Congresso de Segurança da Informação das Fatec

IMPLEMENTAÇÕES PARA A CONFORMIDADE À LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DE CIBERSEGURANÇA

IMPLEMENTATIONS FOR COMPLIANCE WITH THE DATA PROTECTION GENERAL LAW IN CYBERSECURITY AREA

Augusto Finotti Oliveira, Fatec Ourinhos, augusto.oliveira11@fatec.sp.gov.br

Rodrigo Moura Juvenil Ayres, Fatec Ourinhos, rodrigo.ayres@fatec.sp.gov.br

Resumo

Observa-se um aumento exponencial na manipulação de dados, e da conscientização sobre a privacidade de dados pessoais na sociedade ultimamente, o que culminou na elaboração da LGPD (Lei Geral de Proteção de Dados). Porém, pelo fato de a legislação não ter uma linguagem técnica, a identificação das implementações necessárias na segurança cibernética se torna mais difícil, além de exigir das empresas um maior controle tecnológico e jurídico. Logo, será feita uma revisão bibliográfica a fim de reconhecer e identificar técnicas e melhores práticas de cibersegurança organizacional para a conformidade à legislação.
Palavras-chave: Implementação LGPD, proteção de dados, cibersegurança.

Abstract

There has been an exponential increase in data manipulation, and awareness about the privacy of personal data in society lately, which resulted in the development of the LGPD (General Data Protection Law). However, because the legislation does not have technical language, identifying the necessary implementations in cybersecurity becomes more difficult; in addition, it requires greater technological and legal control from the companies. Therefore, a bibliographic review will be carried out in order to consider and identify cybersecurity business techniques and best practices for compliance with legislation.
Keywords: LGPD Implementation, data protection, cybersecurity.

1. Introdução

Considerando a evolução das Tecnologias de Informação e Comunicação (TIC's) presentes nos sistemas atuais, o processamento de dados pessoais já é uma rotina comum dentro das empresas. Contudo, agentes maliciosos têm ciência desse fato e evoluem suas técnicas. Como consequência, uma quantidade enorme de dados é violada ilegalmente todos os anos.

Nessa mesma lógica, segundo o relatório anual do custo de violação de dados de 2023, publicado pela *International Business Machines Corporation* - I.B.M. (2023), 82% dos alvos de ataques foram a dados armazenados. A pesquisa, conduzida de forma independente pelo Ponemon Institute e patrocinada, analisada e publicada pela IBM Security, analisou 553 empresas que sofreram violações de dados ocorridas entre março de 2022 e março de 2023.

Em resposta a esse cenário, a União Européia foi a pioneira a implementar uma legislação completa que defende a privacidade dos dados pessoais, GDPR - *General Data Protection Regulation*, de acordo com Zaeem e Barber (2020) é considerada como uma referência global. Nos últimos anos o Brasil tem acompanhado tais mudanças, promulgando e aperfeiçoando uma lei semelhante: a LGPD, lei de número 13.709 Brasil (2019), onde são previstos direitos, deveres, sanções e normas no que se refere aos dados pessoais.

Portanto, o presente artigo se justifica pelo fato de que essa legislação, ao fazer o uso de uma linguagem abrangente e não técnica em seus artigos, consequentemente, pode gerar dúvidas e dificultar a interpretação do escopo técnico de suas exigências, principalmente em empresas menor escala que não possuem o apoio jurídico e/ou tecnológico necessário.

Por isso, questiona-se quais são, de fato, as implementações que o setor de segurança cibernética necessita colocar em prática, a fim de acatar todas as especificações técnicas que a LGPD apresenta.

Logo, para responder esse questionamento, o objetivo geral deste estudo é ser um guia de referência para o reconhecimento dos principais processos técnicos na tecnologia corporativa que devem ser aplicados, visando a conformidade à LGPD. E como resultado dessa pesquisa, foi desenvolvido um *e-book* chamado: Guia Essencial de Cibersegurança para LGPD Augusto Finotti, Rodrigo Moura e Isaque (2024), onde foram documentadas

as implementações descobertas no presente estudo.

Sendo assim, os objetivos específicos consistem na identificação das exigências de teor técnico da LGPD, e explorar possíveis técnicas para a conformidade. Tendo como base a segurança da informação. Entretanto, observa-se que este estudo não tem por objetivo se detalhar nos meios de implementação, considerando que cada empresa tem suas peculiaridades.

Paralelamente, é notável a implantação de diversos *frameworks* de segurança da informação nas organizações, fato que segundo Baars et al. (2018) instaura um ponto de equilíbrio de interesses na empresa, por conta da padronização da qualidade e da garantia da continuidade do negócio. Portanto, coloca-se a suposta hipótese de que a adoção das principais práticas de frameworks de segurança da informação pode ser um meio para a adequação à LGPD.

2. Referencial Teórico

Com a finalidade de se obter uma sólida base referencial, estão descritos nesta seção os materiais que apresentam conceitos fundamentais para o entendimento do estudo.

2.1. Tecnologia da Informação

Lévy (2010) aponta que a evolução das técnicas é um dos grandes motores que movimenta a sociedade, fenômeno que também acaba por aprimorar a tecnologia. A evolução das tecnologias traz muito mais recursos e praticidade em todas as atividades, incluindo atividades que são exercidas no meio corporativo.

Segundo Rezende e Abreu (2000), a Tecnologia da Informação (TI) é primordial para a organização do fluxo de informações de uma empresa, se tornando parte essencial do fluxo de trabalho empresarial. De acordo com o mesmo autor em outro estudo: **??**), a engenharia de software e a tecnologia da informação são ferramentas que se complementam e moldam as técnicas utilizadas atualmente.

2.2. Segurança da Informação

De acordo com a literatura de **??**), existem três principais conceitos na segurança da informação: Confidencialidade, Integridade e Disponibilidade.

- **Confidencialidade:** diz respeito a práticas de prevenção contra acesso não autorizado e garantia do devido sigilo de uma informação.
- **Integridade:** referente ao estado de uma informação, ou seja, ao grau de confiabilidade que se tem de que uma informação não foi alterada indevidamente.
- **Disponibilidade:** esse princípio se refere à acessibilidade de uma informação, pois os dados precisam estar disponíveis para sua utilização.

Percebe-se que para o cumprimento dos princípios citados, se faz necessária uma adequação de todos os processos que envolvem a segurança da informação nas empresas, o que pode ser denominado como Gestão de Segurança da Informação.

2.2.1. Política de Segurança da Informação (PSI)

Segundo Kohls, Dutra e Welter (2022), a PSI é um conjunto de normas e práticas estabelecidas que têm a função de prezar pela proteção das informações, sendo aplicável

a diversas rotinas no ambiente físico e digital do trabalho, que possam criar brechas de segurança. Se exercitadas corretamente, a PSI pode mitigar várias vulnerabilidades.

Muitos se referem a PSI apenas como uma simples documentação, mas para ter um real efeito ela deve ser aplicada todos os dias, por esse motivo muitas empresas definem penalidades aos seus colaborados caso alguma política seja quebrada.

2.2.2. Gestão de Riscos e Vulnerabilidades

Lima et al. (2022) realiza uma síntese da área de gestão de vulnerabilidades, dizendo que as vulnerabilidades surgem em três principais perspectivas: pessoas, processos e tecnologias, abordagem que os principais frameworks de segurança da informação também sugerem.

Azmi, Tibben e Win (2018) apresentou um comparativo dos principais frameworks de segurança da informação, e afirma que a implementação desses modelos desempenha um papel determinante no sucesso da gestão de vulnerabilidades.

Nowak (2015) evidencia o acompanhamento de possíveis vulnerabilidades que possam surgir não só na estrutura interna da empresa, mas também em terceirizados e fornecedores, o que leva a uma gestão de vulnerabilidades integral, que considera inclusive os stakeholders.

2.2.3. Resposta a Incidentes e Continuidade de Negócios

Lima et al. (2022) realiza uma síntese da área de gestão de vulnerabilidades, dizendo que as vulnerabilidades surgem em três principais perspectivas: pessoas, processos e tecnologias, abordagem que os principais frameworks de segurança da informação também sugerem.

2.3. LGPD

LGPD é a sigla para Lei Geral de Proteção de Dados, lei número 13.709 que assegura a todos os brasileiros o direito à privacidade como um direito fundamental e irrevogável. É a principal lei brasileira em defesa da privacidade dos dados pessoais. Ela trouxe novas regulamentações para as organizações, com o intuito de aprimorar a privacidade e transparência durante todo o ciclo de vida de uma informação.

De acordo com Donda (2020), na eventualidade de sua correta implementação, a legislação em questão impulsionará o progresso no setor econômico e tecnológico brasileiro.

Segundo Peck (2020), as regulações de privacidade de dados surgiram por volta de 1990, e atualmente essas regulações são consequências diretas do modelo de negócios da economia atual, que acontece majoritariamente no meio digital.

Para Mulholland (2020), a LGPD é mecanismo no qual o cidadão pode se defender de possíveis abusos por parte dos agentes econômicos, que venham a fazer o uso indevido de seus dados, logo, pretende-se estabelecer uma confiança maior entre uma pessoa natural e as organizações por meio da legislação.

3. Metodologia

A metodologia escolhida para este estudo é a Revisão Sistemática da Literatura Bibliográfica, considerada como uma metodologia confiável para pesquisas acadêmicas, com sua confiabilidade conferida por Marconi e Lakatos (2012) e **??**) em seus estudos sobre tal método de pesquisa científica.

1. **Formulação das *Strings* de busca:** para a pesquisa ter a abrangência de diferentes tecnologias que a LGPD permeia, foram selecionadas as *Strings* (expressões): ”implementação + LGPD”, ”LGPD + cibersegurança”, ”LGPD + tecnologia”.
2. **Escolha das plataformas de pesquisa:** Serão feitas pesquisas de **artigos e livros** nas **plataformas**: **IEEE - Xplore:** banco de artigos internacional mantido pelo *Institute of Electrical and Electronic Engineers*, e **Google Acadêmico:** ferramenta de grande poder de busca de materiais de diferentes repositórios..
3. **Pesquisa Exploratória dos Materiais:** análise exploratória dos materiais encontrados por meio de uma leitura de forma breve e seletiva, visando a possível associação com o tema deste estudo.
4. **Organização dos Materiais por Relevância:** após o levantamento inicial, a relevância dos materiais foi conferida, materiais que apresentam maior especificidade técnica, e conformidade com a lei foram considerados mais relevantes.
5. **Seleção dos Materiais mais Relevantes:** Seleção dos materiais mais relevantes.
6. **Análise, Interpretação dos Materiais:** a leitura analítica foi feita utilizando a leitura aplicada, mencionada pelo autor COSTA (2007). Etapa onde foi empenhado

um esforço para se alcançar um entendimento mais profundo sobre os detalhes e especificidades técnicas demonstradas.

7. **Formulação das Conclusões:** Etapa onde foram identificadas e exploradas as principais implementações de cibersegurança para a LGPD. Etapa na qual ocorre o desenvolvimento do e-book, chamado: ”Guia Essencial de Cibersegurança para a LGPD”, conforme mencionado nos objetivos específicos (1)

4. Resultados e Discussões

Aplicando a metodologia descrita, chegou-se aos seguintes materiais:

Figura 1. Tabela dos materiais selecionados para a pesquisa. Fonte: Elaborado pelo Autor.

Materiais Selecionados				
Título	Plataforma	Formato	Ano	Autoria
LGPD – Uma visão de tecnologia e agnóstica	Google Academico	Artigo	2024	Luiz Fernando Pereira Nunes José Carlos Francisco dos Santos
Impactos da LGPD na Tecnologia da Informação: Desafios para os Profissionais da Área	Google Academico	Artigo	2022	Ana Rita Akayama Kanagusku Marcus Vinícius Lahr
LGPD – From Theory to Practice	IEEE Xplore	Artigo	2022	Francyelcyo Pussi Farias Rodolfo Barros
A cibersegurança no tratamento de dados pessoais: a chave de ouro para efetividade da lei geral de proteção de dados (lei nº 13.709/2018)	Google Academico	Artigo	2022	Mártin Marks Szinvelski Taynara Silva Arceno
Guia Prático de Implementação da LGPD	Google Academico	Livro	2020	Daniel Donda
Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem	Google Academico	Artigo	2020	Márcio Aurélio de Souza Fernandes et al.
Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)	Google Academico	Artigo	2019	Nairobi Spiecker de Oliveira et al.
Lgpd - lei geral de proteção de dados pessoais em tecnologia da informação: revisão sistemática	Google Academico	Artigo	2019	Cláudio Filipe Lima Rapôso et al.

Figura 2. Gráfico dos materiais encontrados e selecionados por plataforma.
Fonte: Elaborado pelo Autor.

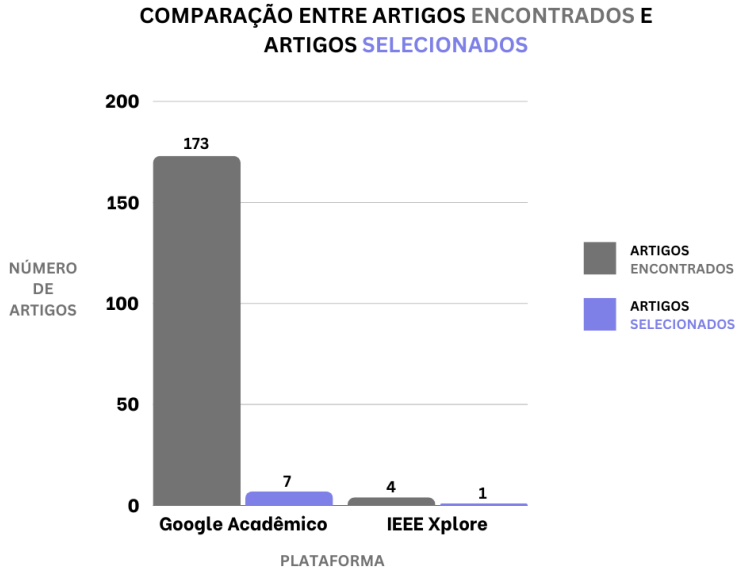
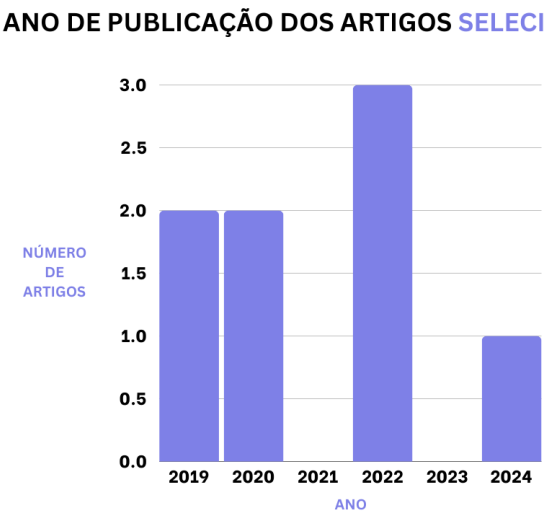


Figura 3. Gráfico dos materiais selecionados classificados por ano de publicação. Fonte: Elaborado pelo Autor.



Segue abaixo as questões levantadas pelo estudo.

Analisando os trabalhos consultados, considerando o grande número de artigos encontrados e o baixo número de artigos selecionados, observa-se que apesar do assunto LGPD estar em alta, essa área ainda se destina para a administração e governança. Logo, observa-se que a LGPD ainda é um campo pouco explorado por profissionais da tecnologia.

Tendo em vista o baixo número de artigos encontrados na plataforma IEEE - Xplore, pode-se inferir que existe pouquíssimo material científico sobre a LGPD no cenário internacional, muito menos sobre aspectos da tecnologia na LGPD.

Donda (2020) coloca uma série de implementações, dentre elas, destacam-se:

- ***Hardening* de Servidores:** consiste na otimização da segurança dos servidores da empresas. Como existem diversos tipos de servidores e serviços, a análise deve ser focada e personalizada. Pode-se ter como base medidas de segurança básicas como padrão como: proteção de rede com firewall, definição de usuários e suas permissões para o acesso ao servidor, aplicação correta das políticas de grupos para usuários do Active Directory.
- **Proteção das estações de trabalho:** faz-se necessária a utilização de antivírus

para maior segurança geral do computador, seja relacionado à sites suspeitos, e-mails infectados ou até *malwares* presentes na rede.

- **Proteção das Aplicações Web:** a adoção do framework OWASP *(Open Web Application Security Project)*, que é um projeto que se atualiza regularmente trazendo as principais correções de segurança. Dentre as principais vulnerabilidades que devem ser corrigidas estão: *SQL Injection*, Falha de Autenticação e Exposição de Dados Sensíveis.
- **Autenticação:** a possibilidade de autenticação com fator biométrico (digital ou reconhecimento facial com Windows Hello por exemplo) é muito bem vinda para maior segurança na autenticação do usuário da estação de trabalho.
- **Controle de Acesso e Auditoria:** o registro das operações realizadas no tratamento de dados é de suma importância para a devida legalidade do processo, visto que alterações nos dados pessoais são feitas.

Oliveira et al. (2019), ressalta o conflito entre economia de recursos computacionais em dispositivos IoT *(Internet of Things)*, considerando que métodos de criptografia e armazenamento seguro de arquivos demandam maiores recursos computacionais. Ele menciona ainda que métodos alternativos de criptografia e acesso à internet podem ser aplicados a depender da possibilidade de serem implementados no dispositivo em questão.

Fernandes et al. (2021) coloca que o cenário internacional se adequou antes aos padrões europeus de segurança, sendo assim, a maioria dos provedores de serviços de computação em nuvem já dispuseram de medidas de segurança condizentes com a legislação. Portanto não existem tantas adaptações para provedores de serviço em nuvem.

Rapôso et al. (2019) menciona que, em sua revisão bibliográfica, foi encontrada uma carência da aplicabilidade de mecanismos de proteção de dados em favor da lei.

Nunes e Santos (2023) levanta questões importantes como: técnicas de mascaramento e anonimização dos dados, monitoramento contínuo para detecção de anomalias e a realização da devida gestão de documentos para o gerenciamento correto do ambiente de tecnologia.

Kanagusku e Lahr (2022) menciona que a implementação de segurança nos *"endpoints"* (dispositivos informáticos), assim como a autentificação de múltiplos fatores e política de senhas, são medidas fundamentais para se proteger de ataques, principalmente dos ataques de força bruta, quando a senha é quebrada por tentativa e erro de forma mas-

siva e automática.

Farias e Barros (2022) e Szinvelski e Arceno (2022) exploraram aspectos voltados á gestão e governança. Também mencionam que as medidas de cibersegurança são relevantes para os negócios, porém não mencionaram especificamente as técnicas de segurança digital.

Apesar da notável falta de teor técnico nos materiais encontrados, em geral, verificou-se uma concordância geral entre os autores sobre a relevância jurídica da LGPD para o devido processo legal nacional e internacional, além de uma possível adesão maior á lei por parte das empresas no futuro.

Considerando o cumprimento dos requisitos de **segurança** e **prevenção**, mencionados no artigo 6º da lei Brasil (2019), foram identificadas algumas medidas citadas pelos autores:

- **Criptografia:** a aplicação de métodos de criptografia que inviabilizem a interpretação da mensagem, seja e trânsito ou em repouso, desde que sejam métodos eficazes e modernos, não sendo passíveis de reversão, preservando assim o princípio da confidencialidade.
- **Gestão de Riscos e Vulnerabilidades:** processo de gestão dos riscos e vulnerabilidades envolvidas no tratamento de dados. Isso inclui uma identificação inicial, um planejamento para a mitigação, um plano de ação para mitigação e uma reavaliação contínua do processo.
- **Backup:** consiste na cópia dos dados para a possibilidade de repor esses dados caso venham a ser corrompidos, alterados indevidamente ou mesmo excluídos. Cabe a empresa avaliar os dados que são críticos ao negócio, quais os meios possíveis para a realização do backup, além do planejamento e implementação de uma política de backup.
- **Autenticação de múltiplos fatores:** a autenticação apenas com login e senha tem sido cada vez mais fácil de ser quebrada, porém com dois ou mais fatores elementos para realizar a autenticação.

  Exemplo de fatores adicionais que podem ser utilizados para a autenticação: algo que você tem como um token ou certificado digital, algo que você sabe como endereços ou outros dados, e até algo que você é: reconhecimento facial ou biometria.

- **Política de Senha:** normas ao se utilizar senhas. Alguns aspectos enlglobados na política de senha podem ser: frequência na troca de senhas, exigência de símbolos especiais e números nas senhas, caracteres mínimos para criação de senhas e indicação de meios oficiais de recuperação de senhas.

Portanto, considerando a quantidade de artigos analisados, observa-se um enorme interesse da área de governança e gestão sobre a LGPD, entretanto a área de tecnologia e cibersegurança têm se aliado conjuntamente à LGPD, dispondo de ferramentas e recursos para o cumprimento da legislação.

Conclui-se que apesar das implementações de cibersegurança para a LGPD não terem sido exploradas amplamente pelo meio acadêmico, até o presente momento, os princípios de segurança da informação foram observados nas medidas básicas encontradas: criptografia e backup, por exemplo. Pela falta de material técnico, esse campo de estudo apresentou um alto potencial de crescimento.

Referências

AUGUSTO FINOTTI, O.; RODRIGO MOURA, A.; ISAQUE, K. ***Guia Essencial de Cibersegurança para LGPD***. 2024. Disponível em:. Disponível em: ⟨https://augustofinotti.com.br/e-book-lgpd⟩. 2

AZMI, R.; TIBBEN, W.; WIN, K. T. **Review of cybersecurity frameworks:** context and shared concepts. *Journal of Cyber Policy*, Routledge, v. 3, n. 2, p. 258–283, 2018. Disponível em: ⟨https://doi.org/10.1080/23738871.2018.1520271⟩. 5

BAARS, H. et al. ***Fundamentos de Segurança da Informação:*** *Com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018. 3

BRASIL. ***LGPD***. 2019. Disponível em: ⟨https://bit.ly/3AobOHE⟩ Acesso: 18 de Outubro de 2024. 2, 11

COSTA, R. e. a. **Metodologia científica**. *Faetec/IST. Paracambi*, v. 2, 2007. 6

DONDA, D. ***Guia prático de implementação da LGPD***. Editora Labrador, 2020. Acesso: 18 out. 2024. Disponível em: ⟨https://bit.ly/3C3cT8m⟩. 6, 9

FARIAS, F. P.; BARROS, R. **LGPD – From Theory to Practice**. In: *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2022. p. 1–6. 11

FERNANDES, M. A. de S. et al. **Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem**. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. E42, p. 374–385, 2021. 10

I.B.M. ***Relatório de Violação de Dados***. 2023. Disponível em: ⟨https://www.ibm.com/br-pt/reports/data-breach⟩ Acesso: 31 out. 2024. 2

KANAGUSKU, A. R. A.; LAHR, M. V. **Impactos da LGPD na Tecnologia da Informação:** desafios para os profissionais da área. In: *FatecSeg-Congresso de Segurança da Informação*. [S.l.: s.n.], 2022. 10

KOHLS, C.; DUTRA, L. H.; WELTER, S. ***LGPD da Teoria à implementação das empresas***. [S.l.]: Editora Rideel, 2022. ISBN 978655738745-0. 4

LÉVY, P. ***As tecnologias da inteligência:*** *O futuro do pensamento na era da informática*. [S.l.]: Editora 34, 2010. 4

LIMA, A. de et al. ***LGPD Manual de Implementação***. [S.l.]: Thomson Reuters, 2022. ISBN 978655991320-6. 5

MARCONI, M. d. A.; LAKATOS, E. M. **Técnicas de pesquisa: planejamento e execução de pesquisa; amostragens e técnicas de pesquisa;** elaboração, análise e interpretação de dados. In: *Técnicas de pesquisa: planejamento e execução de pesquisa; amostragens e técnicas de pesquisa; elaboração, análise e interpretação de dados*. [S.l.: s.n.], 2012. p. 277–277. 6

MULHOLLAND, C. ***A LGPD e o novo marco normativo no Brasil***. [S.l.]: Arquipélago Editorial, 2020. v. 6. 6

NOWAK, G. **Information Security Management with accordance to ISO27000 Standards:** characteristics, implementations, benefits in global supply chains. *Logistyka*, v. 2, p. 639–654, 2015. 5

NUNES, L. F. P.; SANTOS, J. C. F. dos. **LGPD–Uma visão de tecnologia e agnóstica**. *Revista Direito & Paz*, v. 2, n. 49, p. 218–237, 2023. 10

OLIVEIRA, N. S. de et al. **Segurança da informaçao para internet das coisas (iot):** uma abordagem sobre a lei geral de proteçao de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019. 10

PECK, P. P. ***Proteção de dados pessoais:*** *Comentários à lei n. 13.709/2018-lgpd*. [S.l.]: Saraiva Educação SA, 2020. 6

RAPÔSO, C. F. L. et al. **Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação:** revisão sistemática. *RACE-Revista de Administração do Cesmac*, v. 4, p. 58–67, 2019. 10

REZENDE, D. A.; ABREU, A. F. d. **Tecnologia da informação aplicada a sistemas de informação empresariais**. *São Paulo: Atlas*, v. 3, p. 30, 2000. 4

SZINVELSKI, M. M.; ARCENO, T. S. **A cibersegurança no tratamento de dados pessoais:** a chave de ouro para efetividade da lei geral de proteção de dados (lei nº 13.709/2018). *REVISTA DA AGU*, 2022. 11

ZAEEM, R. N.; BARBER, K. S. **The effect of the GDPR on privacy policies:** recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, ACM New York, NY, USA, v. 12, n. 1, p. 1–20, 2020. 2