www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 160, 2026 | DOI: 10.69849/nbt4hg72

Arquitetura da segurança da informação aplicada à gestão de arquivos: perspectivas da implementação da lei geral de proteção de dados (lei 13.709/2028).

Information Security Architecture Applied to Records Management: Perspectives on the Implementation of the General Data Protection Law (Law No. 13,709/2018).

Marcela Paul Mireski[1]
Gabriel Vieira[2]
Luís Roberto Sousa Mendes[3]

RESUMO

O presente estudo investiga a convergência estratégica entre a Arquitetura de Segurança da Informação (ASI) e a Gestão de Arquivos, fundamentando-se nas diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD). Diante de uma transição de padrões nos processos operacionais, caracterizada pela automação programada e pelo uso de inteligências artificiais, identifica-se um cenário de vulnerabilidade latente devido ao elevado fluxo de dados manipulados.

Nesse contexto, a segurança da informação é definida como um processo organizacional crítico, orientado pelos pilares da confidencialidade, integridade, disponibilidade, autenticidade, auditabilidade e legalidade. O objetivo central da pesquisa é analisar a relevância do planejamento institucional no desenvolvimento de uma ASI que atue como salvaguarda jurídica e proteção ao fluxo de compartilhamento do acervo documental.

[1] Acadêmica do curso de graduação em Arquivologia na Universidade Federal de Santa Catarina (UFSC). marcela.mireski@grad.ufsc.br
[2] Graduado em Ciência da Computação na Estácio. Gabriel.programmer@gmail.com
[3] Professor Doutor e Pesquisador na Universidade Federal de Santa Catarina (UFSC). mendes.luis@ufsc.br

De forma específica, o trabalho propõe-se a analisar a aplicação da LGPD na gestão de arquivos públicos e privados, compreender os mecanismos de acesso e disponibilização de informações para usuários internos e externos e identificar dispositivos de segurança, tanto físicos quanto digitais, empregados na proteção de dados em ambientes informacionais.

A fundamentação metodológica estrutura-se em uma pesquisa bibliográfica de natureza reflexiva, explorando a evolução das Tecnologias de Informação e Comunicação (TICs) e a necessidade de adaptação a novos mecanismos de comunicação segura nas infraestruturas de informação.

Palavras-chave: Arquitetura de segurança, Gestão de arquivos, LGPD, Segurança da informação.

ABSTRACT

The present study investigates the strategic convergence between Information Security Architecture (ISA) and Records Management, based on the guidelines established by the General Data Protection Law (LGPD). Facing a paradigm shift in operational processes, characterized by programmed automation and the use of artificial intelligence, a scenario of latent vulnerability is identified due to the high volume of handled data.

In this context, information security is defined as a critical organizational process, guided by the pillars of confidentiality, integrity, availability, authenticity, auditability, and legality. The main objective of this research is to analyze the relevance of institutional planning in the development of an ISA that serves as a legal safeguard and protection for the flow of sharing the documentary collection.

Specifically, the study aims to analyze the application of the LGPD in the management of public and private archives, understand the mechanisms for accessing and providing information to internal and external users, and identify both physical and digital security devices employed in data protection within information environments.

The methodological framework is structured around a reflective literature review, exploring the evolution of Information and Communication Technologies (ICTs) and the need to adapt to new secure communication mechanisms within information infrastructures.

Keywords: Security architecture, Records management, LGPD, Information security.

1. INTRODUÇÃO

A contemporaneidade está marcada pela centralidade dos fluxos de informação e conhecimento, elementos vitais para a formulação de estratégias financeiras, políticas e econômicas. Conforme observa Bioni (2019), a evolução tecnológica permitiu um acúmulo

sem precedentes de dados que revelam perfis detalhados dos indivíduos, gerando questionamentos sobre a eficácia das políticas de proteção vigentes.

Nesse cenário, os dados pessoais converteram-se em ativos de elevado valor estratégico para as organizações, impulsionados pela disseminação de sistemas de informação compartilhados que fundamentam à Gestão de Documentos Arquivísticos.

Com advento da Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei nº 13.709/2018, as instituições se viram obrigadas a readequar os processos de coleta, tratamento e compartilhamento de informações. Atualmente o desafio imposto aos gestores de arquivos consiste em integrar a Arquitetura da Informação (AI) aos mecanismos de Segurança da Informação (SI), visando assegurar que a acessibilidade aos dados não resulte em prejuízos à privacidade dos titulares.

Este estudo propõe uma reflexão sobre a importância estratégica de um bom planejamento e elaboração da Arquitetura de Segurança da Informação. O objetivo central consiste em identificar como os modelos de arquitetura em arquivos físicos e digitais, mediante uma estruturação adequada, atuam na proteção do acesso e do fluxo informacional sob a legislação da LGPD.

2. REVISÃO TEÓRICA

Com o advento da globalização, da revolução tecnológica e inovações digitais experimentadas após o século 20, a economia e as organizações passaram por transformações significativas tornando o mercado mais competitivo e evidenciando a necessidade de adaptações rápidas às novas tecnologias (BIONI, 2019,p.39) gerando desse modo, ativos que garantiriam a sobrevivência destas instituições a longo prazo.

Diante desse cenário, se fez necessário criar estratégias competitivas que se adaptassem às mudanças tecnológicas, e as mudanças macroambientais de forma eficaz e eficiente. Logo, a maneira como as organizações passaram a captar as informações também sofreu uma modificação significativa com a ajuda de novos sistemas de informação e tecnologias de armazenamento e processamento de dados.

Segundo Bioni (2019,p.39) a tecnologia da informação (dos bits ao Sistema de informação) permitiu agregar e acumular dados que revelam muito sobre nós. Entender o comportamento e hábitos de consumo dos clientes tem se tornado um desafio e uma importante ferramenta para definir estratégias competitivas em todos os cenários políticos, econômicos e sociais.

A inovação digital proporcionou um avanço na economia, política e cultura. As identificações de possíveis consumidores e de pontos que podem gerar oportunidades de negócios aliado à

possibilidade de integrar e interagir com diferentes públicos, propiciou o afloramento de um mecanismo eficiente de coleta de dados pessoais feitas pelas organizações através de uso de inteligências artificiais ou algorítimos de rastreabilidade.

De acordo com Ferreira; Pinheiro e Marques(2023);

> [….] “Com a disseminação do uso das tecnologias da informação os indivíduos tendem a ser vistos como um dado estatístico a ser analisado de acordo com suas postagens nas redes sociais. O conhecimento produzido em relação a estas informações despertam o interesse de organizações.

Considerando o cenário de vulnerabilidade decorrente do elevado fluxo de dados e da automação dos processos operacionais, emergiu a imperatividade da criação de uma estrutura normativa robusta, alicerçada na Lei Geral de Proteção de Dados (LGPD) para regulamentar a proteção de ativos informacionais.

Esta legislação estabelece mecanismos de salvaguarda jurídicas fundamentais para assegurar os direitos à privacidade e à individualidade dos usuários em plataformas digitais, integrando-se à Arquitetura de Segurança da Informação (ASI) como uma ferramenta estratégica na preservação da integridade e confidencialidade dentro do ciclo de vida documental.

2.1 LEI nº 13.709/2018 — Lei geral de Proteção de Dados (LGPD).

A defesa dos direitos à privacidade e ao anonimato torna-se essencial diante da crescente exposição dos usuários em redes digitais e da vigilância informacional exercida por algoritmos e inteligência artificial.

No Brasil esta preocupação vem de longa data, iniciou com a elaboração da Constituição Brasileira. O artigo 5º da Constituição Federal trata deste tema onde se refere ao resguardo, inviolabilidade a intimidade da vida privada, honra e imagem bem como a correspondências independente do tipo ou suporte utilizado pelo indivíduo, (Brasil,1988).

Contudo, a proteção constitucional mostrou-se insuficiente para coibir os danos oriundos de vazamentos e da comercialização indevida de dados pessoais devido aos avanços tecnológicos e sistemas de compartilhamento de informações em rede.

Consequentemente, foi sancionada a Lei nº 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) para legislar sobre princípios, direitos e deveres no tratamento de dados, tanto em meios físicos quanto digitais.

A finalidade desta legislação consiste em proteger as informações pessoais coletadas de pessoas físicas através da normalização e adequação de tratamento, armazenamento e disseminação de informação dos indivíduos tanto em ambiente online quanto offline.

2.2 Finalidade da LGPD (13.709/2018)

A Lei Geral de Proteção de Dados é um marco regulatório importante que nutre as políticas de proteção de Dados no Brasil a qual consiste em preservar o direito à privacidade, intimidade e à autodeterminação informativa. Esta se resume na autorização prévia do usuário no que se refere a disponibilização, coleta e tratamento de dados pessoais feitas por controladores e/ou operadores que detêm e utilizam as informações dos usuários.

Segundo Dotti (1980,p.37), a erosão da privacidade causada pelos instrumentos, meio e condições resultantes do desenvolvimento científico e tecnológico constitui fonte de apreensões para muitos países, devido aos perigos que podem emergir da maior velocidade da memorização e divulgação de informações que ainda não forma delimitados pela doutrina com rigor necessário (DOTTI,1980).

Nota-se, desse modo, que a lei geral de proteção de dados aflorou uma mudança social e cultural com relação à questão de compartilhamentos de dados e informações pessoais. Isso se dá pelo aumento da conscientização coletiva em relação a valoração dessas informações, a autodeterminação informativa e aos impactos psicossociais ou financeiros causados pelo vazamento de informações sensíveis.

Outro ponto importante que essa legislação trouxe foi a definição sobre os dados pessoais e tratamento dessas informações. Os artigos estão distribuídos ao longo de 10 capítulos que organizam todo o texto da lei (Lei nº 13.709/2018). Resumidamente do Art. 1º a 4º, tratam das disposições preliminares, definindo o alcance, os objetivos e os fundamentos da lei.

Os Art. 5º a 6º, tratam dos conceitos essenciais sobre o que é dado pessoal, dado sensível, dados anonimizados e pseudo-anonimizado, entre os Art. 7º a 16º tratam das Condições para o tratamento de dados (as bases legais) e os direitos dos titulares, definindo os agentes de tratamento e suas respectivas responsabilidades.

Já os Art. 17º a 33º, se referem a Transferência internacional de dados, operadores e as regras de segurança e boas práticas, os Art. 37º a 51º dizem respeito a Fiscalização e governança corporativa, incluindo a obrigatoriedade da figura do Encarregado (DPO), (BRASIL,2018).

Quanto à fiscalização das adequações legais e aplicação de políticas de tratamento de dados nas organizações, em 2019 criou-se a ANDP (Agência Nacional de Proteção de Dados)utilizando com base normativa referencial o capítulo IX e X, (Art. 52º a 65º) da Lei Geral de Proteção de Dados.

O intuito dela consiste em zelar pela proteção de dados e observância dos tratamentos realizados, elaborar diretrizes para Políticas de Proteção e Privacidade de Dados, realizar auditorias em agentes de tratamento, elaborar regulamentos e aplicar sanções civis e

administrativas quando houver descumprimento da legislação por parte das Instituições. (BRASIL, 2018).

2.3 Arquitetura de segurança da Informação

A Arquitetura de Segurança da Informação ou Privacy By Desing, consiste em desenvolver mecanismos de segurança em sistemas e softwares de compartilhamento de dados que atuem como inibidores de vazamento de dados e informações; sejam eles utilizados por agentes de tratamentos ou usuários de ferramentas digitais.

Conforme Motta (2024) a inteligência artificial, embora seja uma área de grande potencial e inovação, não é um mundo sem restrições ou limitações. Para que ela seja utilizada de modo seguro e sob observância da legislação, todo o sistema deve ser projetado de forma padronizada e segura, observando e prevendo todo o fluxo de produção e compartilhamento de informações. O combo internet das coisas, big datas e inteligência artificial, certamente tem transformado e ainda transformará muito a sociedade, (MOTTA,2024).

Os arquivos como custodiadores e responsáveis pela gestão de documentos necessitam observar a escolha de tais arquiteturas com maior cautela. A automação de alguns processos de gestão e gerenciamento de arquivos devem seguir padrões e níveis de segurança para que o fluxo de informação não seja afetado e as garantias de autenticidade e integridade dos documentos sejam mantidos.

Sabe-se que, os sistemas de machine learning são treinados usando grandes conjuntos de dados e algoritmos que os ajudam a identificar padrões e melhorar seu desempenho (MOTTA, 2024). No entanto, esta estruturação de arquitetura de segurança voltada aos arquivos não pode se basear tendenciosamente em propostas que visem somente a interação entre IA, sistemas e máquinas, excluindo dessa elaboração a interação humana.

É imprescindível a realização de um estudo de gerenciamento de risco interno e externo, entender o contexto e a panorâmica entre a interação homem/máquina, e a realização estudos de usuários que farão uso ou aplicarão efetivamente os comandos dentro dos sistemas, evitando desse modo falhas na segurança e vazamento de informações.

Logo, as boas práticas para a segurança da informação vão além da estruturação da arquitetura de segurança impecável. É necessário entender as variáveis que surgem no fluxo informacional, determinar as responsabilidades dos gestores na promoção da cultura organizacional voltada à segurança da informação, promover a conscientização dos usuários quanto às dimensões éticas e morais na disponibilização dos arquivos evitando processos de negligência de segurança em meio online ou offline.

3. GERENCIAMENTO DE RISCOS E PADRÕES DE ACESSO ADOTADOS EM ARQUIVO.

A preservação da informação em arquivos físicos ou digitais envolvem ações políticas, estratégicas, metodológicas e técnicas que garantem a confiabilidade, a integridade, a autenticidade e o acesso contínuo aos documentos ao longo do tempo.

Sob esta perspectiva de segurança da informação,se faz necessário a adoção de práticas e padrões de acessos que inibam a desinformação ou vazamento de dados e informações que possam causar danos aos seus usuários ou usos indevidos das informações.

Usualmente para estruturação de arquitetura de segurança da informação em arquivos físicos ou digitais são utilizados diferentes modelagens para acesso e disponibilização do acervo institucional. Dentre eles estão cadastros de senhas e usuários com autenticação em 2 fatores e criptografias ou assinatura eletrônica.

Já em arquivos institucionais físicos, os acessos aos arquivos se dão mediante a assinatura de livros de registros, acesso por portas automáticas e detectores de metais, acesso com biometria, videomonitoramento ou monitoramento de segurança privada. Embora a biometria represente um importante mecanismo de autenticação, estudos demonstram que esses sistemas permanecem vulneráveis a ataques de falsificação biométrica (biometric spoofing), tornando recomendável a adoção de mecanismos de detecção de ataques de apresentação (Presentation Attack Detection – PAD) para aumentar sua confiabilidade (KARTIKEY; KOMNINOS, 2026; YE, 2026).

4. JUSTIFICATIVA

A pesquisa bibliográfica utilizada neste projeto visa oferecer um panorama reflexivo sobre publicações científicas de estudos relacionados à Arquitetura da Segurança da Informação no contexto da Gestão de Arquivos, considerando as diretrizes da Lei Geral de Proteção de Dados.

Observa-se atualmente uma mudança nos processos operacionais de organizações públicas e privadas. A substituição da mão de obra humana por processos de automação programada baseada na eficiência e produtividade e uso de inteligências artificiais, geram vulnerabilidade na segurança da informação devido ao alto fluxo de dados manipulados simultaneamente por diferentes operadores.

Assim, pode-se definir segurança da informação como um processo organizacional que visa permitir que a instituição alcance seus objetivos, garantindo os pilares da confidencialidade, integridade, disponibilidade, autenticidade, auditabilidade e legalidade feitas através da governança de Dados, definindo papéis e responsabilidades entre seus integrantes e adotando políticas de controles para acesso e manipulação de arquivos..

Diante desse cenário, torna-se imprescindível investigar e compreender as dinâmicas de coleta, tratamento, armazenamento, compartilhamento de dados e informações sistemas

integrados bem como, compreender como a Arquitetura de Segurança da Informação pode atuar como um instrumento de salvaguarda jurídica para todos os agentes envolvidos no ciclo de vida documental.

5. METODOLOGIA

Esta pesquisa adota uma abordagem qualitativa e de natureza exploratória. A abordagem qualitativa se justifica por meio do levantamento bibliográfico de produções científicas que tratam sobre os temas relacionados a arquitetura de segurança da informação e lei geral de proteção de dados realizados em bases de dados científicas, como BRAPCI e SciELO, utilizando descritores específicos como "Gestão de arquivos", “Arquitetura da Informação”, "LGPD" e "Segurança da informação". O corpus de análise foi constituído por artigos científicos, livros e o texto da legislação brasileira pertinente.

6. DISCUSSÃO E RESULTADOS

As análises preliminares indicam que o debate sobre a implementação de arquiteturas de segurança da informação tem evoluído lentamente devido à ausência de estruturas pré estabelecidas para a rápida adequação normativa segundo as exigências da Legislação de proteção de dados. Por outro lado, nota-se uma melhora considerável na conscientização da importância do adequado tratamento de dados coletados pelas organizações graças à autodeterminação informativa.

A fiscalização por parte da Agência Nacional de Proteção de Dados também é um fator que passou a moldar as políticas e estruturações adequadas de sistemas de coletas e tratamentos de dados que passaram a operar com maior visibilidade e transparência para o usuário.

No entanto, ainda não é possível identificar se tais alterações de comportamento das organizações são resultantes de uma mudança de cultura organizacional pautadas nos princípios éticos ou meramente receio de sanções administrativas decorrentes dos órgão fiscalizadores.

7. CONSIDERAÇÕES FINAIS

Este estudo sintetiza superficialmente a importância estratégica da Arquitetura de Segurança da Informação (ASI) como um pilar fundamental para a conformidade com a Lei Geral de Proteção de Dados (LGPD) no âmbito da gestão documental. A transição para processos de automação e o uso intensivo de Inteligência Artificial ampliaram a vulnerabilidade dos fluxos informacionais, exigindo que a segurança seja compreendida não

apenas como um aparato técnico, mas como um processo organizacional contínuo que garante a confidencialidade, integridade e legalidade dos dados.

Evidenciou-se que uma arquitetura de segurança eficaz deve transcender a interação entre máquinas, incorporando o gerenciamento de riscos internos e externos e o estudo do comportamento humano no fluxo de dados buscando mitigar falhas ocasionadas por negligência no acesso aos sistemas dos arquivos e práticas de segurança tanto em ambientes online quanto offline.

Nesse sentido, a implementação de controles de acesso, que variam de criptografia e autenticação de dois fatores no meio digital, a videomonitoramento e biometria no meio físico, é essencial para assegurar a integralidade, autenticidade e o acesso contínuo aos documentos ao longo do tempo.

Nesse sentido, a implementação de controles de acesso, que variam de criptografia e autenticação em dois fatores no meio digital a videomonitoramento e sistemas biométricos dotados de mecanismos de detecção de ataques de apresentação (Presentation Attack Detection – PAD) no meio físico, é essencial para assegurar a integridade, a autenticidade e o acesso contínuo aos documentos ao longo do tempo.

A análise realizada nas bibliografias destacou que os dados pessoais tornaram-se ativos de elevado valor estratégico, o que obrigou as instituições a integrarem a Arquitetura da Informação (AI) aos mecanismos de segurança para harmonizar a acessibilidade com o direito à privacidade.

A LGPD, ao estabelecer mecanismos de salvaguarda jurídica e definir papéis claros como o do Encarregado (DPO) e a fiscalização pela ANPD, consolidou a Arquitetura de Segurança da Informação como um instrumento de proteção tanto para os titulares quanto para os agentes de tratamento no ciclo de vida documental.

Por fim, embora se observe um avanço na conscientização institucional impulsionado pela autodeterminação informativa e pelo receio de sanções administrativas, a implementação dessas estruturas ainda ocorre de forma morosa. Considera-se que o desafio persistente para as organizações reside em converter a conformidade normativa, muitas vezes motivada apenas pela fiscalização da aplicação das diretrizes da legislação em uma mudança genuína, de cultura verdadeiramente organizacional pautada em princípios éticos e na proteção integral dos direitos fundamentais dos cidadãos. Deste modo, evidencia-se que a implementação de uma arquitetura de segurança adequada na proteção integral dos direitos fundamentais dos cidadãos configura-se como uma ferramenta estratégica essencial para a proteção de ativos informacionais e para a garantia do acesso seguro dentro do fluxo documental nos âmbitos econômicos, políticos e sociais.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. 313 f.

DOTTI, René Ariel. Proteção à vida privada e liberdade de informação: possibilidades e limites. São Paulo: Revista do Tribunal, 1980.

KARTIKEY, Kumar; KOMNINOS, Nikos. On the Study of Biometric Spoofing Detection using Deep Learning. School of Science and Technology, City St George's University of London, London, United Kingdom, 2026.

CHAGAS, Ana Paula Monteiro Almeida; CARVALHO, Telma de. Interação entre usuários, tecnologia e sistema informatizado de gestão arquivística de documentos: percepções teóricas. InCID: R. Ci. Inf. e Doc., Ribeirão Preto, v. 16, p. e-217194, 2025. Disponível em DOI: https://doi.org/10.11606/issn.2178-2075.incid.2025.217194 - Acesso em: 12/03/26.

MOTTA,C.M.F.G. A interseção entre a Inteligência Artificial e a Privacidade de Dados: conformidade com a LGPD e segurança da informação. ARC: Av. Repr. Conh.,BH, v.4, n.2, ano IV, ago. 2024.disponível e: https://periodicos.ufmg.br/index.php/advances-kr/article/view/53024 - Acesso: 15/05/26.

PESSOA, L. G. S. B.; SOUZA, M. R. F.; FERREIRA, V. C. A. A influência da lgpd nas estratégias de segurança de dados. In:. Anais [...] Disponível em: https://brapci.inf.br/v/227616 - Acesso : 12/03/26.

BRASIL, Constituição Federal do Brasil,1988. Dos Direitos e Garantias, artigo 5º. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm - Acesso em: 20/05/2026.

PLANALTO, Lei Geral de Proteção de Dados Pessoais (LGPD). LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 .Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm - Acesso em: 20/05/2026.

YE, Weibo. Deepfake Attacks on Biometric Systems: Threats, Detection, and Defense Mechanisms – A Systematic Survey. Journal of Intelligence and Knowledge Engineering, v. 4, n. 1, p. 48–54, 2026.