risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 23/10/2020
Aceitação/Acceptance: 13/12/2020

Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem

Márcio Aurélio de Souza Fernandes[1], Fernando Gonçalves de Oliveira[2], Felipe Silva Ferraz[3], Daniel Alves da Silva[4], Edna Dias Canedo[5], Rafael Timóteo de Sousa Jr[6]

marcio.fernandes@redes.unb.br; fernando.oliveira@redes.unb.br; fsf@cesar.org.br; daniel.alves@redes.unb.br; ednacanedo@unb.br; desousa@unb.br

[1] Universidade de Brasília – UNB, Campus Universitário Darcy Ribeiro, Brasília -DF, CEP: 70910-900, Brasil

[2] CESAR School, Cais do Apolo, 77, Bairro Recife – Recife-PE, CEP:50030-390, Brasil

Pages: 374-385

Resumo: Este trabalho tem por objetivo analisar os impactos causados pela Lei Geral de Proteção de Dados (LGPD) no uso da computação em nuvem. O estudo traz o conceito e utilização da computação em nuvem, reflexão sobre a LGPD no ordenamento jurídico atual e análise dos impactos que causa nà computação em nuvem. A lei foi publicada através da Medida Provisória nº 869, em 2712/2018, a fim de assegurar os direitos do usuário. A metodologia para a elaboração desse trabalho foi revisão bibliográfica, através de consultas em livros, revistas, periódicos, artigos, arquivos e sites relacionados ao tema. Conclui-se que a lei trouxe alguns desafios, porém, entende-se sua importancia, uma vez que assegura a proteção de dados de pessoas físicas ou jurídicas, além de trazer sanções civis e penais em caso de divulgação de dados pelas empresas.

Palavras-chave: LGPD; Computação em nuvem; Segurança de dados; armazenamento de dados; Direito do Usuário.

Impacts of the Brazilian Data Protection Law (LGPD) on the use of Cloud Computing

Abstract: This work aims to analyze the impacts caused by the General Data Protection Law (LGPD) on the use of cloud computing. The study brings the concept and use of cloud computing, reflection on LGPD in the current legal system and analysis of the impacts it causes on cloud computing. The law was published through Provisional Measure No. 869, on 2712/2018, in order to ensure the rights of the user. The methodology for preparing this work was a bibliographic review, through consultations in books, magazines, periodicals, articles, files and websites related to the theme. It is concluded that the law brought some challenges, however, its importance is understood, since it ensures the protection of data of individuals or legal entities, in addition to bringing civil and criminal sanctions in case of data disclosure by companies.

Keywords: LGPD; Cloud computing; Data security; Data storage; User Right.

1. Introdução

Cloud computing ou computação em nuvem é a utilização de memória, dispositivos de armazenamento, compartilhamento de recursos, processamento e servidores interligados por meio da internet.

O *National Institute of Standards and Technology* (NIT), define computação em nuvem como uma tecnologia que permite gerenciar recursos compartilhados tais como: servidores, redes, sistemas de armazeamento e serviços (Mell & Grance, 2011).

Com a evolução da ciência, sobretudo na área tecnológica, grande parte da população vem tendo acesso às tecnologias e aos dados disponíveis através da nuvem e de bancos de dados virtuais. Consequentemente, tem crescido a preocupação acerca da segurança e privacidade desses dados tanto por parte dos usuários quanto das organizações.

O armazenamento de dados na nuvem (ou disco virtual) tem a função de guardar e compartilhar arquivos e/ou diretórios que contenham dados de maneira segura, a fim de evitar a perda destes por roubo ou softwares maliciosos como os vírus (Galan, 2019).

A fim de assegurar os direitos do usuário, elaborou-se a Lei nº 13709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD) publicada através da Medida Provisória nº 869, de 27 de dezembro de 2018. A LGPD trouxe inovações relevantes a respeito da temática do armazenamento em nuvem, além de trazer disposições sobre a proteção de dados pessoais e alterações no texto da Lei nº 12.965 de 23 de abril de 2014, considerada como o Marco Civil da Internet.

A elaboração desta lei foi baseada nos direitos fundamentais de liberdade e de privacidade, como a livre iniciativa e o desenvolvimento econômico e tecnológico do país. Ela traz alguns dos requisitos quanto a sua adequação que são operações de tratamento realizadas em território nacional; oferta de bens, serviços e tratamentos de dados em território nacional e coleta de dados pessoais em território nacional (Ezidio, 2019; Somadossi, 2019).

Nesse contexto, o presente artigo tem como objetivo analisar os impactos causados pela LGPD no tocante ao uso da computação em nuvem para o armazenamento de dados. Para alcançar esse objetivo, o estudo trará uma visão geral sobre o conceito de computação em nuvem, o panorama sobre uso e o armazenamento de dados na nuvem, reflexão sobre a lei de proteção de dados vigente no ordenamento jurídico atual e uma análise dos impactos da nova LGPD na computação em nuvem.

Posto isso, o presente estudo se propõe a responder a seguinte questão de pesquisa: quais os impactos causados pela Lei Geral de Proteção de Dados na Computação em Nuvem? Tendo como objetivo geral analisar as normas relativas à proteção de dados, os objetivos específicos são: conceituar a computação em nuvem e o seu uso para o armazenamento de dados, refletir sobre a LGPD vigente no ordenamento jurídico atual e analisar os impactos que a LGPD traz para a computação em nuvem.

O estudo se justifica diante da importância que o tema tem para toda a sociedade, visto que é essencial que as informações e os dados de todo seres humanos devem estar protegidos na nuvem ou na rede, pois, todos tem o direito, amparados pela legislação, à privacidade de suas informações, seja pessoa física ou jurídica.

O presente trabalho está organizado como descrito a seguir. A seção 1 traz uma visão geral acerca da metodologia utilizada na revisão bibliográfica. A Seção 2 apresenta uma definição e características do modelo de computação em nuvem, conceitos sobre segurança no armazenamento de dados na nuvem, além de abordar a Lei Geral de Proteção de Dados e seus impactos na computação em nuvem. A Seção 3 trata da análise dos dados e discussão dos resultados, sumarizando descobertas relevantes de trabalhos já publicados acerca do tema. Por fim, a Seção 4, traz as conclusões a respeito do estudo realizado.

1.1. Metodologia

A metodologia utilizada para elaboração do estudo foi baseada em revisão bibliográfica, com consultas em livros, revistas, periódicos, artigos, arquivos e sites relacionados ao tema abordado.

Boccato (2006, p. 266) diz que a pesquisa bibliográfica é aquela que busca a resolução de um problema (hipótese) por meio de referências teóricas publicadas, analisando e discutindo as várias contribuições científicas.

Utilizaram-se como critério de inclusão trabalhos sobre o tema da LGPD e seus impactos na computação em nuvem publicados entre os anos de 2009 a 2020.

1.2. Contribuições da Metodologia Proposta

Por meio do estudo realizado, espera-se que os resultados contribuam para apresentar os desafios que serão enfrentados com a nova Lei Geral de Proteção de Dados e suas consequências ante a organizações, sejam elas públicas ou privadas, no que tange a segurança e proteção de dados, avaliando os itens a seguir:

1. principais riscos às empresas que armazenam seus dados em nuvem;
2. penalidades e sanções por descumprimento de normas da nova lei;
3. principais itens contemplados na nova lei no quesito armazenamento em nuvem;
4. soluções, métodos e ferramentas de segurança.

2. Estado da arte

Nesta seção serão apresentados conceitos básicos acerca dos principais tópicos objetos de estudo deste trabalho, a fim proporcionar uma maior compreensão dos temas abordados por todo o texto.

2.1. Computação em Nuvem

Pode-se considerar que as definições para computação em nuvem envolvem uma série de conceitos computacionais. Segundo Pinheiro (2016), a computação em nuvem é um

modelo que está sendo cada vez mais utilizado, proporcionando acesso compartilhado e configurável, seguro e facilitando a gestão dos recursos de Tecnologia da Informação com mínimo esforço. Contudo, cada parte desta infraestrutura é provida como serviços normalmente alocados em *data centers*, utilizando hardware compartilhado para computação e armazenamento.

2.2. Definição, Características e Modelos de Computação em Nuvem

A computação em nuvem é um modelo para permitir acesso conveniente à rede sob demanda para um conjunto compartilhado de recursos de computação configuráveis que podem ser rapidamente provisionados e lançados com esforço mínimo de gerenciamento ou interação do provedor de serviços (Almubadde & Elmogy, 2016).

Os modelos de implantação da computação em nuvem podem ser divididos em: pública, privada, comunitária e híbrida (Mell & Grance, 2011). Abaixo, na Figura 1, Ziani (2019) ilustra os quatro modelos de implantação de nuvem.

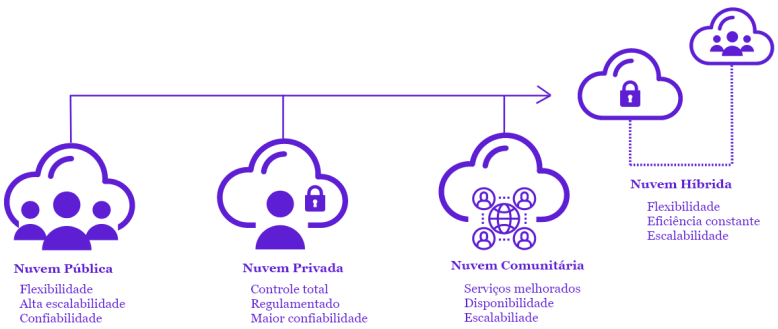

Figura 1 – Modelos de implnação de nuvem. Fonte: Ziani (2019) – Modelo adaptado pelo autor

Um dos termos mais utilizados em conjunto com computação em nuvem são os *Software as a Service* (SaaS), ou seja, softwares disponibilizados na "grande rede" através de serviços que normalmente são contratados pelas empresas para os mais diversos fins. Isso permite que as organizações dispensem altos investimentos na aquisição e manutenção de espaços físicos para comportar *data centers* próprios, a fim de armazenar e fornecer acesso aos seus recursos com a velocidade e disponibilidade que demandam.

Após um estudo onde foram consideradas várias definições distintas para o conceito de computação em nuvem, Vaquero *et al.* (2008) chegaram a conclusão de que as nuvens são grandes repositórios de recursos virtualizados, tais como hardware, plataformas de desenvolvimento e software, que são facilmente acessíveis.

2.3. Recursos de Computação em Nuvem e Armazenamento

O armazenamento em nuvem possibilita que empresas que precisam de infraestrutura de TI tenham a opção de adquirir somente as soluções pontuais de que necessitam para que seu negócio possa funcionar. Os dados armazenados em servidores em nuvem

podem ser acessados de qualquer lugar, desde que o usuário tenha acesso à internet no dispositivo utilizado (Moreira, 2017).

Sendo assim, estes serviços são ofertados para as empresas por meio de pacotes que buscam solucionar tais necessidades, disponibilizando estruturas ágeis e flexíveis no armazenamento e acesso a estes dados. Destacaremos alguns desses recursos a seguir.

Os primeiros deles são a elasticidade e escalonamento. De acordo com Buyya (2011), a computação em nuvem proporciona a ilusão de recursos computacionais infinitos e disponíveis para o uso. Portanto, os usuários têm a expectativa de que nuvem seja capaz de fornecer os recursos rapidamente, em qualquer quantidade e a qualquer momento. É esperado que recursos adicionais sejam adicionados ou removidos, possivelmente de forma automática, de acordo com o aumento ou diminuição da demanda.

O *self-service* (autoatendimento) é outro benefício importante. Segundo Buyya (2011), o consumidor de serviços da computação em nuvem espera adquirir recursos computacionais instantâneamente de acordo com suas necessidades. Para suportar este tipo de expectativa, as nuvens devem permitir o acesso em autoatendimento para que os usuários possam solicitar, personalizar, pagar e usar os serviços desejados sem intervenção humana.

Ainda segundo Buyya (2011), o faturamento e medição por uso é outra questão importante sobre os serviços oferecidos na nuvem com relação ao método/sistema de cobrança por utilização. Ou seja, uma vez que o usuário tem a opção de requisitar e utilizar somente a quantidade de recursos e serviços que ele julgar necessário, os serviços devem ser precificados com base em um uso de baixa duração, como por exemplo, medido em horas de uso.

Por esta razão, as nuvens devem implementar recursos que garantam um comércio eficiente de serviços, tais como tarifação adequada, contabilidade, faturamento, monitoramento e otimização de uso. Esta medição de uso dos recursos deve ser feita de forma automática, alinhada com os diferentes tipos de serviços oferecidos (armazenamento, processamento e largura de banda) e prontamente reportada, a fim de garantir uma maior transparência comercial.

Mell & Grance (2011) apresentam outros dois recursos importantes com relação aos serviços em nuvem: o amplo acesso à rede e a customização. Com relação ao primeiro, os recursos devem estar disponíveis através da rede de modo que possam ser acessados por meios convencionais que permitam a utilização dos mesmos por plataformas heterogêneas, como *smartphones*, *laptops*, PDAs, entre outros. Entendemos que todo e qualquer dispositivo que se conecte de alguma forma à internet, deverá ter totais condições de acessar os dados armazenados/providos na nuvem, aumentando o leque de opções e não se limitando apenas a computadores e derivados.

Com relação à customização, no atendimento a múltiplos usuários verifica-se a grande disparidade entre as necessidades dos mesmos, tornando essencial a capacidade de personalização dos recursos na nuvem, desde os serviços de infraestrutura, à serviços de plataforma e de software (Mell & Grance, 2011).

2.4. Segurança no Armazenamento de Dados na Nuvem

A segurança na nuvem é um tema bastante delicado e fruto de divergência na literatura. Há autores que defendem a segurança dos dados na nuvem, enquanto outros a enxergam com certo receio. Os pessimistas justificam sua desconfiança em qualquer incidente que venha a comprovar os riscos das aplicações em nuvem.

Conforme artigo publicado por Araújo (2020), a segurança cibernética não pode ser mais encarada como uma decisão que está à parte das inovações e operações do dia a dia do negócio. Para isso, no entanto, é preciso que as companhias avancem em seus planos de segurança, entendendo a LGPD e outras regras de conformidade digital.

A computação em nuvem ainda tem problemas por falta de uma retaguarda legal, de modelos contratuais e de controles adequados. O modelo também falha por dificultar processos de auditoria de segurança e de regulamentação dos dados para *backups* e das informações hospedadas na nuvem. Interfaces para a integração adequada entre os serviços na nuvem e aqueles hospedados nas empresas completam a lista de deficiências deste modelo de computação.

De acordo com CIO (2010), "os gestores de TI, no entanto, precisam analisar o projeto de adoção da computação em nuvem como qualquer outra iniciativa ligada à área de tecnologia. Isso exige um processo de avaliação dos riscos e dos benefícios, um plano bem estruturado para implementação e uma estratégia de aperfeiçoamento contínuo". Neste caso, cabe a cada profissional/organização tentar equilibrar essa equação da melhor maneira.

Dentre os diversos riscos à privacidade da informação estão: a invasão por meio de técnicas de ataque e o vazamento de informações, que podem ocorrer por uma falha humana ou de alguma ferramenta.

No tocante à segurança e proteção de dados pessoais, podemos destacar outros três riscos: pessoas, metodologias e ferramentas de proteção.

Em relação às pessoas, a engenharia social ainda é uma forma muito eficiente de colher informações importantes. Nela, indivíduos mal-intencionados se valem de conversas informais para extrair informações acerca do nível de segurança, metodologias adotadas para implementar e garantir a privacidade dos dados e/ou até mesmo as ferramentas utilizadas para a segurança das aplicações.

No que tange as metodologias de segurança da informação, é importante ressaltar que não há uma fórmula mágica ou receita infalível. Ainda assim, é possível, por meio de estudos e implementações de rotinas básicas, garantir que a informação esteja 99% segura. Algumas boas práticas podem minimizar os riscos de uma empresa ter seus dados expostos e/ou roubados e tais práticas devem ser adotadas não somente pelos profissionais da área de TI, mas por todos da organização. A organização, por sua vez, deve assegurar que os cuidados com a segurança sejam culturalmente difundidos no dia a dia.

O profissional de TSI – Tecnologia em Segurança da Informação – é o responsável por criar essas rotinas e/ou produzir o material que os demais profissionais da corporação

terão como base para implementação de suas atividades. A qualificação desse profissional deverá ser comprovada, ou seja, ele deverá possuir certificações que comprovem seus conhecimentos, básicos e avançados, para a referida atividade.

Entre as diversas ramificações da segurança da informação, há algumas que possuem certificações específicas, como: avaliação de segurança de sistemas; análise de ataques ou crimes virtuais; avaliação e controle de níveis de acessos; e análise do nível de segurança da informação.

Na Figura 2, é possível verificar as principais certificações para o especialista em proteção de dados.

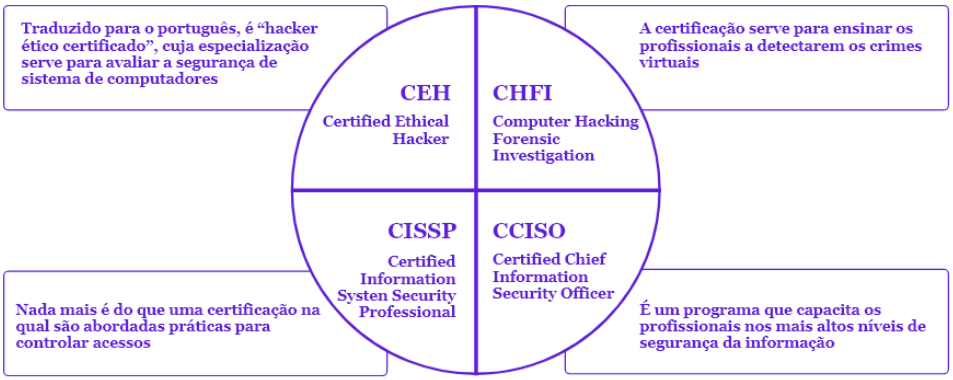

Figura 2 – Principais certificações para o especialista em proteção de dados.
Fonte: Elaborado pelo autor.

Outra técnica de segurança que deve ser adotada é uma rotina de *backup*s, que embora não iniba ou minimize ataques com intenção de roubo de informações, reduz os danos à informações que foram acessadas, mas não foram perdidas. Segundo informações da empresa especialista em armazenamento em nuvem "*backupgarantido*", há 6 ataques muito praticados por *hackers*, são eles: DDOS *attack*; *port scanning attack*; *ransomware*; cavalo de troia; ataque de força bruta; cryptojacking.

O DPO (*Data Protection Officer*) é responsável pela segurança da corporação, cabendo a ele descrever toda política de segurança, desde a criação de usuários de rede até as ferramentas de detecção de tentativas de invasão. Isto é um grande desafio, uma vez que não temos uma cultura de seguir o que foi escrito, ou seja, o que vemos na prática são usuários que instalam suas próprias ferramentas de proteção (*shadow it*). Segundo o site "*securityreport*", apenas 10% das empresas possuem seu sistema de proteção de nuvem homologado.

Com a informação sendo um ativo precioso e necessário em tempo integral, o uso crescente de dispositivos móveis se tornou uma grande ameaça à privacidade, o termo "BYOD - *Bring Your Own Device*" tornou-se muito conhecido. Mas a questão é: como se proteger para minimizar os riscos com essa tendência? Criar uma política de uso para

os colaboradores da empresa, seja ela pública ou privada, iniciando com a cultura de informar sobre os riscos de redes sociais, *links* recebidos, uso de *websites* e aplicativos, pode ser um bom começo. O uso de aplicativos de segurança de acesso é uma ótima ferramenta, associada a tantas outras como: identificação de redes desprotegidas; uso de virtualização; bloqueio de armazenamento interno; soluções de criptografia; ferramentas de remoção total de conteúdo; logins e senhas em caso de perda ou roubo do dispositivo, entre outras.

2.5. A LGPD: Implicações, regras e o cenário atual

Segundo a Lei nº 13.709 (Brasil, 2018), que foi sancionada no dia 14 de agosto de 2018, e entra em vigor a partir de agosto de 2020, a LGPD (Lei Geral de Proteção de Dados) tem como objetivo principal, garantir a transparência no uso dos dados de pessoas físicas sob qualquer meio. Esta lei substitui a então Lei 12.965 de 2014 (Brasil, 2014).

A Lei nº 13.709 (Brasil, 2018) baseou-se na GDPR (Regulamento Geral de Proteção de Dados), de base européia, revisou como as empresas processam e tratam dados. Desta forma, o Brasil está agora coberto pelas regras mais fortes de proteção de dados do mundo. O Regulamento Geral de Proteção de Dados (GDPR) mutuamente acordado entrou em vigor em agosto de 2020 no Brasil e foi projetado para modernizar as leis que protegem as informações pessoais dos indivíduos.

Antes da LGPD começar a ser aplicada, as regras anteriores de proteção de dados em toda a Europa (base para a lei no Brasil), foram criadas durante os anos 90 e buscavam acompanhar as rápidas mudanças tecnológicas. A LGPD altera como as empresas e organizações do setor público podem lidar com as informações de seus clientes. Também aumenta os direitos dos indivíduos e dá a eles maior controle sobre suas informações (CENP, 2019).

Em suma, todas as organizações e empresas que são controladoras ou processadores de dados pessoais serão cobertas pela LGPD. Ou seja, tanto os dados pessoais públicos quanto os confidenciais serão cobertos pela LGPD. Dados pessoais, uma categoria complexa de informações, geralmente dizem respeito a uma informação que pode ser usada para identificar uma pessoa. Como exemplo temos um nome, endereço, data de nascimento, CPF, endereço IP, etc. Os dados pessoais sensíveis englobam dados genéticos, informações sobre visões religiosas e políticas, orientação sexual e muito mais (CENP, 2019).

As empresas cobertas pelo RGPD – Regulamento Geral sobre a Proteção de Dados – são responsáveis pelo tratamento dessas informações pessoais dos indivíduos. Isso pode incluir políticas de proteção de dados, avaliações de impacto na proteção destes e documentos relevantes sobre como tais dados são processados.

Nos últimos anos, houve uma série de violações massivas de dados, incluindo milhões de detalhes de contas do Yahoo, LinkedIn e MySpace. De acordo com a LGPD, a destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais devem ser relatados ao regulador de proteção de dados de um país, acarretando em possíveis impactos negativos, que podem incluir perdas financeiras, violação de confidencialidade, danos à reputação, entre outros.

Além disso, as empresas que têm monitoramento regular e sistemático de indivíduos em larga escala ou processam muitos dados pessoais confidenciais precisam contratar um diretor de proteção de dados (DPO). Para muitas organizações cobertas pela LGPD, isso pode significar ter que contratar um novo membro da equipe – embora empresas maiores e autoridades públicas possam já ter pessoas nessa função.

Também é necessário que as empresas obtenham consentimento para processar dados em algumas situações. Quando uma organização depende do consentimento para usar legalmente as informações de uma pessoa, elas precisam explicar claramente que tal direito está sendo concedido e que deve haver uma aceitação positiva para que possa o fazer.

3. Análise dos dados e discussão dos resultados

A Política de Segurança da Informação e Proteção de Dados define como as organizações e seus parceiros, fornecedores, etc., gerenciam e fornecem segurança entre si, e às informações confidenciais de seus clientes dentro dos limites do desenvolvimento de software de agências autorizadas para o recrutamento e do processamento e hospedagem de informações pessoais em empresas que buscam através da adequação das diretrizes baseadas na Lei nº 13.709 de 2018.

Ressalta-se que algumas empresas largaram na frente e já se adequaram a esta nova realidade. Apesar de, no Brasil, a lei passar a vigorar apenas em agosto de 2020, na Europa a lei vigora a mais de 2 anos e por isso já existem empresas especializadas em políticas de segurança adequadas a lei, que apoiam e cumprem totalmente os princípios do Regulamento Geral de Proteção de Dados (GDPR), que estão resumidos abaixo:

De acordo com Guaracho (2018), tais políticas devem contemplar ações baseadas em dados pessoais, onde os mesmos devem ser:

1. processados de forma legal, justa e transparente em relação ao titular dos dados (legalidade, justiça transparência);
2. coletados para finalidades especificadas, explícitas e legítimas e não processados de maneira que seja incompatível com esses fins (limitação de finalidade);
3. adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados (minimização de dados);
4. precisos e, quando necessário, atualizados; (precisão);
5. mantidos em uma forma que permita a identificação dos titulares dos dados por um período não superior ao necessário para os fins os quais os dados pessoais são processados (limitação de armazenamento);
6. processados de maneira a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais adequadas (integridade e confidencialidade).

Ter uma política de segurança da informação é uma prática recomendada do governo e dos setores organizacionais de empresas que buscam tal competência sobre a LGPD.

Ajuda a evitar eventos acidentais ou maliciosos que resultem no acesso e/ou divulgação não autorizados de arquivos eletrônicos, documentos em papel e serviços online.

As organizações precisam estar comprometidas em manter e desenvolver uma infraestrutura de sistemas de informação, com um nível adequado de segurança e proteção de dados. É preciso que os conselhos administrativos das organizações, se comprometam com o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e aprimoramento do gerenciamento de sistemas de informação (Guaracho, 2018).

O compromisso das organizações, perante a Lei 13.709 inclui atividades como garantir que os recursos adequados estejam disponíveis para trabalhar nesses sistemas e que todos os funcionários afetados tenham o treinamento, a conscientização e a competência adequados (Guaracho, 2018).

Assim sendo, Filho (2018), retrata que as políticas de segurança baseadas nas diretrizes da Lei, precisam:

1. trazer à atenção de todo pessoal à necessidade de melhorar e manter a segurança dos sistemas de informação e aconselhar os gerentes sobre a abordagem adotada para alcançar o nível apropriado de segurança;
2. trazer à atenção de todos os gerentes e funcionários suas responsabilidades de acordo com os requisitos da legislação, incluindo a própria legislação e a orientação sobre proteção dos dados e direitos humanos, bem como a importância de garantir a confidencialidade dos dados pessoais e sensíveis.
3. garantir que a empresa cumpra a legislação vigente e as diretivas da lei e cumpra suas normas, obrigações e observe padrões de boas práticas.

O Diretor de Segurança da Informação é o proprietário responsável da Política de Segurança da Informação e Proteção de Dados e é responsável pela sua manutenção e revisão em conjunto com o Diretor de Proteção de Dados. Qualquer exceção à Política de Segurança da Informação e Proteção de Dados deve ser avaliada e aprovada pelo Diretor de Segurança da Informação. A delegação de responsabilidades é descrita em detalhes nos Procedimentos de Gerenciamento de Segurança da Informação (Filho, 2018).

4. Conclusões

Apesar dos requisitos em constante mudança do mundo dos negócios, com novos direitos para os indivíduos e notícias recentes relacionadas a violações da segurança de dados, não há indicativos de que o Regulamento Geral de Proteção de Dados (GDPR) tenha sérias implicações nos provedores de serviços em nuvem, processos e armazenamento de dados pessoais.

Os provedores de nuvem precisam integrar essa lei em seus processos e fazer retificações de acordo com as novas disposições. A legislação de proteção de dados existente antes da aplicação da lei tornou-se obsoleta, uma vez que não atende aos novos desenvolvimentos em termos de alto uso de redes sociais, crescimento exponencial de dados e uso em larga escala da tecnologia de computação em nuvem.

Atualmente, o uso da computação em nuvem é parte integrante de uma empresa moderna, pois pode oferecer vantagem competitiva reduzindo custos e permitindo que pequenas empresas concorram com as grandesmultinacionais sem altos custos de inicialização. É fato que mais de 80% dos novos aplicativos corporativos comerciais usarão a nuvem como plataforma até 2025. A comissão da União Européia (EU), onde tudo começou, entende a importância da computação em nuvem e deseja adaptar políticas amigáveis à nuvem de modo que possam gerar receitas e contribuir para o PIB.

Isso resultará em um crescimento substancial no mercado de trabalho, produzindo cerca de 3,8 milhões de empregos para diretamente ligados à computação em nuvem, com políticas e leis adequadas que fornecem ambiente adequado para este mercado. O principal obstáculo ao uso da computação em nuvem é a legislação de proteção de dados. As leis existentes não eram abrangentes, uma vez que ofereciam aos Estados a opção de implementar apenas padrões mínimos que, devido a isso, resultaram em padrões inadequados de proteção de dados e criaram mais incerteza na adoção da tecnologia em nuvem.

A implicação do GDPR, que é a base central da LGPD, é abrangente e os provedores de nuvem precisam alterar e modificar seus serviços, processos e contratos para atender aos requisitos da legislação. O documento de pesquisa inicialmente discute a jornada de transformação e as causas subjacentes para aprimorar a Diretiva de Proteção de Dados (DPD) em GDPR.

Desta forma, o presente trabalho destacou as disposições do GDPR e seu impacto nos provedores de serviços em nuvem, seguido por uma comparação entre a atual Diretiva de Proteção de Dados e as alterações no GDPR. O documento de pesquisa resumiu o impacto legal e geral do GDPR no Provedor de Serviços em Nuvem (CSP) e como isso afetará os processos e procedimentos durante o processamento ou armazenamento de dados.

Agradecimentos

Os autores agradecem o apoio das Agências Brasileiras de Pesquisa, Desenvolvimento e Inovação CAPES (concessão 23038.007604/2014-69 FORTE), CNPq (concessão 465741/2014-2 INCT em Segurança Cibernética) e a FAP-DF (concessões 0193.001366/2016 UIoT e 0193.001365/2016 SSDDC), bem como as cooperações com o Ministério da Economia (TED DIPLA 005/2016), Advocacia Geral da União (TED AGU 697.935/2019) e a CESAR School.

Referências

Araújo, G. (2020). Os impatos da LGPD para as ações de Segurança da Informação. Disponível em: https://cio.com.br/os-impactos-da-lgpd-para-as-acoes-de-seguranca-da-informacao/.

Boccato, V. R. C. (2006). Metodologia da pesquisa bibliográfica na área odontológica e o artigo científico como forma de comunicação. Rev. Odontol. Univ. Cidade São Paulo, São Paulo, 18(3), 265-274.

Brasil. (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União (23 abr. 2014).

Brasil. (2018). Lei nº 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil (14 ago. 2018).

Buyya, R., Broberg, J., & Goscinski, A. M. (Eds.). (2010). Cloud computing: Principles and paradigms (Vol. 87). John Wiley & Sons.

CENP. (2019). Lei geral de proteção de dados pessoais: perguntas e respostas sobre os impactos da nova regulamentação no setor de publicidade. Disponível em: https://www.cenp.com.br/downloads/LGPD.pdf.

CIO. (2010). O que as empresas precisam saber sobre cloud computing. Disponível em: https://cio.com.br/gestao/o-que-as-empresas-precisam-saber-sobre-cloud-computing/.

Ezidio, E. (2019). LGPD: Como a nova lei pode impactar o uso da cloud pelas empresas. SEGS. Disponível em: https://www.segs.com.br/info-ti/198857-lgpd-como-a-nova-lei-pode-impactar-o-uso-da-cloud-pelas-empresas.

Galan, A. (2019). Entenda como funciona o armazenamento de dados na nuvem. RENOVAMIDIA. Disponível em: https://renovamidia.com.br/entenda-como-funciona-o-armazenamento-de-dados-na-nuvem.

Guaracho, R. F. (2018). A privacidade, as novas regras de proteção de dados e o futuro digital. Revista Conceito Jurídico. Disponível em: http://www.gandramartins.adv.br/project/ives-gandra/public/uploads/2019/02/21/22f3605085417p.pdf.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Moreira, E. (2017). IAAS, PAAS, SAAS: conheça os modelos fundamentais de Cloud Computing. Disponível em: https://introduc eti.com.br/blog/iaas-paas-saas-conheca-os-modelos-fundamentais-de-cloud-computing/.

Pinheiro, A. (2016). Arquitetura baseada em confiança para a verificação da integridade de arquivos em nuvens computacionais.

Reinaldo Filho, D. (2018, 21 julho). Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados. *Revista Jus Navigandi*, Teresina (ISSN 1518-4862, Ano 23, nº 5498).

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition.

Ziani, A., & Medouri, A. (2018). Security Requirements for Cloud Environments: The Public Cloud Case. In The Proceedings of the Third International Conference on Smart City Applications (pp. 757-770). Springer, Cham.