A LGPD através da criptografia em empresas privadas: Uma revisão da literatura(*)

LGPD through encryption in private companies: A literature review

LGPD a través del cifrado en empresas privadas: una revisión de la literatura

Marco Aurelio Muniz de Pontes[1]

Diogo Severino Ramos da Silva[2]

RESUMO

Objetivo: Apresentar a evolução tecnológica dentro das empresas privadas, através da criptografia em consonância com a Lei Geral de Proteção de Dados. **Método:** Trata-se de uma revisão da literatura que trata sobre a LGPD e a criptografia, e como ambas pode proporcionar um ambiente de segurança nas empresas privadas. Os dados bibliográficos foram coletados dentro da base de dados da Biblioteca Virtual de Saúde- BVS, livros e sites jurídicos externos. Como descritores, utilizamos "Dados Criptografados, Proteção de Dados, Setor privado". Para construção deste artigo, foram incluídos trabalhos, livros e artigos que tratavam da temática abordada, a Lei Geral de Proteção de dados, surgimento da criptografia, utilização de segurança cibernética em empresas privadas. Como critério de exclusão, eliminamos o ramo do terceiro setor, trabalhos escritos com datas abaixo do ano de 2015, leis brasileiras elaboradas que não condiz com segurança virtual. **Resultados:** o surgimento da 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 o estado estão cada vez vulneráveis a espionagem ou de ataques de Hackers como evidenciado as divulgações de áudios de empresas e dos principais poderes do Brasil. Com essas narrativas justificamos o aumento de investimento nos setores de TI corporativo, tomando ações para que problemas com vazamento de dados, ou problemas com informações de terceiros não prospere. **Conclusão:** A implementação de criptografia como medida de segurança oferece não apenas conformidade legal, mas também uma defesa robusta contra ameaças cibernéticas em um ambiente digital cada vez mais complexo. Empresas que adotam essa abordagem não apenas protegem os interesses de seus clientes e colaboradores, mas também posicionam-se como líderes éticos em seus setores.

(*) Recibido: 05/10/2022 | Aceptado: 12/11/2022 | Publicación en línea: 30/12/2022.

[1] Graduado em direito. Especialista em Bioética e Biodireito pela Faculdade dos Palmares (FAP). Membro da Comissão de Perícias Forenses do Estado de Pernambuco. Email: marcoaureliopontesadv@gmail.com. ORCID: https://orcid.org/0009-0002-8049-2975

[2] Professor do Curso de Direito da Faculdade Católica Imaculada Conceição do Recife. Mestre em Perícias Forenses pela Universidade de Pernambuco. E-mail: diogoramos.adv@gmail.com. ORCID: https://orcid.org/0000-0002-3149-7756. Lattes: http://lattes.cnpq.br/0713261804075770

Descritores: Dados Criptografados, Proteção de Dados, Setor privado.

SUMMARY

Objective: To present technological evolution within private companies, through encryption in line with the General Data Protection Law. **Method:** This is a review of the literature that deals with LGPD and encryption, and how both can provide a security environment in private companies. Bibliographic data were collected within the Virtual Health Library - VHL database, books and external legal websites. As descriptors, we use “Encrypted Data, Data Protection, Private Sector”. To construct this article, works, books and articles were included that dealt with the topic addressed, the General Data Protection Law, the emergence of encryption, the use of cybersecurity in private companies. As an exclusion criterion, we eliminated the third sector branch, written works with dates below the year 2015, Brazilian laws drawn up that do not comply with virtual security. **Results:** the emergence of globalization and the development of new technologies, develops an increasingly voracious competition between companies, developing questions about the security of corporate information and that of its customers. Companies and the state are increasingly vulnerable to espionage or hacker attacks, as evidenced by the release of audio recordings from companies and the main powers in Brazil. With these narratives we justify the increase in investment in the corporate IT sectors, taking actions so that problems with data leaks, or problems with third-party information do not prosper. **Conclusion:** Implementing encryption as a security measure provides not only legal compliance, but also a robust defense against cyber threats in an increasingly complex digital environment. Companies that adopt this approach not only protect the interests of their customers and employees, but also position themselves as ethical leaders in their industries.

Descriptors: Encrypted Data, Data Protection, Private sector.

RESUMEN

Objetivo: Presentar la evolución tecnológica dentro de la empresa privada, a través del cifrado en línea con la Ley General de Protección de Datos. **Método:** Esta es una revisión de la literatura que trata sobre LGPD y el cifrado, y cómo ambos pueden proporcionar un entorno de seguridad en empresas privadas. Los datos bibliográficos fueron recolectados dentro de la Biblioteca Virtual en Salud - base de datos de la BVS, libros y sitios jurídicos externos. Como descriptores utilizamos “Datos cifrados, Protección de datos, Sector privado”. Para la construcción de este artículo se incluyeron obras, libros y artículos que abordaron el tema abordado, la Ley General de Protección de Datos, el surgimiento de la encriptación, el uso de la ciberseguridad en la empresa privada. Como criterio de exclusión, eliminamos la rama del tercer sector, trabajos escritos con fechas inferiores al año 2015, leyes brasileñas redactadas que no cumplen con la seguridad virtual. **Resultados:** el surgimiento de la globalización y el desarrollo de nuevas tecnologías, desarrolla una competencia cada vez más voraz entre las empresas, desarrollándose interrogantes sobre la seguridad de la información corporativa y la de sus clientes. Las empresas y el Estado son cada vez más vulnerables al espionaje o ataques de piratas informáticos, como lo demuestra la divulgación de grabaciones de audio de empresas y de las principales potencias de Brasil. Con estas narrativas justificamos el aumento de la inversión en los sectores corporativos de TI, tomando acciones para que no prosperen los problemas de fuga de datos, o problemas con información de terceros. **Conclusión:** La implementación del cifrado como medida de seguridad proporciona no solo cumplimiento legal, sino también una defensa sólida contra las amenazas cibernéticas en un entorno digital cada vez más complejo. Las empresas que adoptan este enfoque no sólo protegen los intereses de sus clientes y empleados, sino que también se posicionan como líderes éticos en sus industrias.

Descriptores: Datos cifrados, Protección de datos, Sector privado.

1 INTRODUÇÃO

Após vazamento de dados da população brasileira em 2021, rotulado de Vazamento de Dados do Fim do Mundo, revelou dados de brasileiros, vivos e mortos, expondo CPFs, e-mails, telefones de mais de 223,7 milhões de indivíduos. Esse episódio somente foi descoberto após os dados terem sido colocados à venda na internet. O que ainda não se tem conhecimento é a fonte onde esses dados foram obtidos, porém sabe-se que alguns fazem referências a empresas e serviços, assim é possível que sua origem pode ser de diversas fontes (Mello & Corino, 2022, p.1).

A Lei Geral de Proteção de Dados (LGPD) foi um marco significativo na regulamentação da privacidade no cenário empresarial brasileiro. Com a crescente preocupação em relação à segurança e privacidade das informações pessoais, as empresas privadas estão buscando meios eficazes para se adequar às exigências da LGPD, garantindo a proteção adequada dos dados de seus clientes e colaboradores. Um dos requisitos da LGPD é a implementação de estratégias de criptografia. Ela serve como ferramenta de segurança, desempenha um papel crucial na proteção dos dados sensíveis, tornando-os ininteligíveis para terceiros não autorizados.

Este artigo busca realizar uma revisão da literatura sobre a integração da criptografia como uma medida essencial no contexto da LGPD, concentrando-se nas práticas e desafios enfrentados por empresas privadas na implementação eficaz dessas tecnologias de segurança.

No comparativo entre a LGPD e a criptografia, esta revisão visa fornecer uma compreensão abrangente das estratégias adotadas por empresas para garantir conformidade com a legislação de proteção de dados, ao mesmo tempo em que preserva a eficácia operacional e a confiança dos clientes.

> A LGPD é a lei nº 13.709, aprovada em agosto de 2018 e com vigência a partir de agosto de 2020. Para entender a importância do assunto, é necessário saber que a nova lei quer criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja

confusão, a lei traz logo de cara o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação. Ela estabelece ainda que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida. Determina também que é permitido compartilhar dados com organismos internacionais e com outros países, desde que isso ocorra a partir de protocolos seguros e/ou para cumprir exigências legais (SERPRO, 2024).

A tabela abaixo, apresenta o funcionamento da LGPD:

Consentimento	O consentimento do cidadão é a base para que dados pessoais possam ser tratados. Mas há algumas exceções a isso. É possível tratar dados sem consentimento se isso for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.
Automatização com autorização	É essencial saber que a lei traz várias garantias ao cidadão, que pode solicitar que dados sejam deletados, revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações. E o tratamento dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão. Por exemplo, se a finalidade de um tratamento, feito exclusivamente de modo automatizado, for construir um perfil (pessoal, profissional, de consumo, de crédito), o indivíduo deve ser informado que pode intervir, pedindo revisão desse procedimento feito por máquinas.
ANPD e agentes de tratamento	A instituição vai fiscalizar e, se a LGPD for descumprida, penalizar. Além disso, a ANPD terá, é claro, as tarefas de regular e de orientar, preventivamente, sobre como aplicar a lei. Cidadãos e organizações

	poderão colaborar com a autoridade. Mas não basta a ANPD - que está em formação - e é por isso que a Lei Geral de Proteção de Dados Pessoais também estipula os agentes de tratamento de dados e suas funções, nas organizações: tem o controlador, que toma as decisões sobre o tratamento; o operador, que realiza o tratamento, em nome do controlador; e o encarregado, que interage com cidadãos e autoridade nacional (e poderá ou não ser exigido, a depender do tipo ou porte da organização e do volume de dados tratados).
Gestão em foco	A administração de riscos e falhas. Isso quer dizer que quem gere base de dados pessoais terá que redigir normas de governança; adotar medidas preventivas de segurança; replicar boas práticas e certificações existentes no mercado. Terá ainda que elaborar planos de contingência; fazer auditorias; resolver incidentes com agilidade. Se ocorrer, por exemplo, um vazamento de dados, a ANPD e os indivíduos afetados devem ser imediatamente avisados. Vale lembrar que todos os agentes de tratamento sujeitam-se à lei. Isso significa que as organizações e as subcontratadas para tratar dados respondem em conjunto pelos danos causados. E as falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil – e no limite de R$ 50 milhões por infração. A autoridade nacional fixará níveis de penalidade segundo a gravidade da falha. E enviará, é claro, alertas e orientações antes de aplicar sanções às organizações.

Fonte: SERPRO. Acesso em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd

Assim, a investigação detalhada sobre como a criptografia pode ser eficazmente incorporada no ambiente empresarial em conformidade com a LGPD, e é essencial para informar práticas futuras e promover um ambiente digital mais seguro e ético para todas as partes envolvidas.

Este artigo tem como objetivo apresentar a evolução tecnológica dentro das empresas privadas, através da criptografia em consonância com a Lei Geral de Proteção de Dados.

2 MÉTODO

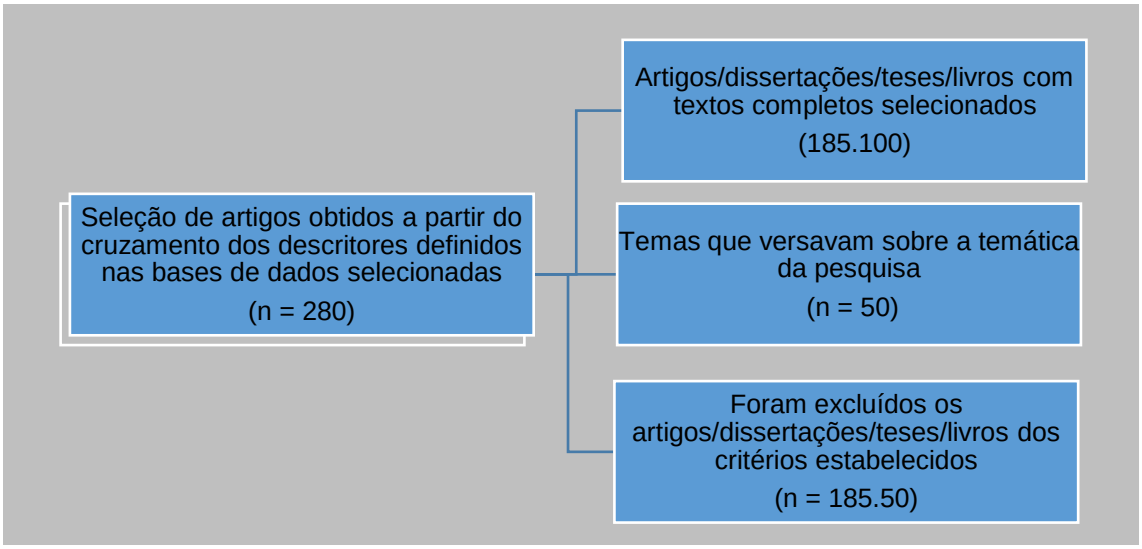
Trata-se de uma revisão da literatura que trata sobre a LGPD e a criptografia, e como ambas pode proporcionar um ambiente de segurança nas empresas privadas.

Os dados bibliográficos foram coletados dentro da base de dados da Biblioteca Virtual de Saúde- BVS, livros e sites jurídicos externos. Como descritores, utilizamos “Dados Criptografados, Proteção de Dados, Setor privado”.

Para construção deste artigo, foram incluídos trabalhos, livros e artigos que tratavam da temática abordada, a Lei Geral de Proteção de dados, surgimento da criptografia, utilização de segurança cibernética em empresas privadas.

Como critério de exclusão, eliminamos o ramo do terceiro setor, trabalhos escritos com datas abaixo do ano de 2015, leis brasileiras elaboradas que não condiz com segurança virtual.

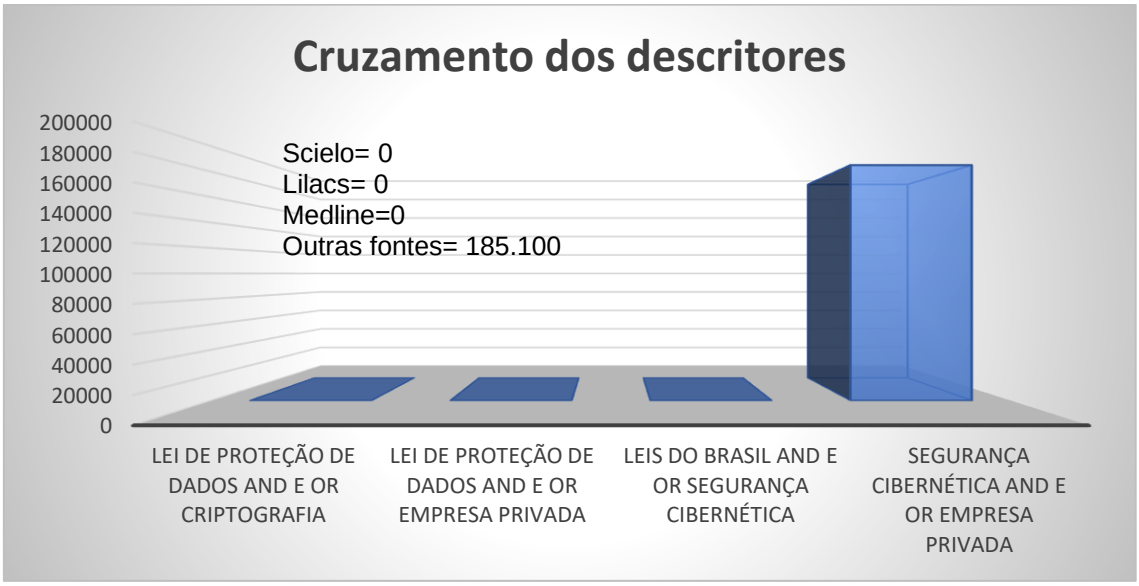
Como achados, foram levantados em torno de 280 artigos, livros, dissertações e teses; analisamos minuciosamente 150 trabalhos, restando 50 pesquisas para realizar nosso artigo.



Fonte: Elaboração própria em 2024.

3 RESULTADOS

O fluxograma a seguir, apresenta os resultados da busca da pesquisa:



Fonte: Biblioteca virtual em saúde. Acesso em https://decs.bvsalud.org/ do dia 14 fev. 2024. Outras fontes de acesso extraídas dez. a fev. 2024

Segundo os resultados, o surgimento da 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 o estado estão cada vez vulneráveis a espionagem ou de ataques de Hackers como evidenciado as divulgações de áudios de empresas e dos principais poderes do Brasil.Com essas narrativas justificamos o aumento de investimento nos setores de TI corporativo, tomando ações para que problemas com vazamento de dados, ou problemas com informações de terceiros não prospere. Não seria nenhuma novidade se casos de empresas que fazem o uso de forma incorreta dos dados de seus clientes, vendendo ou fornecendo os dados pessoais sem a conscientização e consentimento deles (Lima Rapôso et al. 2019, p.2).

Podemos verificar que ao implementar criptografia nas operações das empresas privadas, estas permitem que atendam aos requisitos legais da LGPD, demonstrando compromisso com a proteção de dados pessoais e evitando possíveis penalidades e multas.

A criptografia proporciona uma camada adicional de segurança, garantindo a proteção eficaz dos dados sensíveis, o que reduz o risco de violações de segurança e potenciais danos à reputação da empresa. Ao adotar medidas proativas para proteger a privacidade dos dados, as empresas podem ganhar a confiança dos clientes e isso pode resultar em fidelização de clientes e uma imagem positiva da marca.

No que tange aos riscos de acesso não autorizado e vazamentos de dados, ela contribui para um ambiente digital mais seguro. Essa redução de riscos é crucial em um cenário onde as ameaças cibernéticas estão em constante evolução. As empresas que adotam práticas sólidas de proteção de dados, incluindo criptografia em conformidade com normas como a LGPD, podem se destacar internacionalmente, ganhando uma vantagem competitiva em mercados globais.

Para Lunkes & Borges (2022, p.1), a criptografia utiliza técnicas de computação e matemática para transformar informações em códigos, ou seja, técnicas para comunicação segura na presença de terceiros, chamados atacantes ou Eve, um exemplo de como isso ocorre na computação em nuvem, que executa determinadas funções computáveis nos dados, preservando os recursos da função utilizada e o formato dos dados criptografados. Esse crescimento no uso de tecnologias, tanto na indústria quanto no cotidiano, e a demanda de aplicativos para facilitar a conexão nas redes sociais, transações bancárias, armazenamentos de arquivos, seja em celulares ou computadores, salientamos uma preocupação com a segurança e privacidade dos dados.

4 DISCUSSÃO

É possível observar a importância de seguir as regras da LGPD e a implantação da criptografia em empresas privadas, assim como é necessário a associação positiva entre a ênfase em aprendizagem contínua na cultura das empresas e as atitudes dos funcionários em relação às oportunidades de crescimento nas organizações, sem que aja constrangimento e sendo maior nas empresas onde há maior ênfase em aprendizagem. Além disso, a força da aprendizagem contínua na cultura das empresas também está positivamente

associada a uma maior cidadania organizacional e importância do desempenho formal nos grupos estudados por via da percepção de oportunidade de crescimento (Cavazotte, Moreno jr, Turano, 2015, p.17).

Segundo o Ministério Público Federal (2024):

> A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes. A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes. Esclarece ainda que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação. Além disso, a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. A lei autoriza também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos (MPF, 2024).

Se tratando da história da criptografia, Sousa et al. (2020, p.1), explica que o problema de comunicação clássico em que dois entes (Alice e Bob) buscam se comunicar de forma segura mesmo na presença de um adversário (Eve) capaz de acessar, ler, ou mesmo modificar o canal de comunicação. Pode-se afirmar que a criptografia é plenamente capaz de resolver esse problema, através de algoritmos de sigilo, troca de chaves, resumo e assinatura digital, que garantem a autenticidade, confidencialidade e integridade da comunicação. Portanto, soluções de comunicação por texto ou voz, videoconferências, acesso remoto via redes privadas virtuais (VPN) e similares podem, se bem

implementadas, prover segurança suficiente para proteger tanto a privacidade dos usuários quanto a própria empresa que se responsabiliza pelos dados, garantindo a conformidade com a lei. A criptografia sempre foi importante para garantir a segurança das informações e das comunicações, proteger o sigilo de conhecimentos e de documentos sensíveis e, na era da informação, tornou-se fundamental para a preservação da privacidade de indivíduos no mundo digital. Ainda assim, tal importância tende a aumentar em virtude das novas leis para a proteção de dados que surgiram, primeiro na Europa com a General Data Protection Regulation (GDPR) e, posteriormente, em vários países ao redor do mundo.

Mediante o contexto, ocorre a grande polêmica sobre moderação e remoção de conteúdo. O artigo 19 do Marco Civil da Internet determina que as empresas não podem ser responsabilizadas por conteúdos publicados por terceiros. Com isto, as empresas retiram conteúdo ou suspendem contas de acordo com as suas políticas e a seu próprio tempo. Muitas vezes após a ocorrência de fatos graves, como ficou demonstrado na invasão do Capitólio em 6 de janeiro de 2021, nos Estados Unidos, e em sua versão brasileira de 8 de janeiro de 2023. De forma semelhante com o que ocorre nos Estados, onde a seção 230 está em revisão pela Suprema Corte, no Brasil, o STF (2023), que discute justamente a constitucionalidade do artigo 19 do Marco Civil da Internet, dentre outros aspectos da lei, que se demonstrou ineficaz na prevenção da disseminação de conteúdo falso e abriu brechas para a perpetuação de crimes contra o próprio Estado (Meireles, 2023, p.19).

CONCLUSÃO

Ao adaptar-se no cenário regulatório em constante evolução, a integração eficaz da Lei Geral de Proteção de Dados (LGPD) com práticas avançadas de criptografia emerge como uma estratégia essencial. Esta revisão da literatura buscou explorar os impactos e benefícios resultantes dessa convergência, destacando os resultados positivos que podem ser alcançados por organizações comprometidas com a proteção de dados sensíveis.

A implementação de criptografia como medida de segurança oferece não

apenas conformidade legal, mas também uma defesa robusta contra ameaças cibernéticas em um ambiente digital cada vez mais complexo. A proteção efetiva dos dados sensíveis não só atende aos requisitos da LGPD, mas também constrói a confiança dos clientes, fortalecendo a reputação da empresa no mercado.

Empresas que adotam essa abordagem não apenas protegem os interesses de seus clientes e colaboradores, mas também posicionam-se como líderes éticos em seus setores; os desafios persistem, desde a implementação técnica até a adaptação cultural dentro das organizações. A constante evolução das ameaças cibernéticas exige uma abordagem ágil e aprimoramento contínuo das estratégias de proteção de dados.

O estudo destaca a importância crucial dessa abordagem e fornece uma base sólida para futuras pesquisas e implementações práticas neste domínio dinâmico e vital.

REFERÊNCIAS

Cavazotte, F. d S. C. N., Moreno Jr, V. d A., Turano, L. M. (2015). *Cultura de aprendizagem contínua, atitudes e desempenho no trabalho: uma comparação entre empresas do setor público e privado*. Rev. Adm. Pública — Rio de Janeiro 49(6):1555-1578. DOI: http://dx.doi.org/10.1590/0034-7612136534

Governo Federal. O que muda com a LGPD? (2024). Acesso em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd

Lima Rapôso, C. F., Melo de Lima, H., de Oliveira Junior, W. F., Ferreira Silva, P. A., & Elaine de Souza Barros, E. . (2019). *LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática*. RACE - Revista De Administração Do Cesmac, *4*, 58–67. https://doi.org/10.3131/race.v4i0.1035

Lunkes, A. d L. Z.; Borges, F. (2022). *Sobre a aplicação de homomorfismo na criptografia*. Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP. DOI: http://dx.doi.org/10.5540/03.2022.009.01.0306

Meireles, A. V. (2023). *Privacidade no século 21: proteção de dados, democracia e modelos regulatórios*. Rev. Bras. Ciênc. Polít. (41) • 2023 • https://doi.org/10.1590/0103-3352.2023.41.265909

Mello, V. C. D; Corino, M. J. V. *Estudo para adequação de um provedor de internet a LGPD* (2022). Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS), Campus Veranópolis – RS – Brasil. Acesso em: https://ifrs.edu.br/veranopolis/wp-content/uploads/sites/10/2022/04/Artigo-TCC-Vinicius-Mello-2022-Pub.pdf

Ministério Público Federal (2024). O que é LGPD? Acesso em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd

Sousa, T. R.; Coutinho, M; Coutinho, L; Albuquerque, R. (2020). *LGPD: Levantamento de Técnicas Criptográficas e de Anonimização para Proteção de Bases de Dados*. In: Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais (SBSEG), 20. Petrópolis. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação. p. 55-68. DOI: https://doi.org/10.5753/sbseg.2020.19227.