REVISTA
MATO GROSSENSE DE
GESTÃO, INOVAÇÃO E
COMUNICAÇÃO
ISSN: 2965-0909
REVISTA CIENTÍFICA REMAGIC - VOLUME 3 - NÚMERO 2 - NOVEMBRO DE 2024.

GESTÃO DA PRIVACIDADE DE DADOS NAS ORGANIZAÇÕES: CONFORMIDADE COM AS LEIS DE PROTEÇÃO DE DADOS

PAMELA BOSING VALDAMERI[1]
WILLIAN RODRIGO DATSCH[2]

RESUMO: O presente trabalho possui como temática a gestão da privacidade de dados nas organizações, com foco na conformidade com as leis de proteção de dados, destacar a importância deste tema, impulsionada pelo avanço tecnológico e pela conscientização sobre os riscos associados à coleta, armazenamento e processamento de informações pessoais. O direito à privacidade é discutido em relação à legislação e aos direitos humanos e enfatizado a necessidade de regulamentações específicas para proteger os indivíduos. A proposta é a análise de como as organizações implementam a gestão desses dados, como alcançam melhorias na proteção do mesmo, gestão de incidentes de segurança e conformidade com regulamentações. Além de investigar como a conformidade é gerenciada e avaliação do impacto nas práticas de privacidade. É destacado lacunas existentes na pesquisa atual, como a falta de abordagem sobre desafios a longo prazo da regulamentação, a deficiência de pesquisas qualitativas aprofundadas e a necessidade de considerar as diferenças nas leis de proteção de dados entre jurisdições. A confiança do consumidor é ressaltada como um resultado desejado. Também, são apresentados os princípios e requisitos exigidos nessas leis, como transparência, segurança, responsabilidade e prestação de contas. A necessidade de adaptação contínua às mudanças nessas leis é enfatizada, juntamente com a importância de avaliações de impacto sobre a privacidade e medidas de segurança.
PALAVRAS-CHAVE: GDPR. LGPD. Privacidade.

DATA PRIVACY MANAGEMENT IN ORGANIZATIONS: COMPLIANCE WITH DATA PROTECTION LAWS

ABSTRACT: The present work focuses on data privacy management in organizations, with an emphasis on compliance with data protection laws. It highlights the importance of this topic, driven by technological advancements and increasing awareness of the risks associated with the collection, storage, and processing of personal information. The right to privacy is discussed in relation to legislation and human rights, emphasizing the need for specific regulations to protect individuals. The proposal includes an analysis of how organizations implement data management, achieve improvements in data protection, manage security incidents, and ensure regulatory compliance. It also investigates how compliance is managed and assesses the impact on privacy practices. The work highlights gaps in current research, such as the lack of long-term regulatory challenges, the deficiency of in-depth qualitative studies, and the need to consider differences in data protection laws across jurisdictions. Consumer trust is emphasized as a desired outcome. Additionally, the principles and requirements demanded by these laws, such as transparency, security, accountability, and responsibility, are presented. The need for continuous adaptation to changes in these laws is emphasized, along with the importance of privacy impact assessments and security measures.

[1]Graduada em Administração. Curso de Administração. Faculdade Fasipe. Endereço eletrônico: pamelabosingvaldameri6@gmail.com
[2] Professor Especialista em Pedagogia Empresarial. Curso de Administração, Faculdade Fasipe. Endereço eletrônico: willian_datsch@hotmail.com

KEYWORDS: GDPR. LGPD. Privacy.

1. INTRODUÇÃO

A gestão da privacidade e segurança de dados nas organizações ganhou destaque nas últimas décadas devido ao rápido avanço da tecnologia da informação e ao aumento na coleta, armazenamento e processamento de informações pessoais, expressando riscos significativos. A conscientização sobre a privacidade de dados e a necessidade de regulamentações específicas para proteger os direitos das pessoas remontavam a vários anos.

O conceito de privacidade, conforme definido pelo Dicionário Escolar da Língua Portuguesa da Academia Brasileira de Letras, referia-se à condição do que dizia respeito unicamente ao indivíduo. A gestão da privacidade de dados nas organizações tornou-se uma área de extrema importância no cenário atual, à medida que as informações pessoais se tornaram um ativo valioso e sensível.

A Declaração Universal dos Direitos Humanos (DUDH), promulgada em 1948, constituiu o direito do ser humano à privacidade, estabelecendo que ninguém seria sujeito à interferência em sua vida privada, família, lar ou correspondência, nem a ataques à sua honra e reputação (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 1948).

Doneda (2006) destacou que a evolução do conceito de privacidade enfatizava elementos relacionados a diversas necessidades, como a busca por igualdade, liberdade de escolha e o desejo de evitar discriminação. O autor salientou a mudança crucial na concepção da privacidade para a proteção de dados pessoais, onde o foco do direito deixou de ser o sentimento abstrato e difícil de mensurar da privacidade para tornar-se os dados pessoais sob controle de terceiros.

A implementação do GDPR (Regulamento Geral sobre a Proteção de Dados) teve um impacto profundo nas práticas de gestão de dados em organizações em todo o mundo. Desde então, a conscientização sobre a importância da privacidade de dados e a conformidade com regulamentações de proteção de dados cresceu significativamente. A gestão da privacidade de dados nas organizações tornou-se uma prioridade essencial para garantir a proteção dos direitos das pessoas e a confiança do consumidor.

A conformidade com leis de proteção de dados, como o GDPR da União Europeia, tornou-se crucial para garantir que as organizações coletassem, armazenassem e processassem dados pessoais de maneira ética e legal. A pesquisa nessa área poderia ajudar a avaliar a eficácia das organizações na conformidade, evitar penalidades financeiras e promover práticas de segurança mais rigorosas.

Em um mundo onde muitas organizações terceirizavam serviços ou tinham parcerias com terceiros, entender como essas práticas impactavam na proteção de dados e a conformidade com as leis era fundamental para garantir que a privacidade e segurança se estendessem a todos os aspectos das operações. A pesquisa poderia influenciar na confiança do consumidor, vital para o sucesso de qualquer organização.

Apesar do crescimento na pesquisa sobre segurança de dados, lacunas persistiam, especialmente em relação aos desafios apresentados por novas tecnologias como inteligência artificial e Internet das Coisas. Faltavam estudos sobre os impactos a longo prazo das regulamentações e pesquisas qualitativas aprofundadas sobre as experiências das partes interessadas.

A hipótese era que muitas organizações no Brasil poderiam não estar totalmente conscientes dos requisitos legais e tecnológicos, levando a uma adoção lenta das medidas de conformidade. Organizações que se adaptassem rapidamente à conformidade da LGPD poderiam ganhar vantagem competitiva, demonstrando comprometimento com a privacidade e segurança de dados.

O objetivo geral era analisar o impacto da LGPD e GDPR nas organizações, investigando melhorias na segurança, proteção da privacidade e gestão de incidentes. Buscava-se também analisar o nível de conformidade das organizações, identificar áreas de melhoria, apurar a gestão de terceirizados com acesso a dados pessoais e identificar casos de sucesso na implementação dessas regulamentações.

2. REVISÃO DE LITERATURA

A gestão da privacidade e segurança de dados nas organizações ganhou destaque nas últimas décadas devido ao rápido avanço da tecnologia da informação e ao aumento na coleta, armazenamento e processamento de informações pessoais. A conscientização sobre a importância da proteção de dados e a necessidade de regulamentações específicas remontavam a vários anos.

2.1 Contexto Histórico

Na década de 1970, começou a surgir a conscientização sobre a importância da segurança, proteção e privacidade de dados com o rápido crescimento da automação e do uso de sistemas de informação. A preocupação com a coleta e o uso indevido de informações pessoais pelas organizações levou à criação de algumas das primeiras leis de proteção de dados, como a Lei de Proteção de Dados na Suécia em 1973.

O Conselho da Europa editou resoluções em 1973 e 1974 para estabelecer princípios para a proteção de informações pessoais em bancos de dados automatizados, tanto no setor público como privado (MALDONADO, 2019). Durante as décadas seguintes, várias nações introduziram leis de proteção de dados para regulamentar a coleta e o processamento de informações pessoais. Também foi nessa época que surgiu o conceito de "Privacy by Design", propondo que a privacidade deveria ser considerada desde o início do desenvolvimento de sistemas e processos.

Com a expansão da Internet e o crescimento das atividades online, a privacidade de dados tornou-se um tema com maior destaque. Os Estados Unidos promulgaram a Lei de Portabilidade e Responsabilidade no Seguro de Saúde (HIPAA), estabelecendo padrões para a proteção de informações médicas. A União Europeia criou a Diretiva de Proteção de Dados em 1995, um precursor importante para o General Data Protection Regulation (GDPR).

O GDPR foi iniciado em 2012 pela União Europeia, publicado em 2016 e entrou em vigor em 2018, estabelecendo um padrão global para a proteção de dados pessoais. Ele impôs regras rigorosas para a coleta, armazenamento, processamento e exclusão de informações pessoais, estabelecendo direitos dos titulares de dados, regras de notificação de violações e penalidades significativas para não conformidade.

2.2 Contexto histórico brasileiro

A matriz de inspiração das leis com intenção protetiva de dados pessoais foi a Declaração Universal dos Direitos Humanos de 1948, que estabeleceu as fundações de liberdade, justiça e paz mundiais, reconhecendo valores de proteção da privacidade individual e familiar (MALDONADO, 2019).

A gestão da privacidade de dados nas organizações no Brasil começou a ganhar destaque principalmente a partir de 2018, com a entrada em vigor da LGPD (Lei n°13.709/2018). A LGPD, inspirada em regulamentações europeias como o GDPR, estabeleceu um conjunto abrangente de regras para a coleta, armazenamento e processamento de informações pessoais no país.

Pinheiro (2020) afirmou que a base legal da Constituição Federal do Brasil estava baseada nos direitos fundamentais da DUDH, refletindo a proteção aos direitos fundamentais evidente no art. 2º da LGPD.

2.3. Relação da gestão da privacidade de dados e as leis de proteção de dados

A gestão da privacidade de dados estava intrinsecamente ligada às leis de proteção de dados, que eram conjuntos de regulamentações e normas estabelecidos para garantir a proteção dos direitos individuais em relação ao tratamento de informações pessoais. Essa relação era fundamental para assegurar que as organizações coletassem, processassem, armazenassem e compartilhassem dados pessoais de maneira ética, transparente e legal.

Mayer-Schõnberger destacou o custo social que os indivíduos enfrentavam ao exercer seu direito à privacidade, questionando se era aceitável que a proteção de dados fosse acessível apenas para aqueles dispostos a se isolar socialmente.

Mendes (2018) apontou que as normas de proteção de dados pessoais levantavam uma controvérsia sobre a efetividade do consentimento do cidadão e seu verdadeiro exercício de liberdade de escolha. Em um contexto em que a não divulgação de dados poderia resultar na exclusão social, havia um dilema entre garantir a liberdade informacional e a necessidade do Estado de dados para suas funções burocráticas.

As leis de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil, estabeleciam os requisitos legais que as organizações deveriam seguir em relação à privacidade de dados. A gestão era essencial para garantir a conformidade com essas leis, além de definir princípios e requisitos específicos que as organizações deveriam seguir ao lidar com dados pessoais.

Estudos quantitativos dos riscos da indústria 4.0 indicaram que, do ponto de vista tecnológico, os riscos em sua maioria destacavam questões de conectividade. No entanto, ataques cibernéticos e divulgação de dados privados estavam entre os primeiros riscos no ranking. Nas figuras demonstradas pela revista Gestão e Desenvolvimento (set./dez. 2020), é notável os crescentes os riscos tecnológicos diante de dados alarmantes de ataques cibernéticos e vazamento de dados.

A gestão eficaz da privacidade de dados não apenas garantia a conformidade legal, mas também construía confiança com clientes e partes interessadas, promovendo uma cultura organizacional que valorizava a privacidade e a segurança dos dados pessoais.

A LGPD e o GDPR eram regulamentações de privacidade de dados implementadas em diferentes jurisdições, com o objetivo comum de proteger os direitos dos titulares de dados pessoais. O quadro comparativo entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia evidenciava as semelhanças e diferenças nas abordagens de privacidade e segurança de dados.

Ambos os regulamentos compartilhavam princípios fundamentais, como transparência, segurança e responsabilidade, mas diferiam em suas bases legais, requisitos contratuais entre controlador e operador de dados, e especificidades sobre transferências internacionais de dados.

A LGPD ainda dependia de definições adicionais pela Autoridade Nacional de Proteção de Dados (ANPD), enquanto a GDPR já possuía normas detalhadas. Essas nuances refletiam as particularidades jurídicas e operacionais de cada região, sublinhando a importância de uma adaptação cuidadosa por parte das organizações para assegurar conformidade em múltiplas jurisdições.

O GDPR era considerado mais restritivo e detalhado que a LGPD, destacando-se por especificações mais abrangentes, especialmente em relação ao papel do Encarregado de Dados (DPO). Uma diferença relevante era a exigência mais clara do GDPR sobre quando realizar Avaliação de Riscos, conhecida como Relatório de Impacto de Proteção de Dados. Essa avaliação analisava os riscos de segurança de dados, gerando preocupações na LGPD, especialmente para micro e pequenas empresas devido aos custos envolvidos.

A LGPD deixou lacunas a serem preenchidas pela Autoridade Nacional de Proteção de Dados (ANPD), indicando a necessidade de avanços e adaptações nas atividades comerciais que lidavam com dados pessoais, enfrentando desafios em setores como segurança, saúde e instituições públicas. A evolução contínua da LGPD era necessária, seguindo o exemplo do GDPR na União Europeia.

Vigente desde agosto de 2021, a LGPD exigia que organizações públicas e privadas implementassem controles para respeitar a privacidade das pessoas físicas. Seu objetivo era proteger os direitos fundamentais de liberdade e privacidade, focando na prevenção do uso indevido de dados pessoais por organizações sem autorização.

A lei (LGPD, Lei n. 13.709/2018), composta por 65 artigos, definia o escopo, princípios, penalidades e estrutura de governança. As organizações poderiam enfrentar penalidades significativas por uso inadequado de dados pessoais, e a interpretação da lei ainda não estava completamente clara.

A LGPD possuía sete fundamentos, destacando o respeito à privacidade, a autodeterminação informativa e a proteção da liberdade de expressão. Além disso, considerava aspectos sociais e de desenvolvimento econômico, tecnológico e inovação, buscando equilíbrio entre a privacidade individual e o progresso coletivo.

3. PROCEDIMENTOS METODOLÓGICOS

A metodologia adotada para este projeto fundamentou-se na pesquisa exploratória, com coleta de dados por meio de pesquisa bibliográfica e relato de experiência. A pesquisa bibliográfica focou-se em analisar e investigar se as organizações que implementavam o GDPR experimentavam melhorias significativas na proteção da privacidade de dados, gestão de incidentes de segurança e conformidade regulatória.

O estudo buscou compreender como as organizações lidavam com a conformidade em contextos de terceirização ou parceria, onde os dados pessoais poderiam ser partilhados com terceiros, com foco na proteção da privacidade dos dados e na gestão de incidentes de segurança. A pesquisa incluiu a avaliação do nível de conformidade das organizações que implementavam o GDPR em relação aos regulamentos e à implementação de políticas e práticas de proteção de dados. Isto envolveu identificar áreas para melhoria, bem como examinar registros de incidentes de segurança de dados nas organizações, incluindo a frequência, gravidade e eficácia das respostas a esses incidentes.

Além disso, o estudo visou investigar como as organizações gerenciavam e monitoravam terceiros ou parceiros com acesso a dados pessoais e garantiam o cumprimento das regulamentações de privacidade. Foi realizada uma comparação com organizações que mantinham todos os serviços internamente para identificar desafios específicos e melhores práticas.

A pesquisa também buscou estudos de caso de organizações que alcançaram melhorias significativas na proteção de dados, gestão de incidentes de segurança e conformidade regulatória após a implementação do GDPR. Teve como objetivo identificar os principais fatores de sucesso e avaliar a percepção dos clientes e partes interessadas em relação à privacidade dos dados, incluindo a confiança na gestão de dados.

4. BASE LEGAL E REGULATÓRIA NACIONAL E EUROPÉIA

A expressão "sociedade de informação" descrevia o contexto técnico-econômico do século XXI, no qual a circulação de informações entre os diversos segmentos da sociedade era fundamental.

Essa sociedade era impulsionada pelo avanço tecnológico, que viabilizava uma série de serviços e atividades cotidianas, como compras online, educação à distância e entretenimento digital.

Estudos acadêmicos destacavam a LGPD como um marco importante para a proteção de dados no Brasil, alinhando o país às melhores práticas internacionais e promovendo um ambiente de maior segurança jurídica e confiança no uso de dados pessoais.

4.1 Direito a privacidade e segurança de dados na legislação brasileira

A legislação brasileira, com a LGPD, buscava equilibrar a inovação tecnológica com a proteção dos direitos fundamentais dos cidadãos, promovendo a privacidade e a segurança dos dados em um contexto de rápido avanço tecnológico.

Gavison (1980) ressaltava a importância de proteger a privacidade dos cidadãos tanto de outros indivíduos quanto do próprio Estado. Isso implicava estabelecer limites claros para prevenir interferências indevidas e garantir que a vida íntima fosse respeitada.

Diante disso, surgiram leis de proteção de dados em todo o mundo, como a LGPD no Brasil, para o tratamento regulamentar dessas informações. O vazamento de dados, um dos incidentes de segurança mais preocupantes, ocorria quando as informações eram acessadas indevidamente e utilizadas por terceiros.

4.1.1 Segurança da Informação

A segurança da informação visava proteger a confidencialidade, integridade e disponibilidade dos dados. O vazamento de dados era uma das maiores preocupações, podendo ocorrer por ataques cibernéticos, erro humano ou negligência. A LGPD obrigava os agentes de tratamento a adotar medidas de segurança adequadas e definia o tratamento irregular como aquele que não cumpria a legislação ou não garantia a segurança esperada.

4.1.2 Responsabilização e Incidentes de Segurança

A LGPD responsabilizava os agentes de tratamento por danos causados por violação da legislação e exigia medidas para prevenir incidentes de segurança. O vazamento de dados podia ter consequências graves, como roubo de identidade e extorsão.

A Autoridade Nacional de Proteção de Dados (ANPD) era o órgão responsável por zelar pela proteção dos dados pessoais e por implementar e fiscalizar o cumprimento da LGPD.

4.2 Princípios da GDPR e LGPD semelhanças e diferenças

A LGPD apresentava uma abordagem que, além de estar alinhada com a GDPR, trazia especificidades que refletiam o contexto brasileiro. A inclusão de princípios como "livre acesso" e "não discriminação" na LGPD destacava preocupações específicas e proporcionava um guia mais detalhado para as organizações sobre os direitos dos titulares de dados.

Ambas as regulamentações enfatizavam a importância da transparência no tratamento dos dados pessoais, garantindo que os titulares fossem informados sobre como seus dados eram tratados. Tanto a GDPR quanto a LGPD exigiam que medidas técnicas e organizacionais fossem adotadas para garantir a segurança e integridade dos dados pessoais.

A responsabilidade era outro princípio compartilhado por ambos os regulamentos. As organizações eram responsabilizadas pela conformidade com as normas e deviam ser capazes de comprovar a adoção de medidas adequadas para a proteção dos dados pessoais.

A finalidade e limitação das finalidades era uma área onde as abordagens divergiam ligeiramente. A GDPR enfatizava a limitação das finalidades como um princípio fundamental, permitindo o tratamento posterior de dados para fins públicos, científicos ou estatísticos, desde que compatíveis com as finalidades iniciais (UNIÃO EUROPÉIA, 2019). Já a LGPD agrupava esse

conceito sob os princípios de "finalidade" e "adequação", focando em propósitos específicos e informados ao titular (BRASIL, 2018).

A LGPD incluía explicitamente o direito ao livre acesso e consulta sobre o tratamento dos dados, garantindo aos titulares o acesso facilitado e gratuito a informações sobre a duração e forma do tratamento de seus dados pessoais.

Princípios como prevenção e não discriminação eram explicitamente destacados na LGPD (BRASIL, 2018). A prevenção tratava da adoção de medidas para evitar danos decorrentes do tratamento de dados, enquanto a não discriminação impedia o uso dos dados para fins discriminatórios ilícitos ou abusivos.

Iramina (2020) destacava que a aplicabilidade do GDPR para além da União Europeia impactou diretamente o Brasil. Além disso, com a sua vigência, o bloco passou a listar oficialmente os países que possuíam "níveis adequados de proteção de dados".

4.3 Violação de dados, incidentes de segurança e vazamento de dados

A proteção de dados pessoais evoluiu do direito à privacidade, tornando-se essencial na era digital. Esses dados eram cruciais para a formação da personalidade e valiosos no mercado atual. A Lei nº 13.709/2018 garantia aos cidadãos o direito de saber como seus dados eram coletados, processados e armazenados, e conferia à Autoridade Nacional de Proteção de Dados (ANPD) a função de fiscalização.

4.3.1 Exemplos de violação e vazamentos de dados no Brasil

Os incidentes de vazamento de dados no Brasil tornaram-se uma preocupação crescente, destacando a necessidade de rigorosas medidas de segurança cibernética e conformidade com a Lei Geral de Proteção de Dados (LGPD). As empresas e instituições deveriam investir continuamente em tecnologias de segurança e capacitação de seus profissionais para mitigar os riscos e proteger as informações sensíveis dos cidadãos.

Costa, Archegas e Steibel (2021a) relataram que, em abril de 2021, um pesquisador de segurança expôs vulnerabilidades no sistema da Fundação Oswaldo Cruz (Fiocruz), que poderiam alterar os resultados da produção de vacinas contra a covid-19. Em novembro de 2020, o Superior Tribunal de Justiça (STJ) sofreu um ataque cibernético severo, interrompendo suas atividades por semanas. Esses incidentes evidenciavam um padrão de falhas na cibersegurança brasileira, alimentando o comércio de dados ilícitos na dark web.

Soprana (2021) relatou dois grandes vazamentos de dados em 2021, envolvendo 223 milhões de CPFs e informações pessoais sensíveis. Costa, Archegas e Steibel (2021b) destacaram que, entre 2018 e 2019, o número de vazamentos de dados no Brasil aumentou 493%, evidenciando a fragilidade cibernética do país.

A Autoridade Nacional de Proteção de Dados (ANPD) publicou decisões sancionando o Instituto Nacional de Seguro Social (INSS) e a Secretaria de Estado de Educação do Distrito Federal (SEEDF) por violarem disposições da LGPD. Lopes (2024) enfatizou a importância da comunicação aos titulares para que pudessem se proteger após um incidente de segurança.

4.3.2 Controvérsias da privacidade na legislação e falhas no cumprimento da LGPD

Várias controvérsias relacionadas à privacidade e à legislação surgiram, refletindo os desafios complexos de equilibrar segurança, inovação, responsabilidade e eficiência. Questões como a capacidade da ANPD de fiscalizar efetivamente, a responsabilidade em casos de vazamentos, o

equilíbrio entre segurança nacional e privacidade individual, e a proteção de dados em setores críticos foram levantadas.

A análise dos casos citados revelou falhas significativas no cumprimento da LGPD, incluindo inadequações nas medidas de segurança, falta de preparação para resposta a incidentes e não conformidade com obrigações de comunicação e registro. As instituições mencionadas não adotaram medidas de segurança cibernética adequadas, não foram suficientemente transparentes na comunicação de incidentes, e não seguiram todas as diretrizes estabelecidas.

4.3.3 Terceirização dos dados e confiança do consumidor

A terceirização dos dados podia oferecer vantagens, como acesso a tecnologias avançadas e especialistas em segurança cibernética. No entanto, também podia introduzir riscos adicionais se os provedores terceirizados não aderissem aos padrões de segurança e conformidade necessários. As instituições precisavam assegurar que qualquer terceirização envolvesse controles rigorosos e conformidade estrita com a LGPD e outras regulamentações aplicáveis para minimizar riscos e proteger os dados pessoais dos cidadãos.

A confiança do consumidor podia ser profundamente impactada por incidentes de vazamento de dados e controvérsias em torno da privacidade e da legislação de proteção de dados. Para manter e recuperar a confiança do consumidor, era fundamental que as empresas e instituições adotassem medidas robustas de segurança cibernética e fossem transparentes em suas comunicações. Implementar e cumprir rigorosamente a LGPD era crucial para garantir que os dados pessoais dos consumidores fossem protegidos de forma adequada.

4.4 Respostas aos incidentes cibernéticos de segurança

A resposta a incidentes de segurança minimizava os impactos de perda ou roubo de informações e interrupção de serviços. Também permitia a atualização e melhoria contínua dos procedimentos de tratamento de incidentes com base nas lições aprendidas.

4.4.1 Estrutura Organizacional de Tratamento de Incidentes Cibernéticos na APF

Na Administração Pública Federal (APF), o Gabinete de Segurança Institucional (GSI) da Presidência da República, através do Departamento de Segurança da Informação e Cibernética (DSIC), era responsável pela segurança da informação. Suas atribuições incluíam a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas.

O CTIR Gov, parte do DSIC, funcionava como um "Computer Security Incident Response Team (CSIRT)" que recebia, analisava e respondia a notificações de segurança. Ele coordenava e integrava ações de gestão de incidentes, promovia intercâmbio científico-tecnológico e estabelecia diretrizes para a gestão de incidentes computacionais.

O Decreto nº 10.748, de 16 de julho de 2021, criou a Rede Federal de Gestão de Incidentes Cibernéticos (Regic), visando melhorar a coordenação entre órgãos federais para prevenção, tratamento e resposta a incidentes cibernéticos.

4.4.2 Planejamento de Resposta a Incidentes Computacionais

Cada organização devia criar uma política de gestão de incidentes, incluindo planos específicos para incidentes que violassem a proteção de dados pessoais. Esses planos deviam minimizar os impactos aos titulares e comunicar a Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares quando necessário.

4.4.3 Mecanismos para Desenvolvimento de Políticas de Gestão de Incidentes

Os principais mecanismos para a implementação do desenvolvimento de políticas de gestão de incidentes incluíam: Plano de Resposta a Incidentes, Equipes para Tratamento de Incidentes, Procedimentos Internos e Relatórios, Diretrizes e Plano de Comunicação, Linhas de Comunicação, Modelo Estrutural de Equipes e Serviços Providos.

4.4.4 Tratamento de Incidentes Computacionais

O processo de resposta a incidentes, segundo o NIST, possuía quatro fases: Preparação, Detecção e Análise de Incidentes, Contenção, Erradicação e Recuperação, e Atividades Pós-incidente.

4.4.5 Barreiras contra vazamento de dados

As empresas podem criar barreiras contra o vazamento de dados através da implementação de políticas de segurança rigorosas, capacitação de funcionários, conformidade com a LGPD, investimento em tecnologia de segurança avançada, monitoramento e auditoria contínua, e criptografia de dados.

Para as pessoas afetadas, medidas como alteração de senhas complexas, utilização de gerenciadores de senhas, monitoramento de extratos bancários e relatórios de crédito, configuração de alertas de segurança, proteção de identidade, e aprendizado sobre reconhecimento de ataques de phishing eram recomendadas.

Era essencial notificar bancos e outras instituições financeiras em caso de suspeita de comprometimento de dados, além de reportar incidentes às autoridades competentes, como a ANPD no Brasil. A implementação dessas estratégias fortalecia as defesas contra vazamentos de dados e mitigava os impactos de incidentes de segurança.

5. CONSIDERAÇÕES FINAIS

Os incidentes de vazamento de dados no Brasil evidenciaram vulnerabilidades significativas na segurança cibernética e a necessidade de conformidade com a Lei Geral de Proteção de Dados (LGPD).

Dentre os problemas citados, houve a vulnerabilidade em sistemas de instituições públicas como a Fundação Oswaldo Cruz (Fiocruz) e Superior Tribunal de Justiça (STJ), que possibilitou a manipulação de resultados de vacinas e interrupção de atividades judiciais. Além disso, o comércio ilegal de dados na Dark Web causou a venda de dados pessoais de 223 milhões de brasileiros em 2021, levando a uma violação massiva de privacidade e segurança de dados.

O crescimento intensivo nos vazamentos de dados posicionou o Brasil no Índice Global de Cibersegurança em 70° posição, possibilitando o mercado de Cyberattack-as-a-Service (CAaaS), a comercialização, enriquecimento, e mineração de dados pessoais. Mesmo com as sanções do INSS e SEEDF por violação da LGDP e não comunicação dos incidentes de segurança, entre outras infrações, a complexidade nas investigações e repressão desse mercado ilegal permaneceu.

As soluções propostas eram abrangentes e formavam uma base sólida para melhorar a segurança cibernética e a proteção de dados. No entanto, sua suficiência e eficiência dependiam de uma implementação contínua e diligente, bem como de uma adaptação às novas ameaças e tecnologias emergentes. A colaboração entre o setor público e privado, bem como entre diferentes departamentos dentro das organizações, era fundamental para fortalecer ainda mais a resiliência contra ciberataques e vazamentos de dados.

As políticas eram adequadas se continuamente atualizadas para refletir novas ameaças e tecnologias. A eficiência dessas políticas dependia da efetiva implementação, monitoramento, adesão e compreensão dos funcionários, além de conformidade regulatória para evitar sanções legais, proteger os dados de acordo com a LGPD e treinamentos regulares para garantir a eficácia.

O investimento era fundamental, mas requeria avaliação constante para garantir que as soluções fossem as mais adequadas e atualizadas. O monitoramento era essencial para identificar e corrigir vulnerabilidades em tempo real e muito eficaz se realizado por equipes competentes e com ferramentas de monitoramento de alta qualidade.

O controle de acesso era necessário para proteger dados sensíveis, dependendo da rigorosidade na aplicação e atualização dos acessos permitidos para ser eficaz. Os planos de resposta eram críticos para minimizar os danos e responder adequadamente a incidentes, se testados e atualizados regularmente.

Para uma resolução mais completa e eficiente dos problemas, as empresas e indivíduos deviam adotar uma abordagem proativa, estar sempre um passo à frente das ameaças emergentes, investir em pesquisa e desenvolvimento, fomentar parcerias e colaboração entre governo, empresas e a sociedade civil para fortalecer a infraestrutura de cibersegurança nacional. Além disso, era necessário incentivar a denúncia e a transparência, criar uma cultura de comunicação aberta sobre incidentes de segurança, para aprender e melhorar continuamente as práticas de proteção de dados.

A implementação inadequada das soluções propostas podia abrir brechas significativas na segurança cibernética e proteção de dados, expondo organizações e indivíduos a riscos elevados. Era essencial que as práticas de segurança fossem rigorosamente seguidas, atualizadas regularmente e auditadas para garantir sua eficácia contínua. Somente com uma abordagem proativa, detalhada e comprometida era possível minimizar os riscos e proteger adequadamente as informações sensíveis contra vazamentos e ataques cibernéticos.

Caso contrário, os riscos e impactos negativos podiam levar a grandes danos diante da maior suscetibilidade a ataques avançados que exploravam vulnerabilidades desconhecidas, a falta de sistemas de detecção e prevenção de intrusões (IDS/IPS) e a incapacidade de detectar e responder a ameaças em tempo real.

REFERÊNCIAS

BARRETO, G.G.; ANTONIO, A.L.S.; LIMA, A.G.B. Governança em privacidade de dados: uma visão integrada aos negócios empresariais. SERPRO. Editorial Casa. Curitiba, 2022.

BRASIL, STJ - Superior Tribunal Federal. Bibliografia selecionada LGPD. Biblioteca Ministro Oscar Saraiva. Brasília, DF.

BRASIL, Assembleia Geral das Nações Unidas. Declaração Universal dos Direitos Humanos. Resolução 217 A III, Art. 12. 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 19/10/2023.

BRASIL, Secretaria do Governo Federal. Guia de resposta a incidentes de segurança a proteção de dados pessoais. Setembro de 2021. Disponível em: https://images.app.goo.gl/oKwNvacjTCYjoHxo7

BRASIL, Ministério da Justiça e segurança Pública – Autoridade Nacional de proteção de Dados (ANPD). ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD; 2024.

Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd. Acessado em: 21/04/2024

BRASIL, Governo Federal. Guia de Resposta a Incidentes de Segurança. 31 de março de 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf

BRASIL; Ministério da Justiça e segurança Pública. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CÁTEDRA, Instituto de Desenvolvimento Profissional e Pós – Graduação. GDPR: o que é e qual q diferença em relação a LGPD? Cuiabá - Duque de Caxias. Agosto de 2021. Disponível em: https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/.

COSTA, J.; ARCHEGAS, J. V.; STEIBEL, F.. Instituto de Sociedade e Tecnologia (ITS). Vazamento de dados e o "broking" no Brasil. MIT Sloan Management Review Brasil. Rio de Janeiro, 2021. Disponível em: https://www.mitsloanreview.com.br/post/vazamento-de-dados-e-o-broking-no-brasil. Acessado em: 22/04/2024.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados. Rio de Janeiro: Renovar, 2006. Pg.70-90.

FOTIOS, Ricardo. Vazamento de dados aumentaram 493% no Brasil, mostra pesquisa do MIT. UOL, 2021. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-dedados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html. Acessado em: 24/04/2024

GAVISON, Ruth. Privacy and the limits of law. The Yale Law Journal, v. 89, nº 3, 1980. p. 438. Disponível em: https://digitalcommons.law.yale.edu/ylj/vol89/iss3/1

IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, no 2, p. 91-117, outubro de 2020, p. 102

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Nota de Rodapé nº 9, p. 21-22.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Comentários ao GDPR. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 46-66.

MARQUES, Leonardo Narciso. O mapeamento do modelo data management maturity (DMM) a Lei Geral de Proteção de Dados (LGPD). Orientador: Adriana Silveira Souza.2020. Tese (Bacharel em Engenharia da Computação) – Pontifícia Universidade Católica de Goiás, PUC, Goiás, 2020. Versão eletrônica.

MAYER-SCHÓNBERGER, Viktor. Generational Development of Data Protection in Europe, cit., p. 228.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno especial LGPD. P.35-56. São Paulo: Ed, RT. Nov. 2019.

MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. Orientador: Cristiano Paixão Araújo Pinto. Tese (Pós-graduação em Direito) – Faculdade de Direito da Universidade de Brasília, UNB, Brasília- DF, 2018. Pgs. 75-79. Versão eletrônica.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (LEI 13.709/2018) e o direito do Consumidor. Thomson Reuters - Revista dos Tribunais, vol.1009. Rio Grande do Sul, nov. 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 73.

RAPÔSO, C. F. L., et al. LGPD – Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: revista sistemática. RACE Revista de Administração, vol. 04. Universidad Autónoma de Asuncion. Paraguay, 2019.

SOLTOVSKI, R., et al. Um estudo quantitativo sobre os riscos da indústria 4.0 no contexto industrial: uma revisão sistemática da literatura. Revista Gestão e Desenvolvimento, vol. 17, n.03. Novo Hamburgo, set./dez. 2020.

SIVIERI, Edson Vicente. Estruturação do departamento de segurança da informação para atender a gestão de dados em conformidade a lei geral de privacidade de dados (LGPD). Universidade do sul de Santa Catarina, UNISUL – Universidade. São Paulo,2021.

SOPRANA, Paula. Hacker oferta base com dados de 223 milhões de brasileiros atribuída ao Poupatempo. Folha de São Paulo, São Paulo, 2021. Disponível em: https://www1.folha.uol.com.br/mercado/2021/03/hacker-oferta-base-com-dados-de-223-milhoesbrasileiros-atribuida-ao-poupatempo.shtml?origin=folha. Acessado em: 20/04/2024.

UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. 27 de abril 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT.