Revista Multidisciplinar do Nordeste Mineiro, v.10, 2024
ISSN 2178-6925

SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS NO BRASIL

INFORMATION SECURITY FOR COMPANIES IN BRAZIL

Kalleb Ribeiro Machado
Discente em Sistemas de Informação, Universidade Presidente Antônio Carlos de Teófilo Otoni - Unipac, Brasil
E-mail: kalleb12k@gmail.com

Kaio Oliveira Cata Preta
Discente em Sistemas de Informação, Universidade Presidente Antônio Carlos de Teófilo Otoni - Unipac, Brasil
E-mail: kaiofsteam@gmail.com

João César Mendel Pungirum
Discente em Sistemas de Informação, Universidade Presidente Antônio Carlos de Teófilo Otoni - Unipac, Brasil
E-mail: jpungirum@gmail.com

Resumo

Este artigo discute a importância da segurança da informação para as empresas no Brasil. À medida que os processos se tornam cada vez mais digitais e as ameaças cibernéticas aumentam, a proteção de dados tornou-se essencial para a sobrevivência e credibilidade das organizações. O estudo examina os desafios enfrentados pelas empresas brasileiras em relação à segurança da informação, incluindo ameaças, vulnerabilidades e o impacto potencial de ataques cibernéticos. Também analisa as principais estratégias e práticas que as organizações utilizam para gerenciar esses riscos, como políticas de segurança, tecnologias de proteção, conscientização dos funcionários e conformidade com regulamentações como a LGPD (Lei Geral de Proteção de Dados). Por meio de uma revisão bibliográfica, o artigo oferece insights e recomendações para ajudar as empresas brasileiras a fortalecer sua segurança da informação, proteger seus dados e garantir a continuidade dos negócios em um cenário digital cada vez mais complexo.

Palavras-chave: Informação, segurança, dados

Abstract

This article discusses the importance of information security for companies in Brazil. As processes become increasingly digital and cyber threats grow, data protection has become essential for the survival and credibility of organizations. The study examines the challenges Brazilian companies face regarding information security, including threats, vulnerabilities, and the potential impact of cyberattacks. It also reviews the main strategies and practices organizations use to manage these risks, such as security policies, protective technologies, employee awareness, and compliance with regulations like the LGPD (General Data Protection Law). Through a literature review, the article provides insights and recommendations to help Brazilian companies strengthen their information security, safeguard their data, and ensure business continuity in an increasingly complex digital landscape.

Keywords: Information, security, data

1. Introdução

.

A segurança da informação é fundamental para o sucesso e sobrevivência das empresas, especialmente em um ambiente digital cada vez mais interconectado. No Brasil, a crescente ameaça de ataques cibernéticos exige que as organizações adotem medidas proativas para proteger seus sistemas e dados, conforme a Lei Geral de Proteção de Dados (LGPD), inspirada na General Data Protection Regulation (Regulamento Geral de Proteção de Dados - GDPR) europeia. Promulgada em 2018 e obrigatória a partir de 2020, a LGPD busca garantir a privacidade e evitar vazamentos de dados. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) foi criada para fiscalizar e regular o cumprimento da LGPD no país.

Este trabalho tem como objetivo explorar e analisar a questão da segurança da informação no contexto empresarial brasileiro. Por meio de uma abordagem abrangente e detalhada, será examinado o panorama atual da segurança cibernética no Brasil, destacando as principais ameaças e vulnerabilidades enfrentadas pelas empresas. Além disso, serão discutidas as melhores práticas e estratégias de segurança que as organizações podem adotar para proteger seus

ativos de informação e mitigar os riscos associados à segurança cibernética.

2.1 Criação da Lei Geral de Proteção de Dados

Com a globalização e o desenvolvimento de novas tecnologias desenvolve uma competição cada vez mais voraz entre as empresas, desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes. As empresas e até o estado estão cada vez mais vulneráveis à espionagem ou de ataques de hackers como evidenciado nas divulgações de áudios de empresas e dos principais poderes do Brasil (PUBLISHED, 2024).

A LGPD (Lei Geral de Proteção de Dados) possui o intuito de capacitar os indivíduos e as empresas em um conjunto de direitos e deveres, em vez da complexidade da proteção parcial das leis setoriais em vigor anteriormente. Portanto, é necessário o desenvolvimento de uma metodologia sólida e assertiva, contendo boas práticas na implementação de projetos que exijam conhecimento total sobre essa lei, proporcionando agilidade no diagnóstico e a obtenção de sucesso nesse mercado, com o objetivo final de que qualquer ameaça seja rapidamente neutralizada (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

2.2 Orientações

De forma resumida, os passos abaixo fornecem um mapeamento detalhado e orientações específicas para implementação dos requisitos e controles exigidos pelo General Data Protection Regulation (Regulamento Geral de Proteção de Dados - GDPR) sendo essa baseada na norma **ISO 27701/2019** que foi criada pela International Organization for Standardization (Organização Internacional de Padronização- ISO) conjuntamente com a International Electrotechnical Commission (Comissão Eletrotécnica Internacional - IEC). Também sugere itens de implementação que mapeiam requisitos e controles de privacidade sugeridos por outros padrões que fazem interface com esse padrão. A metodologia divide-se em **3 fases e 6 etapas**, onde **cada fase possui 2 etapas de execução** (CELIDONIO, T; NEVES, P; DONÁ, C., 2020):

2.3 Fase 1: Diagnóstico (CELIDONIO, T; NEVES, P; DONÁ, C., 2020)

Etapa 1: Estabelecer a Comissão do Sistema de Gestão de Segurança e Privacidade da Informação (SGPI) junto aos principais stakeholders da organização (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

Etapa 2: Executar o gap analysis completo do ambiente considerando aspectos técnicos e jurídicos (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

A fase de diagnóstico é essencial para a implementação eficaz da Lei Geral de Proteção de Dados (LGPD) nas empresas. Essa etapa inicial permite que a organização compreenda o estado atual de suas práticas de tratamento de dados e identifique as áreas que precisam de ajuste para garantir a conformidade com a legislação. O **Sistema de Gestão de Segurança e Privacidade da Informação** (SGPI) tem como objetivo garantir que as políticas, procedimentos e medidas de segurança relacionados ao tratamento de dados pessoais estejam alinhados com os requisitos legais, protegendo tanto as informações da empresa quanto as de seus clientes e parceiros. Ao estabelecer a Comissão do SGPI, a organização cria um grupo de trabalho com stakeholders-chave que serão responsáveis por supervisionar e gerenciar as iniciativas de proteção de dados, assegurando que todas as áreas estejam envolvidas e comprometidas com a conformidade regulatória (VIEIRA, I., 2021).

2.4 Fase 2: Adequação (CELIDONIO, T; NEVES, P; DONÁ, C., 2020)

Etapa 3: Preparar, qualificar e envolver a equipe para adequação à nova legislação (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

Etapa 4: Implementar correções necessárias considerando os "**3 Ps"** da Governança de TI: Pessoas, Processos e Produtos (tecnologia) (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

A fase de adequação alinha as práticas da empresa com a Lei Geral de

Proteção de Dados. Envolve revisar políticas de privacidade, ajustar procedimentos operacionais, implementar medidas de segurança, e definir controles de acesso. Também inclui treinar funcionários, conscientizá-los sobre a proteção de dados, e estabelecer processos claros para obtenção e registro de consentimento dos titulares. A empresa deve criar mecanismos para que os titulares exerçam seus direitos e estabelecer procedimentos para responder às solicitações. Por fim, é essencial implementar monitoramento contínuo e auditorias periódicas para garantir a conformidade com a lei (VIEIRA, I., 2021).

2.5 Fase 3: Conformidade (CELIDONIO, T; NEVES, P; DONÁ, C., 2020)

Etapa 5: Definir e aplicar rotina de auditorias internas (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

Etapa 6: Implantar e iniciar o ciclo PDCA (Planejar, Fazer, Verificar e Agir) (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

A fase de conformidade assegura que a empresa mantenha práticas contínuas alinhadas com a LGPD. Isso inclui monitoramento contínuo e auditorias para avaliar a conformidade, gestão de incidentes para responder a violações de dados, e atualização regular de políticas de privacidade. Treinamentos contínuos e sessões de conscientização garantem que os funcionários estejam sempre informados sobre práticas de proteção de dados usando o PDCA que é: Planejar, Fazer, Verificar e Agir. Além disso, a avaliação e monitoramento de fornecedores garantem que todos os parceiros também cumpram a LGPD (VIEIRA, I., 2021).

Essa metodologia sugere a estrutura desenvolvida pela **ISO 27701/2019** para aprimorar o alinhamento entre suas normas de sistemas de gestão, possibilitando que uma organização alinhe ou integre seu SGPI (Sistema de Gestão de Segurança e Privacidade da Informação) com os requisitos de outras normas de sistemas de gestão (CELIDONIO, T; NEVES, P; DONÁ, C., 2020).

3. Desafios

A Lei Geral de Proteção de Dados Pessoais (LGPD) é considerada um marco significativo na proteção da privacidade e segurança dos dados no Brasil. Entretanto, sua implementação enfrenta diversos desafios, que suscitam preocupações sobre a eficácia da aplicação da lei nas empresas. Um dos principais obstáculos mencionados é a adaptação lenta das organizações às novas exigências legais. Muitas empresas ainda lutam para adequar suas práticas de tratamento de dados, o que pode comprometer a efetividade da lei. Além disso, a falta de clareza em algumas diretrizes e a necessidade de uma estrutura de governança sólida são fatores que dificultam a conformidade plena com a LGPD ("An overview of Brazil's LGPD", [s.d.]; "Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil", 2021).

3.1 Atraso na Implementação e Falta de Preparo

Um estudo da ICTS (Instituições de Ciência e Tecnologia) Protiviti, realizado em novembro de 2019, revelou que 84% das empresas ainda não estavam prontas para cumprir as exigências da LGPD. Essa realidade é particularmente preocupante entre pequenas e médias empresas, que muitas vezes não possuem os recursos ou o conhecimento necessário para se adequar à nova legislação (VELHO, R.,2020).

Um levantamento feito em 2023, revela que comparado a 2019, a porcentagem de empresas que não estão aptas para cumprir as exigências da Lei, baixou em apenas 4%, caindo de 84% para 80%, o que demonstra um baixo incentivo para adequação da lei (VELHO, R.,2020).

3.2 Decisões Automatizadas e o Direito à Revisão

Um ponto crucial da LGPD diz respeito às decisões automatizadas tomadas por algoritmos. A versão inicial da lei concedia aos indivíduos o direito de solicitar revisão humana em caso de decisões algorítmicas que os impactam negativamente. No entanto, essa proposta foi vetada e substituída por um texto que, embora mantenha o direito à revisão, não detalha como ela deve ser realizada.

Essa mudança gerou críticas por parte de especialistas, que argumentam que a nova redação abre margem para interpretações subjetivas, dependendo de decisões judiciais ou diretrizes da Autoridade Nacional de Proteção de Dados (ANPD). Essa situação pode comprometer a efetivação do direito à revisão e prejudicar os titulares dos dados (VELHO, R.,2020).

3.3 Criação da ANPD e Fragmentação de Responsabilidades

A demora na criação da ANPD, órgão responsável pela implementação e fiscalização da LGPD, foi outro fator que gerou apreensão. Especialistas em proteção de dados, alertam que, caso a ANPD não esteja em funcionamento até a data limite, suas funções precisarão ser assumidas por outros órgãos públicos, como o Ministério Público. Essa dispersão de responsabilidades entre diferentes instâncias, aliada à multiplicidade de ações civis públicas, pode resultar em decisões fragmentadas e inconsistentes na aplicação da lei, dificultando a harmonização da jurisprudência e gerando instabilidade jurídica (VELHO, R.,2020).

4. Consequências por não cumprir a lei

Cerca de 80% das empresas ainda não incorporaram a Lei Geral de Proteção de Dados (LGPD) em sua cultura organizacional, o que afeta negativamente a confiança e transparência com os clientes. A Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas, incluindo advertências, multas ou proibição de tratamento de dados. Multas podem chegar a 2% do faturamento da empresa, limitadas a 50 milhões de reais por infração. Além disso, podem ocorrer ações judiciais contra empresas que violam a LGPD (JUSBRASIL, 2018).

O não cumprimento da Lei Geral de Proteção de Dados (LGPD) pode resultar em ações judiciais, especialmente se os dados pessoais de indivíduos forem expostos ou divulgados de maneira inadequada. As vítimas de tais violações têm o direito de processar a empresa responsável, uma vez que essa ação configura uma violação das disposições legais. As consequências da não conformidade podem

variar de acordo com a gravidade do caso, sendo cada situação analisada individualmente. As penalidades por descumprimento da LGPD podem incluir advertências, multas que podem chegar a R$ 50 milhões ou até 2% do faturamento anual da empresa, e até ações que resultem na suspensão de atividades relacionadas ao tratamento de dados pessoais. É crucial que as empresas adotem medidas adequadas para garantir a conformidade com a legislação, a fim de evitar repercussões legais e danos à reputação (“LGPD: 8 penalidades em caso de descumprimento”, 2021; REI ADVOGADO, 2024).

Qualquer organização que manipula dados pode se beneficiar da implementação de normas específicas, como a ISO 27001, que facilita a conformidade com a legislação de proteção de dados. A adoção dessa norma sinaliza o comprometimento da alta direção com a segurança da informação, aumentando a confiabilidade em aspectos como confidencialidade, disponibilidade e integridade dos dados. Além disso, promove investimentos mais eficientes, orientados pelo risco, ao invés de tendências de mercado. Essa certificação também fortalece a confiança e a satisfação entre clientes e parceiros, contribuindo para o crescimento dos negócios e aprimorando o desempenho operacional da organização. Para os clientes, a adoção de tais normas evidencia um forte compromisso com a proteção das informações pessoais (SARTORE, A., OLIVEIRA, R., OLIVEIRA, R.,2023).

5. O que pode ser feito

Para que tanto o Estado brasileiro quanto as empresas se adequem à LGPD, algumas ações podem ser implementadas (“An overview of Brazil’s LGPD”, [s.d.]; “Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil”, 2021):

Educação e Treinamento: Promover campanhas de conscientização e programas de treinamento sobre a importância da proteção de dados, tanto para servidores públicos quanto para funcionários das empresas. Isso pode ajudar a garantir que todos compreendam suas responsabilidades em relação à privacidade e à segurança da informação (“An overview of Brazil’s LGPD”, [s.d.]; “Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil”, 2021).

Fortalecimento da Governança de Dados: Criar uma estrutura de governança robusta que inclua a designação de um Encarregado de Proteção de Dados (DPO) em organizações e a formação de comitês de conformidade que possam monitorar e aplicar as diretrizes da LGPD (“An overview of Brazil’s LGPD”, [s.d.]; “Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil”, 2021).

Essas ações podem ajudar a superar os desafios existentes e garantir a conformidade com a LGPD, promovendo a proteção dos dados pessoais no Brasil (“An overview of Brazil’s LGPD”, [s.d.]; “Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil”, 2021).

6 Conclusão

A Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, introduziu diretrizes significativas para a proteção da privacidade e dos dados pessoais no Brasil, com sua vigência iniciando em 2020. Apesar das penalidades rigorosas para não conformidade, muitas empresas ainda enfrentam desafios para atender aos requisitos da lei, em grande parte devido à falta de compreensão sobre as obrigações legais, complexidade da legislação e limitações de recursos, especialmente entre pequenas e médias empresas. Outros fatores determinantes para o não cumprimento da lei são de origem governamental: falta de clareza em algumas diretrizes e a necessidade de uma governança sólida dificultam a plena conformidade com a LGPD. Para adequar-se à LGPD, é essencial promover educação e treinamento sobre proteção de dados e fortalecer a governança de dados, designando um Encarregado de Proteção de Dados (DPO) e formando comitês de conformidade. Essas ações poderão garantir a proteção de dados pessoais no Brasil.

Referências

An overview of Brazil’s LGPD. Disponível em: https://iapp.org/news/a/an-overview-of-brazils-lgpd/. Acesso em: 2 out. 2024.

Brazilian General Data Protection Act | Risk Advisory | Deloitte Brazil. Disponível em: https://www.deloitte.com/br/en/services/risk-

advisory/perspectives/lgpd.html. Acesso em: 2 out. 2024.

BRUNELLI, S. **2022 foi bem movimentado em relação à LGPD**. Disponível em: https://www.contabeis.com.br/artigos/7958/2022-foi-bem-movimentado-em-relacao-a-lgpd/. Acesso em: 2 out. 2024.

CELIDONIO, Tiago; NEVES, Paulo Sergio; DONÁ, Claudio Melim. **Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira-Um estudo de caso/Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution-A case study**. Brazilian Journal of Business, v. 2, n. 4, p. 3626-3648, 2020.

Jusbrasil. **Lei 13.709 de 14 de agosto de 2018, art. 52**. Disponível em: https://www.jusbrasil.com.br/topicos/200398627/artigo-52-da-lei-n-13709-de-14-de-agosto-de-2018. Acesso em: 05 jun. 2024.

LGPD: 8 penalidades em caso de descumprimento. Disponível em: https://vv.adv.br/lgpd-8-penalidades-em-caso-de-descumprimento/. Acesso em: 2 out. 2024.

PUBLISHED, S. F. **Entire Brazilian population potentially put at risk by major data leak**. Disponível em: https://www.techradar.com/pro/security/entire-brazilian-population-potentially-put-at-risk-by-major-data-leak. Acesso em: 05 jun. 2024.

REDAÇÃO CONJUR. **Consultor Jurídico**. Disponível em: https://www.conjur.com.br/2020-ago-27/dois-anos-atraso-governo-cria-estrutura-anpd/. Acesso em: 2 out. 2024.

REI ADVOGADO. **Consequências e penalidades por descumprimento da LGPD no Brasil**. Disponível em: https://reyabogado.com/brasil/o-que-acontece-

se-violar-a-lgpd/. Acesso em: 2 out. 2024.

SARTORE, Andreia Aparecida; OLIVEIRA, Ronaldo Lopes de. **Certificação ISO 27001: a importância em sua utilização**. 2023.

VELHO, Raphaela. **Em vigor a partir de agosto, implementação da Lei Geral de Proteção de Dados ainda enfrenta desafios**. Ciência e Cultura, v. 72, n. 2, p. 09-11, 2020.

VIEIRA, Iuri Sousa. **Aplicações de software desenvolvidas no contexto da inteligência artificial (IA), machine learning e big data e o direito dos cidadãos de acordo com a lei geral de proteção de dados (LGPD)**. 2021.