RBTI – Revista Brasileira em Tecnologia da Informação
Volume 07, Número 01 – 2025
ISSN: 2675-1828
Editor Científico: Jaime Cazuhiro Ossada

Impacto da Lei Geral de Proteção de Dados (LGPD) na Segurança da Informação: Como a LGPD está Moldando as Práticas de Segurança de Dados no Brasil com Ênfase em Sistemas de Saúde

Rodrigo Estrela
rodrigo.estrela@fiocruz.br

RESUMO

A Lei Geral de Proteção de Dados (LGPD) estabelece um marco regulatório essencial para a proteção de dados pessoais no Brasil, especialmente relevante para o setor de saúde, onde a segurança da informação é crucial. Este artigo explora como a LGPD está moldando as práticas de segurança de dados nas instituições de saúde, destacando a importância de políticas claras de segurança, criptografia e anonimização, treinamentos contínuos e Avaliações de Impacto à Proteção de Dados (PIA). A adoção dessas práticas não apenas assegura a conformidade legal, mas também fortalece a proteção contra riscos de violação de dados, promovendo uma cultura organizacional comprometida com a privacidade e a segurança. A conformidade com a LGPD é, portanto, uma estratégia fundamental para garantir a integridade e a confiança nas operações de tratamento de dados pessoais.

Palavras Chave: LGPD; segurança da informação; proteção de dados pessoais.

Artigo Submetido: 01/09/2024

Artigo Aceito Publicação: 01/02/2025

Impact of the General Data Protection Law (LGPD) on Information Security: How the LGPD is Shaping Data Security Practices in Brazil with Emphasis on Health Systems

ABSTRACT

The General Data Protection Law (LGPD) establishes a crucial regulatory framework for personal data protection in Brazil, particularly significant for the healthcare sector, where information security is vital. This article examines how the LGPD is shaping data security practices in healthcare institutions, highlighting the importance of clear security policies, encryption and anonymization, continuous training, and Privacy Impact Assessments (PIA). Adopting these practices not only ensures legal compliance but also strengthens protection against data breach risks, fostering an organizational culture committed to privacy and security. Therefore, compliance with the LGPD is a fundamental strategy to ensure integrity and trust in personal data processing operations.

Key Words: LGPD; information security; personal data protection.

1 Introdução

A crescente digitalização das informações e a expansão do uso da internet transformaram profundamente a maneira como os dados são coletados, armazenados e utilizados no Brasil e no mundo. Em resposta a essas mudanças, surge a Lei Geral de Proteção de Dados (LGPD), regulamentação que estabelece diretrizes rigorosas para a proteção e privacidade dos dados pessoais. Sancionada em agosto de 2018 e em vigor desde setembro de 2020, a LGPD tem como objetivo principal garantir a transparência e a segurança no tratamento dos dados pessoais, exigindo das organizações um compromisso robusto com a segurança da informação.

O impacto da LGPD é particularmente significativo no setor de saúde, onde os dados sensíveis, como informações médicas, histórico de tratamentos e dados genéticos, são frequentemente manipulados. A proteção inadequada desses dados pode resultar em consequências graves para os indivíduos, incluindo discriminação, estigmatização e perda de privacidade. Além disso, os sistemas de saúde no Brasil, muitas vezes marcados pela precariedade e desatualização tecnológica, enfrentam desafios adicionais para se adequarem às exigências da LGPD.

Neste contexto, a LGPD não só impõe uma série de obrigações às instituições de saúde, como também representa uma oportunidade para a modernização e a adoção de melhores práticas de segurança da informação. Este artigo explora como a LGPD está moldando as práticas de segurança de dados no Brasil, com um enfoque especial nos dados sensíveis e nos desafios enfrentados pelos sistemas de saúde. A análise aborda as principais mudanças trazidas pela LGPD, os benefícios esperados e as dificuldades de implementação, oferecendo um panorama abrangente das transformações em curso no cenário da segurança da informação.

2 Referencial Teórico

Os dados sensíveis, conforme definido pela LGPD, incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. No

setor de saúde, a proteção desses dados assume uma relevância ainda maior devido ao seu potencial impacto na vida dos indivíduos.

As informações médicas e de saúde são extremamente valiosas não apenas para os próprios pacientes, mas também para terceiros mal-intencionados. Vazamentos ou acessos não autorizados a esses dados podem levar a fraudes, roubo de identidade, e até mesmo a chantagens. Portanto, a LGPD enfatiza a necessidade de medidas de segurança mais robustas para garantir a confidencialidade, integridade e disponibilidade dos dados sensíveis.

2.1 Desafios Enfrentados pelos Sistemas de Saúde

Os sistemas de saúde no Brasil enfrentam desafios consideráveis para atender às exigências da LGPD. Muitos hospitais, clínicas e centros de saúde ainda operam com sistemas de TI desatualizados, que carecem de funcionalidades de segurança modernas. Além disso, a falta de recursos financeiros e de pessoal qualificado dificulta a implementação de políticas de proteção de dados abrangentes.

Um estudo recente destacou que uma porcentagem significativa das instituições de saúde no Brasil ainda não está em conformidade total com a LGPD. As principais barreiras identificadas incluem:

- **Infraestrutura Desatualizada:** Muitos sistemas de TI nos hospitais foram desenvolvidos sem considerar as exigências modernas de segurança e privacidade, tornando-os vulneráveis a ataques cibernéticos.
- **Falta de Treinamento e Conscientização:** Profissionais de saúde frequentemente não recebem treinamento adequado sobre práticas de segurança da informação e proteção de dados, resultando em maior risco de violações por erro humano.
- **Recursos Financeiros Limitados:** Implementar medidas robustas de segurança da informação e garantir conformidade com a LGPD requer investimentos significativos, que muitas instituições de saúde, especialmente as públicas, não têm condições de arcar.

2.3 Como a LGPD Está Transformando as Práticas de Segurança de Dados

Apesar dos desafios, a LGPD também tem sido um catalisador importante para a melhoria das práticas de segurança de dados no Brasil. A lei obriga as organizações a adotarem medidas técnicas e administrativas adequadas para proteger os dados pessoais, incluindo:

Implementação de Políticas de Segurança: As instituições precisam desenvolver e implementar políticas claras de segurança da informação, incluindo planos de resposta a incidentes e procedimentos para o tratamento de dados pessoais.

- **Criptografia e Anonimização:** O uso de técnicas de criptografia e anonimização de dados é incentivado para reduzir o risco de exposição de informações sensíveis.
- **Treinamento e Conscientização:** A LGPD enfatiza a importância do treinamento contínuo dos funcionários em práticas de segurança e proteção de dados, promovendo uma cultura organizacional mais consciente e responsável.
- **Avaliação de Impacto de Privacidade:** Organizações devem realizar avaliações de impacto à proteção de dados (Privacy Impact Assessments - PIA) para identificar e mitigar riscos associados ao tratamento de dados pessoais.

2.4 Implementação de Políticas de Segurança

A implementação de políticas de segurança é um passo fundamental para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e proteger adequadamente os dados pessoais, especialmente os dados sensíveis. No contexto da LGPD, essas políticas devem ser abrangentes e detalhadas, cobrindo todas as áreas relevantes da organização. A seguir, exploramos os principais componentes dessas políticas e como elas podem ser desenvolvidas e implementadas de maneira eficaz.

2.4.1 Desenvolvimento de Políticas de Segurança da Informação

- **Diagnóstico Inicial:** O primeiro passo para desenvolver políticas de segurança é realizar um diagnóstico completo da infraestrutura de TI e dos processos de tratamento de dados existentes na instituição. Isso inclui a

identificação dos tipos de dados coletados, armazenados e processados, bem como os sistemas e procedimentos atualmente em uso para proteger esses dados.

- **Definição de Objetivos e Metas:** Com base no diagnóstico, a instituição deve definir objetivos claros para a política de segurança da informação, alinhados com os requisitos da LGPD. Isso pode incluir a proteção de dados sensíveis, a prevenção de violações de dados e a garantia da continuidade dos negócios em caso de incidentes.
- **Criação de Diretrizes e Procedimentos:** A política de segurança deve incluir diretrizes claras para o tratamento de dados pessoais. Isso abrange desde a coleta e armazenamento até o compartilhamento e descarte de dados. As diretrizes devem ser baseadas em princípios de minimização de dados, necessidade e proporcionalidade.

3 Planos de Resposta a Incidentes

- **Definição de Incidentes de Segurança:** A instituição deve definir o que constitui um incidente de segurança, incluindo violações de dados, acessos não autorizados e falhas de sistema. Cada tipo de incidente deve ter um protocolo de resposta específico.
- **Equipe de Resposta a Incidentes:** Formar uma equipe dedicada à resposta a incidentes de segurança é essencial. Essa equipe deve ser composta por profissionais de TI, especialistas em segurança da informação e representantes de outras áreas relevantes, como jurídico e comunicação.
- **Procedimentos de Resposta:** Os procedimentos de resposta a incidentes devem ser detalhados e incluir passos como a identificação e contenção do incidente, análise do impacto, notificação às autoridades competentes (como a Autoridade Nacional de Proteção de Dados - ANPD) e comunicação com os indivíduos afetados. A LGPD exige que a notificação ocorra em prazo razoável, dependendo da gravidade do incidente.
- **Planos de Recuperação:** Além de responder ao incidente, a instituição deve ter um plano de recuperação para restaurar a normalidade o mais rápido

possível. Isso inclui a restauração de sistemas e dados a partir de backups seguros e a implementação de medidas para evitar a recorrência do incidente.

4 Procedimentos para o Tratamento de Dados Pessoais

- **Controle de Acesso:** Garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais é fundamental. Isso pode ser feito através de controles de acesso baseados em função (Role-Based Access Control - RBAC) e autenticação multifator.
- **Registro de Atividades de Tratamento:** A LGPD exige que as organizações mantenham registros detalhados das atividades de tratamento de dados. Esses registros devem incluir informações sobre a finalidade do tratamento, as categorias de dados pessoais envolvidas e as medidas de segurança adotadas.
- **Avaliação de Impacto à Proteção de Dados (DPIA):** Para tratamentos de dados de alto risco, é necessário realizar uma DPIA, que avalia os riscos e impactos potenciais sobre a privacidade dos indivíduos e define medidas para mitigá-los.
- **Consentimento e Direitos dos Titulares:** As políticas devem garantir que o consentimento dos titulares de dados seja obtido de forma clara e inequívoca, e que os direitos dos titulares, como acesso, correção, exclusão e portabilidade dos dados, sejam respeitados e facilitados.

5 Treinamento e Conscientização

- **Programas de Treinamento:** Todos os funcionários, desde o nível operacional até a alta administração, devem participar de programas de treinamento regulares sobre segurança da informação e proteção de dados pessoais. Esses programas devem cobrir as políticas de segurança da instituição, os procedimentos de resposta a incidentes e as melhores práticas de segurança.
- **Cultura de Segurança:** Promover uma cultura de segurança dentro da organização é crucial. Isso pode ser feito através de campanhas de

conscientização, comunicações internas regulares sobre a importância da segurança da informação e incentivos para comportamentos seguros.

6 Monitoramento e Revisão Contínua

- **Monitoramento Contínuo:** Implementar sistemas de monitoramento contínuo para detectar e responder rapidamente a possíveis ameaças e vulnerabilidades. Isso inclui o uso de ferramentas de detecção de intrusões, sistemas de gestão de eventos e informações de segurança (SIEM) e auditorias regulares de segurança.
- **Revisão e Atualização de Políticas:** As políticas de segurança da informação devem ser revisadas e atualizadas regularmente para refletir mudanças na legislação, evolução das ameaças cibernéticas e melhorias tecnológicas. Isso garante que a instituição continue em conformidade com a LGPD e outras regulamentações relevantes.
- **Criptografia e Anonimização:** Reduzindo o Risco de Exposição de Informações Sensíveis

A proteção dos dados pessoais, especialmente os dados sensíveis, é uma das principais preocupações da Lei Geral de Proteção de Dados (LGPD). A adoção de técnicas de criptografia e anonimização é fortemente incentivada para minimizar os riscos associados à exposição não autorizada de informações. Essas técnicas desempenham um papel crucial na segurança da informação, proporcionando camadas adicionais de proteção que dificultam o acesso e o uso indevido de dados pessoais. A seguir, detalhamos a importância, os tipos e as melhores práticas de implementação de criptografia e anonimização.

7 Criptografia de Dados

7.1 Importância da Criptografia

A criptografia é um processo que transforma dados legíveis (plaintext) em dados ilegíveis (ciphertext) usando algoritmos matemáticos, tornando-os acessíveis apenas a quem possui a chave de descriptografia. Esta técnica é essencial para proteger dados em

trânsito (dados sendo transferidos através de redes) e em repouso (dados armazenados em dispositivos de armazenamento).

7.2 Tipos de Criptografia

- **Criptografia Simétrica:** Utiliza a mesma chave para criptografar e descriptografar dados. É eficiente e rápida, sendo adequada para a criptografia de grandes volumes de dados, mas requer um gerenciamento seguro das chaves.
- **Criptografia Assimétrica:** Utiliza um par de chaves – uma pública para criptografia e uma privada para descriptografia. É mais segura para a transmissão de dados, pois a chave privada nunca é compartilhada.
- **Criptografia de Chave Pública (PKI):** Envolve o uso de uma infraestrutura de chave pública para gerenciar chaves e certificados digitais, garantindo a autenticidade e a integridade dos dados.

7.3 Implementação de Criptografia

- **Dados em Trânsito:** Utilizar protocolos seguros como HTTPS, TLS (Transport Layer Security) e VPNs (Virtual Private Networks) para proteger dados transmitidos através de redes.
- **Dados em Repouso:** Implementar criptografia de disco completo (Full Disk Encryption - FDE) e criptografia de arquivos para proteger dados armazenados em servidores, dispositivos móveis e outros meios de armazenamento.
- **Gerenciamento de Chaves:** Utilizar sistemas de gerenciamento de chaves (Key Management Systems - KMS) para armazenar, rotacionar e proteger chaves de criptografia. Garantir que as chaves sejam acessíveis apenas a pessoas autorizadas.

8 Anonimização de Dados

8.1 Importância da Anonimização

A anonimização transforma dados pessoais de maneira que os indivíduos não possam ser identificados, direta ou indiretamente. É uma técnica valiosa para garantir a privacidade,

especialmente em casos onde os dados precisam ser utilizados para análises, pesquisas ou compartilhamento com terceiros sem comprometer a identidade dos indivíduos.

8.2 Técnicas de Anonimização

- **Pseudonimização:** Substitui identificadores diretos (como nomes ou números de identificação) por pseudônimos, que podem ser revertidos se necessário. Embora útil, a pseudonimização não oferece o mesmo nível de proteção que a anonimização completa.
- **Generalização:** Remove ou abstrai detalhes específicos dos dados, como substituir uma data de nascimento exata por uma faixa etária.
- **Perturbação:** Adiciona ruído ou modifica os dados de maneira a dificultar a identificação dos indivíduos, mantendo a utilidade dos dados para análise.
- **Supressão:** Remove completamente informações identificáveis dos dados, tornando impossível a reidentificação dos indivíduos.

8.3 Implementação de Anonimização:

- **Avaliação de Necessidade:** Avaliar a necessidade de anonimização com base no uso pretendido dos dados. Identificar quais dados precisam ser anonimizados para proteger a privacidade dos indivíduos.
- **Escolha de Técnicas Apropriadas:** Selecionar as técnicas de anonimização mais adequadas para o tipo de dados e o contexto de uso, garantindo um equilíbrio entre proteção da privacidade e utilidade dos dados.
- **Monitoramento e Revisão:** Monitorar a eficácia das técnicas de anonimização e revisar periodicamente as práticas de anonimização para assegurar que os dados permaneçam protegidos contra reidentificação.

8.3.1 Benefícios e Desafios

3.3.1.1 Benefícios:

- **Proteção Avançada:** Criptografia e anonimização proporcionam uma camada adicional de segurança, reduzindo significativamente o risco de acesso não autorizado e uso indevido de dados pessoais.

- **Conformidade com a LGPD:** Implementar essas técnicas ajuda as organizações a cumprir os requisitos da LGPD, demonstrando um compromisso com a proteção dos dados pessoais.
- **Confiança do Cliente:** A adoção de medidas robustas de segurança aumenta a confiança dos pacientes e clientes na capacidade da organização de proteger suas informações pessoais.

8.3.1.2 Desafios:

- **Complexidade Técnica:** A implementação de criptografia e anonimização pode ser tecnicamente complexa e requer conhecimentos especializados.
- **Desempenho:** A criptografia pode impactar o desempenho dos sistemas, especialmente durante a criptografia e descriptografia de grandes volumes de dados.
- **Reversibilidade da Pseudonimização:** A pseudonimização, embora útil, não oferece a mesma proteção que a anonimização completa e pode ser revertida sob certas circunstâncias.
- **Treinamento e Conscientização:** Promovendo uma Cultura de Segurança e Proteção de Dados

O treinamento contínuo e a conscientização dos funcionários são cruciais para promover uma cultura de segurança e proteção de dados dentro das organizações. A LGPD enfatiza a importância de educar os colaboradores sobre as melhores práticas de segurança da informação e sobre como manusear dados pessoais de forma adequada. Ao investir em programas de treinamento e campanhas de conscientização, as organizações podem reduzir significativamente os riscos de violação de dados causados por erros humanos e fortalecer a postura de segurança em toda a empresa. Essa abordagem proativa ajuda a criar um ambiente onde todos os funcionários estão cientes de suas responsabilidades e comprometidos com a proteção da privacidade dos indivíduos.

9 Avaliação de Impacto de Privacidade: Identificando e Mitigando Riscos Associados ao Tratamento de Dados Pessoais

As Avaliações de Impacto de Privacidade (Privacy Impact Assessments - PIAs) são ferramentas essenciais que ajudam as organizações a identificar e mitigar riscos associados ao tratamento de dados pessoais. Através das PIAs, é possível avaliar como os dados são coletados, processados e armazenados, garantindo que as práticas adotadas estejam em conformidade com a LGPD. Além disso, elas permitem a identificação precoce de possíveis vulnerabilidades, facilitando a implementação de medidas corretivas antes que ocorram incidentes de segurança. A realização regular dessas avaliações promove um ambiente de tratamento de dados mais seguro e transparente, alinhado às exigências legais e às expectativas de privacidade dos indivíduos.

3 Considerações finais

A implementação da Lei Geral de Proteção de Dados (LGPD) é um avanço crucial na proteção da privacidade e segurança dos dados pessoais no Brasil. Para as organizações, especialmente no setor de saúde, a conformidade com a LGPD não é apenas uma exigência legal, mas também uma oportunidade para fortalecer suas práticas de segurança da informação e aumentar a confiança de seus clientes e pacientes.

Adotar políticas claras de segurança da informação, técnicas de criptografia e anonimização, treinamentos contínuos e avaliações de impacto de privacidade são passos fundamentais para assegurar que os dados pessoais sejam tratados de forma segura e responsável. Essas práticas, quando integradas de maneira eficaz, não apenas protegem contra riscos de violação de dados, mas também promovem uma cultura organizacional comprometida com a privacidade e a segurança.

A LGPD impulsiona as organizações a revisarem e aprimorarem continuamente seus processos e sistemas, garantindo que estejam atualizados frente às novas ameaças e desafios tecnológicos. Este movimento não só minimiza os riscos de exposição de informações sensíveis, mas também fortalece a posição das organizações no mercado, diferenciando-as como líderes em segurança da informação.

Em suma, a conformidade com a LGPD vai além da mera obediência à legislação; é uma estratégia essencial para a construção de um ambiente de confiança e segurança. Ao implementar práticas robustas de proteção de dados, as organizações podem operar

de forma ética e segura, assegurando a integridade e a privacidade das informações pessoais em um mundo cada vez mais digitalizado.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia de boas práticas LGPD para saúde. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia-de-boas-praticas-lgpd-para-saude. Acesso em: 21 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 maio 2025.

SOUZA, F.; SILVA, A. B. Segurança da informação e a Lei Geral de Proteção de Dados no setor de saúde. Revista Brasileira de Gestão de Negócios, Rio de Janeiro, v. 22, n. 2, p. 370-389, abr./jun. 2020. DOI: 10.7819/rbgn.v22i2.4066.