT NBR ISO/IEC. **Tecnologia da Informação - Técnicas de Segurança – Visão geral e vocabulário**. [S.l.]: [s.n.], 2018.

BAARS, H. et al. **Fundamentos de Segurança da Informação**. Tradução de Alan de Sá. 3ª. ed. Rio de Janeiro: BRASPORT, 2018.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Planalto**, 2018. Disponivel em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 out. 2022.

CHAGAS, G. A.; BIAZOTTO, L. H. GESTÃO DE TECNOLOGIADA INFORMAÇÃO NA VISÃO DALGPD. **PROSPECTUS**, Itapira, n. v. 3 n. 1, jan. 2022. Disponivel em: https://prospectus.fatecitapira.edu.br/index.php/pst/article/view/57/50.

DONDA, D. **Guia Prático de Implementação da LGPD**. São Paulo: Labrador, 2020.

POHLMANN, S. Sobre cintos de segurança, LGPD, pequenas empresas e interpretação. **SERPRO**, 2020. Disponivel em: <https://www.serpro.gov.br/lgpd/noticias/2020/cinto-seguranca-lgpd-pequenas-empresas-interpretacao>. Acesso em: 01 nov. 2020.