CRIPTOGRAFIA E LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: A IMPORTÂNCIA DA PROTEÇÃO DE DADOS NA COMPUTAÇÃO EM NUVEM NO BRASIL

ENCRYPTION AND THE GENERAL PERSONAL DATA PROTECTION LAW: THE IMPORTANCE OF DATA PROTECTION IN CLOUD COMPUTING IN BRAZIL

Nicolas Arthur Oliveira Amaral[1]; Alberane Lucio[2]

RESUMO

A popularização da computação em nuvem no Brasil introduz desafios significativos para a proteção de dados pessoais, principalmente após a Lei Geral de Proteção de Dados (LGPD) entrar em vigor. A criptografia surge como a principal medida técnica para diminuir riscos de vazamento e acessos indevidos em ambientes de nuvem. Este trabalho teve como objetivo geral compreender de que maneira a criptografia pode garantir a proteção dos dados e manter a conformidade legal em ambientes de nuvem. A metodologia utilizada foi uma pesquisa qualitativa, exploratória e descritiva, baseada em revisão bibliográfica e documental, analisando artigos científicos, a legislação (LGPD), guias da ANPD e padrões técnicos internacionais, como os do NIST. A pesquisa constatou que a eficácia da criptografia para a conformidade com a LGPD envolve mais do que apenas aplicar algoritmos. A proteção efetiva exige uma abordagem baseada no ciclo de vida do dado, protegendo-o em trânsito, em repouso, em uso (por meio da computação confidencial) e na exclusão (via *crypto-shredding*). Conclui-se que a conformidade legal do Controlador (cliente) depende diretamente de sua capacidade de manter o domínio dos dados através da gestão de chaves (KMS), utilizando modelos como BYOK (Bring Your Own Key) para manter o controle, mesmo em infraestrutura operada por terceiros.

Palavras- chave: Criptografia. Proteção de Dados. Computação em Nuvem.

---

[1] Aluno do Curso de Ciências da Computação do Centro Universitário do Sul de Minas. Email: ni.oliveira800@gmail.com

[2] Professor do Curso de Ciências da Computação do Centro Universitário do Sul de Minas. Email: alberane@unis.edu.br

ABSTRACT

The popularization of cloud computing in Brazil presents significant challenges for personal data protection, especially after the General Data Protection Law (LGPD) came into effect. Encryption has emerged as the primary technical measure for reducing the risk of data leaks and unauthorized access in cloud environments. This study's overall objective was to understand how encryption can ensure data protection and maintain legal compliance in cloud environments. The methodology used was qualitative, exploratory, and descriptive research, based on a literature and document review, analyzing scientific articles, legislation (LGPD), ANPD guidelines, and international technical standards, such as those from NIST. Research has found that the effectiveness of encryption for LGPD compliance involves more than simply applying algorithms. Effective protection requires an approach based on the data lifecycle, protecting it in transit, securely, in use (through confidential computing), and upon deletion (via crypto-shredding). It is concluded that the legal compliance of the Controller (client) depends directly on its ability to maintain data control through key management (KMS), using models such as BYOK (Bring Your Own Key) to maintain control, even in infrastructure operated by third parties.

Keywords: Cryptography. Data Protection. Cloud Computing.

1 INTRODUÇÃO

A popularização da computação em nuvem no Brasil transformou a forma como organizações e indivíduos armazenam, processam e acessam informações. Essa tecnologia oferece flexibilidade, escalabilidade e redução de custos, permitindo que usuários acessem recursos computacionais de maneira remota e sob demanda. Contudo, ao mesmo tempo em que promove benefícios significativos, a computação em nuvem também amplia os riscos relacionados à privacidade e à segurança dos dados, tornando-se alvo frequente de ataques cibernéticos e falhas de proteção.

Nesse cenário, a proteção de dados pessoais assume um papel de destaque, especialmente após a entrada em vigor da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que

impõe às empresas responsabilidades rigorosas quanto ao tratamento das informações pessoais. A legislação exige que organizações adotem medidas técnicas e administrativas capazes de reduzir vulnerabilidades e preservar a confidencialidade, integridade e disponibilidade dos dados, sob pena de prejuízos à sua reputação.

Entre as estratégias disponíveis, a criptografia se apresenta como um recurso essencial, pois possibilita que informações sejam codificadas e acessíveis apenas a indivíduos autorizados. Dessa forma, ainda que haja violações ou acessos indevidos, os dados permanecem ilegíveis para agentes mal-intencionados. A combinação entre criptografia e cumprimento da LGPD, portanto, representa uma aliança estratégica para garantir a proteção da privacidade e a conformidade legal no contexto da computação em nuvem.

A questão central que orienta este estudo é: de que maneira a criptografia pode garantir a proteção dos dados e manter a conformidade com a LGPD ao armazenar informações pessoais em ambientes de nuvem? A hipótese que sustenta a investigação considera que, embora o uso de algoritmos criptográficos robustos seja um ponto crucial, a real conformidade com a LGPD não se limita apenas à criptografia, mas na capacidade do Controlador (o cliente) de manter o controle total sobre os dados através da gestão do ciclo de vida das chaves criptográficas (KMS). Considera-se que a aplicação de modelos como BYOK (Bring Your Own Key) e a proteção do dado em todo o seu ciclo de vida — incluindo em trânsito, em repouso, em uso e na sua exclusão (via *crypto-shredding*) — são os mecanismos técnicos centrais para mitigar os riscos do Modelo de Responsabilidade Compartilhada e assegurar a governança exigida pela lei.

Diante disso, o objetivo geral desta pesquisa é compreender a função da criptografia na proteção de dados em nuvem, analisando sua relação com as diretrizes estabelecidas pela LGPD e sua efetividade na preservação da confidencialidade das informações. De forma mais detalhada, os objetivos específicos incluem:

a) Investigar os princípios da LGPD, focando na definição dos papéis de Controlador e Operador no contexto do Modelo de Responsabilidade Compartilhada da nuvem;
b) Mapear a aplicação de técnicas criptográficas ao longo de todo o ciclo de vida dos dados (em trânsito, em repouso e em uso, abordando computação confidencial);
c) Estudar a gestão de chaves criptográficas (KMS) e os modelos de soberania de dados (BYOK/HYOK) como ferramentas centrais de controle do Controlador;

d) Discutir a técnica de *crypto-shredding* (fragmentação criptográfica) como método de exclusão segura de dados alinhado às exigências da LGPD;
e) Examinar casos reais de falhas de segurança no Brasil, analisando-os sob a perspectiva da falha na gestão criptográfica;
f) Sugerir boas práticas para organizações se adequarem às normas legais.

A justificativa deste trabalho é baseada na relevância social, acadêmica e profissional do tema. Do ponto de vista social, a proteção da privacidade é um direito fundamental que precisa ser assegurado diante do avanço da tecnologia. Do ponto de vista acadêmico, o estudo contribui para ampliar a compreensão sobre a conexão entre tecnologia, segurança e legislação, fornecendo contribuições para pesquisas futuras. Já no âmbito profissional, o tema se torna essencial para orientar empresas e profissionais de tecnologia na adoção de soluções seguras e compatíveis com a legislação vigente, fortalecendo a confiança de clientes e colaboradores.

A metodologia adotada caracteriza-se como uma pesquisa de natureza qualitativa, com abordagem exploratória e descritiva, fundamentada em revisão bibliográfica e documental. Foram analisados artigos científicos de revistas e conferências de alta relevância, livros-texto fundamentais da área de segurança, além de documentos legais, como a própria LGPD e guias da Autoridade Nacional de Proteção de Dados (ANPD), e padrões técnicos internacionais de segurança e Publicações Especiais (SPs) do NIST (National Institute of Standards and Technology).

2 REFERENCIAL TEÓRICO

2.1 Computação em Nuvem e o Modelo de Responsabilidade Compartilhada

A computação em nuvem transformou profundamente a forma como indivíduos e organizações armazenam, processam e compartilham informações. Essa tecnologia baseia-se na disponibilização de recursos computacionais pela internet, de modo que o usuário possa acessar serviços sob demanda, sem a necessidade de infraestrutura física local. Segundo Nunes e Garreto (2023), a nuvem oferece escalabilidade, flexibilidade e economia, permitindo que empresas reduzam custos e aumentem sua eficiência operacional.

Os modelos de serviço mais comuns são o Software as a Service (SaaS), o Platform as a Service (PaaS) e o Infrastructure as a Service (IaaS) (Nunes; Garreto, 2023). Essa diversidade de modelos, embora estratégica, cria um cenário de segurança complexo, governado pelo Modelo de Responsabilidade Compartilhada.

Neste modelo, o provedor de nuvem (ex: Amazon, Google, Microsoft) é responsável pela segurança *da* nuvem (ou seja, a infraestrutura física, o hardware e o software de base), enquanto o cliente é responsável pela segurança *na* nuvem (seus dados, aplicações, configurações de rede e gerenciamento de identidade) (Amazon Web Services, 2024).

Essa distinção é crucial para a conformidade com a Lei Geral de Proteção de Dados (LGPD). Legalmente, o cliente que contrata o serviço e insere os dados pessoais é definido como o Controlador, sendo o principal responsável perante o titular dos dados. O provedor de nuvem atua como Operador, tratando os dados em nome do Controlador. O Artigo 39 da LGPD estabelece que o Operador deve realizar o tratamento segundo as instruções fornecidas pelo Controlador, que, por sua vez, deve verificar o cumprimento das medidas de segurança (Brasil, 2018).

A falha em gerenciar de maneira adequada essa responsabilidade do Controlador eleva o risco de ataques cibernéticos, vazamentos e acessos indevidos. Como destaca Calgaro (2021), o armazenamento em servidores externos exige medidas de segurança sofisticadas. As vulnerabilidades mais comuns surgem de falhas de configuração por parte do cliente, uso de senhas fracas, má gestão de permissões e, especialmente, a ausência de criptografia robusta aplicada aos dados.

2.2 Fundamentos da Criptografia Moderna

A criptografia é um dos pilares fundamentais da segurança da informação, sendo responsável por transformar dados legíveis (texto claro) em códigos incompreensíveis (texto criptografado) para quem não possui a chave correta.

De acordo com NIST (2020), os métodos criptográficos são divididos em criptografia simétrica, criptografia assimétrica e criptografia híbrida.

Na criptografia simétrica, a mesma chave é utilizada para cifrar e decifrar as informações. Isso garante alta velocidade de processamento, sendo ideal para grandes volumes de dados.

Exemplos incluem os algoritmos AES (*Advanced Encryption Standard*) e DES (*Data Encryption Standard*) (NIST, 2023).

Já a criptografia assimétrica utiliza um par de chaves matematicamente vinculadas: uma pública (que pode ser compartilhada) e outra privada (que deve ser mantida em sigilo). Ela é amplamente utilizada em processos de autenticação e troca segura de chaves simétricas, com destaque para o algoritmo RSA (*Rivest–Shamir–Adleman*).

Nos últimos anos, surgiu uma abordagem híbrida, que combina a rapidez da criptografia simétrica para cifrar os dados com a segurança da assimétrica para proteger a chave simétrica. Outro avanço importante é o uso de algoritmos baseados em curvas elípticas (*Elliptic Curve Cryptography* – ECC), que oferecem níveis elevados de segurança com tamanhos de chave menores (Shukla; Dwivedi; Trivedi, 2021).

2.3 A Criptografia Aplicada ao Ciclo de Vida dos Dados na Nuvem

A LGPD exige que a proteção de dados pessoais abranja todo o seu "ciclo de vida" ou "tratamento", desde a coleta até a eliminação (Art. 5º) (BRASIL, 2018). No ambiente de nuvem, a criptografia é a principal medida técnica para garantir essa proteção em três estágios distintos: em trânsito, em repouso e em uso.

2.3.1 Proteção de Dados em Trânsito

Refere-se à proteção dos dados enquanto são transferidos entre o dispositivo do usuário e o servidor na nuvem, ou entre diferentes microsserviços dentro da própria nuvem. A interceptação desses dados (ataques *man-in-the-middle*) é um risco comum. Para mitigá-lo, utilizam-se protocolos de comunicação segura como o TLS (*Transport Layer Security*) — a base do HTTPS — e VPNs (*Virtual Private Networks*) para criar canais de comunicação confidenciais e autenticados (NIST, 2019).

2.3.2 Proteção de Dados em Repouso

Uma vez que os dados chegam à nuvem, eles são armazenados em discos (para os sistemas operacionais e aplicações), bancos de dados (para dados estruturados) ou armazenamento de objetos (usado para arquivos e backups). A proteção de dados em repouso envolve criptografar esses arquivos armazenados, geralmente com algoritmos simétricos como o AES-256. Desta forma, mesmo que um invasor obtenha acesso físico ou lógico aos discos de armazenamento, os dados permanecerão ilegíveis e inúteis sem a chave de decifração correspondente (NIST, 2023).

2.3.3 Proteção de Dados em Uso

Este é o maior desafio da segurança em nuvem. "Dados em uso" são aqueles que estão sendo processados ativamente pela CPU ou carregados na memória RAM. Tradicionalmente, os dados precisam ser descriptografados na memória para que o processador possa realizar cálculos sobre eles, criando uma janela de vulnerabilidade (Ahmad et al., 2023).

Novas tecnologias buscam resolver isso. A Computação Confidencial como o Intel SGX cria ambientes de execução confiáveis na CPU, onde os dados podem ser processados de forma isolada e criptografada, protegidos até mesmo do provedor de nuvem. Ao mesmo tempo, a criptografia homomórfica permite que operações matemáticas sejam realizadas diretamente sobre os dados criptografados, garantindo que o dado jamais seja exposto em sua forma original (Ahmad et al., 2023).

2.3.4 A Exclusão Segura via "Crypto-Shredding"

A LGPD exige que os dados sejam eliminados após o término de sua finalidade. Em ambientes de nuvem, devido à cópia de dados e backups, a exclusão física é complexa e difícil de verificar. A solução mais eficaz é o "Crypto-Shredding" (fragmentação criptográfica). Ao invés de tentar apagar o dado (que pode ter múltiplas cópias), destrói-se permanentemente a chave criptográfica associada a ele. Sem a chave, o dado cifrado torna-se um lixo digital irrecuperável, o que é o mesmo que a sua eliminação segura, para fins práticos e legais (NIST, 2014).

2.4 O Desafio Crítico: Gerenciamento de Chaves Criptográficas (KMS)

A eficácia de toda a estratégia de criptografia (descrita na Seção 2.3) depende de um único ponto: a segurança das chaves criptográficas. Um sistema criptográfico é tão forte quanto o seu gerenciamento de chaves (NIST, 2020). Se um invasor obtém a chave, a criptografia se torna inútil. Em ambientes de nuvem, a gestão de quem cria, armazena, rotaciona e destrói essas chaves é um ponto central de controle e conformidade com a LGPD.

2.4.1 *Key Management Systems* (KMS)

Os principais provedores de nuvem oferecem serviços de Gerenciamento de Chaves (KMS), como o AWS KMS, Google Cloud KMS e Azure Key Vault (Amazon Web Services, 2024; Microsoft, 2024; Google Cloud, 2024). Essas plataformas são projetadas para centralizar a gestão do ciclo de vida das chaves, utilizando Módulos de Segurança de Hardware para protegê-las contra acesso indevido. Elas permitem que o Controlador (o cliente) defina políticas detalhadas de quem pode usar quais chaves para quais operações (ex: "o serviço A pode cifrar, mas não pode decifrar"), criando registros de auditoria essenciais (NIST, 2020).

2.4.2 Controle do Controlador: BYOK e HYOK

Para organizações que exigem um nível ainda maior de domínio sobre seus dados, em total alinhamento com a LGPD, existem modelos avançados de gestão (Microsoft, 2024; Google Cloud, 2024):

a) BYOK (*Bring Your Own Key*): O Controlador gera sua própria chave de criptografia em seu ambiente local (*on-premises*) e a "importa" de forma segura para o KMS do provedor de nuvem. O provedor gerencia o uso da chave, mas não sua origem.
b) HYOK (*Hold Your Own Key*): Este é o modelo mais rigoroso. O Controlador mantém sua chave mestra em um Módulo de Segurança de Hardware (HSM) próprio, fora da nuvem. O provedor de nuvem jamais tem acesso direto à chave, apenas solicita operações a ela. Isso garante que o Controlador mantenha o controle absoluto, impedindo que até mesmo o provedor de nuvem possa, sob qualquer circunstância, decifrar os dados do cliente.

2.5 A Lei Geral de Proteção de Dados e o Princípio da Segurança

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um marco na regulamentação da privacidade no Brasil. Segundo Machado (2019), a LGPD impõe às organizações o dever de adotar medidas técnicas e administrativas para prevenir incidentes.

Entre os princípios fundamentais da LGPD, destacam-se: a) Finalidade e adequação; b) Necessidade; c) Transparência; d) Segurança (Brasil, 2018).

O Artigo 46 da lei é explícito ao determinar que o Controlador e o Operador devem empregar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (Brasil, 2018).

A criptografia é a principal "medida técnica" para este fim. Como Teffé (2023) aponta, ela garante que mesmo em caso de invasão, os dados permaneçam ilegíveis. Portanto, a aplicação das técnicas de proteção do ciclo de vida (Seção 2.3) e a gestão robusta de chaves (Seção 2.4) não são apenas boas práticas, mas um cumprimento direto da exigência legal de segurança.

2.6 Análise de Casos de Vazamentos de Dados no Brasil

Mesmo com o avanço das tecnologias de proteção, os vazamentos de dados continuam sendo uma das maiores ameaças à privacidade.

Um exemplo emblemático ocorreu em 2018, quando o Banco Inter sofreu um vazamento. Segundo Bisso et al. (2019), esse caso ilustra como a ausência de mecanismos robustos pode resultar em prejuízos significativos, uma ameaça que é traduzida em custos milionários, segundo dados globais e regionais sobre incidentes de segurança (IBM, 2024). Analisando este caso sob a perspectiva deste referencial, o incidente evidencia falhas na proteção de dados em repouso (Seção 2.3.2), pois os bancos de dados não estavam adequadamente criptografados, permitindo a extração dos dados em texto claro.

Outro caso nacional, como o vazamento de dados do Ministério da Saúde, demonstra que a falta de criptografia adequada e, crucialmente, a inexistência de uma gestão de chaves centralizada (Seção 2.4) — resultando em chaves de acesso ou credenciais expostas no código ou em servidores vulneráveis — são falhas recorrentes. O erro humano e a falha na configuração de

segurança são, de fato, os vetores de ataque mais comuns e de alto impacto no cenário global de cibersegurança (IBM, 2024).

Esses casos mostram a importância da criptografia, tanto para prevenir problemas quanto para estar em dia com a LGPD. Isso acontece porque a lei pode aliviar as punições de quem usou as medidas técnicas certas, mesmo que um problema de segurança ocorra (Esper, 2022).

2.7 Boas Práticas e Recomendações para Conformidade

A proteção de dados pessoais não se limita ao uso de tecnologias avançadas. Envolve também gestão, conscientização da equipe e treinamento contínuo.

Entre as boas práticas técnicas, destacam-se: a) Implementação de criptografia (conforme Seção 2.3) e pseudonimização de dados sensíveis; b) Adoção de firewalls e monitoramento contínuo de rede; c) Execução de backups regulares (preferencialmente criptografados); d) Um controle rígido sobre quem pode acessar o quê (dando sempre o mínimo de permissão possível) e usar a verificação em duas etapas; e) Uso de conexões seguras (HTTPS, VPN, TLS) para dados em trânsito (ANPD, 2024).

No campo administrativo, é essencial desenvolver uma Política de Segurança da Informação, realizar treinamentos e nomear o encarregado pelo tratamento de dados pessoais. Como destacam Nunes e Garreto (2023), certificações como a ISO/IEC 27001 são instrumentos eficazes para estruturar a gestão de segurança.

2.7.1 Recomendações Formais da Autoridade Nacional de Proteção de Dados (ANPD)

Para além das boas práticas, a própria ANPD tem reforçado a importância das medidas técnicas. Em seu "Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte" – que, embora focado nesse público, estabelece uma linha de base de diligência esperada para todos os agentes –, a autoridade recomenda explicitamente "utilizar criptografia para o armazenamento de dados pessoais" sempre que possível, e "utilizar conexões seguras (HTTPS/TLS)" para a transmissão de dados (ANPD, 2024).

Isso muda o status da criptografia de sugestão para ação esperada pela autoridade. Isso é fundamental para provar as boas intenções e o cuidado do Controlador caso ocorra um incidente de segurança.

3 CONCLUSÃO

Este trabalho de revisão bibliográfica buscou responder ao problema central: de que maneira a criptografia pode garantir a proteção dos dados pessoais e manter a conformidade com a Lei Geral de Proteção de Dados (LGPD) no contexto da computação em nuvem. A análise de bibliografia técnica, jurídica e dos padrões internacionais (como os do NIST) permitiu uma compreensão aprofundada da conexão entre essas três áreas.

Concluiu-se que a conformidade com a LGPD em ambientes de nuvem não é alcançada apenas pela implementação de algoritmos criptográficos robustos, mas sim por uma abordagem estratégica que une a proteção técnica à gestão legal. A hipótese central do estudo foi confirmada: a eficácia da criptografia está diretamente ligada à capacidade do Controlador (o cliente) de manter o controle total sobre os dados.

A pesquisa demonstrou que essa maneira de garantir a proteção se materializa em duas frentes principais, detalhadas no referencial teórico:

a) A Aplicação da Criptografia em todo o Ciclo de Vida do Dado (Seção 2.3): A proteção eficaz exige que os dados sejam criptografados não apenas em trânsito (via TLS) e em repouso (via AES), mas também durante sua exclusão (através do *crypto-shredding*) e, de forma crescente, durante seu processamento (com a computação confidencial e criptografia homomórfica).
b) O Gerenciamento de Chaves como Ferramenta de Controle (Seção 2.4): Este foi identificado como o ponto mais crítico. A gestão centralizada de chaves (KMS) e o uso de modelos como BYOK (Bring Your Own Key) são os mecanismos técnicos que permitem ao Controlador cumprir suas obrigações legais, garantindo que apenas ele tenha o poder de decifrar as informações, independentemente de estarem no ambiente de um Operador (o provedor de nuvem).

A análise teórica do Modelo de Responsabilidade Compartilhada (Seção 2.1) e do Artigo 46 da LGPD (Seção 2.5) reforça que as medidas técnicas exigidas pela lei equivalem à capacidade de controle criptográfico. Os casos de vazamentos de dados no Brasil (Seção 2.6) não

ocorreram por falhas nos algoritmos, mas sim por falhas de implementação, como a ausência de criptografia em repouso e, principalmente, a gestão inadequada de chaves e credenciais de acesso.

Dessa forma, conclui-se que a governança de chaves é indispensável para a integração entre criptografia e LGPD na nuvem. Não basta ao Controlador "ligar a criptografia"; ele deve gerenciá-la ativamente para provar seu cuidado e manter o controle. A adoção dessas práticas, alinhadas às recomendações da ANPD (Seção 2.7.1), é o caminho que transforma a criptografia de uma ferramenta de segurança em um pilar de conformidade legal.

Por fim, recomenda-se que pesquisas futuras aprofundem o estudo das tecnologias de proteção de dados em uso (Seção 2.3.3), como a Computação Confidencial e a Criptografia Homomórfica. Embora ainda apresentem desafios de desempenho e custo, essas tecnologias representam o próximo patamar na garantia da privacidade total em ambientes de nuvem, solucionando vulnerabilidades que a criptografia tradicional, por si só, não consegue solucionar.

REFERÊNCIAS

AHMAD, F.; et al. A Review on Security of Cloud Data Using Fully Homomorphic Encryption. **Electronics**, v. 12, n. 10, p. 2290, 2023. DOI: 10.3390/electronics12102290. Disponível em: https://www.mdpi.com/2079-9292/12/10/2290. Acesso em: 25 out. 2025.

AMAZON WEB SERVICES (AWS). **Modelo de Responsabilidade Compartilhada**. 2024. Disponível em: https://aws.amazon.com/pt/compliance/shared-responsibility-model/. Acesso em: 25 out. 2025.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte.** Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em: 25 out. 2025.

BISSO, R.; KREUTZ, D.; RODRIGUES, G.; PAZ, G. Vazamentos de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. In: **ANAIS DO WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE**, 3, 2019. Anais [...] Brasília, 2019. p. 43–52. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/9230. Acesso em: 25 out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**: Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 out. 2025.

CALGARO, Alexandre Leal. Segurança em computação na nuvem. **Revista FT**, v. 25, n. 88, p. 1-20, 2021. Disponível em: https://www.researchgate.net/publication/383989447_SEGURANCA_EM_COMPUTACAO_NA_NUVEM. Acesso em: 25 out. 2025.

ESPER, A. S. L. **LGPD 2022**: debates e temas relevantes. Recife: Império Jurídico, 2022. Disponível em: https://www.d2smart.com.br/wp-content/uploads/2022/10/LGPD_Ebook.pdf. Acesso em: 25 out. 2025.

GOOGLE CLOUD. **Cloud External Key Manager**. Google Cloud Documentation, 2024. Disponível em: https://cloud.google.com/kms/docs/ekm. Acesso em: 26 out. 2025.

IBM. **Cost of a Data Breach Report** 2024. [S.l.]: IBM Security, 2024. Disponível em: https://www.ibm.com/downloads/documents/br-pt/137a3e32273ed1f5. Acesso em: 25 out. 2025.

MACHADO, Marcelo Fernandes. **Medidas de proteção de dados pessoais no planejamento e operação de smart grid utilizando computação em nuvem**: estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil. 2019. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Tecnológica Federal do Paraná, Curitiba, 2019. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/4618. Acesso em: 25 out. 2025.

MICROSOFT. **Especificação Bring Your Own Key (BYOK) do Azure Key Vault. Microsoft Learn**, 2024. Disponível em: https://learn.microsoft.com/pt-br/azure/key-vault/keys/byok-specification. Acesso em: 25 out. 2025.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-88 Rev. 1: **Guidelines for Media Sanitization. Gaithersburg**, MD: NIST, 2014. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. Acesso em: 25 out. 2025.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-52 Rev. 2: **Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Gaithersburg,** MD: NIST, 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf. Acesso em: 25 out. 2025.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-**57 Part 1 Rev. 5: Recommendation for Key Management. Gaithersburg, MD**: NIST, 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf. Acesso em: 25 out. 2025.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **SP 800-175B Rev. 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. Gaithersburg,** MD: NIST, 2023. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf. Acesso em: 25 out. 2025.

NUNES, M. N. D. C.; GARRETO, C. G. **Uma visão abrangente da computação** – Volume 2. 1. ed. [S. l.]: Editora Pascal LTDA, 2023. DOI: 10.29327/5280411. Disponível em: https://editorapascal.com.br/2023/07/06/uma-visao-abrangente-da-computacao-volume-2/. Acesso em: 25 out. 2025.

SHUKLA, D. K.; DWIVEDI, V. K. R.; TRIVEDI, M. C. Encryption algorithm in cloud computing. Materials Today: **Proceedings,** [S. l.], v. 37, p. 1869–1875, 2021. Disponível em: https://doi.org/10.1016/j.matpr.2020.07.452. Acesso em: 25 out. 2025.

TEFFÉ, C. de. Plataformas digitais e proteção de dados pessoais. In: **Diálogos da pós-graduação em Direito Digital.** Rio de Janeiro, RJ: ITS - Instituto de Tecnologia e Sociedade, 2023. Disponível em: https://itsrio.org/wp-content/uploads/2016/12/20231023_Livro_Pos_ITS-UERJ_Plataformas-digitais-protecao-de-dados_COMPLETO.pdf. Acesso em: 25 out. 2025.