# Confiança Digital e Resiliência Cibernética: Cibersegurança Na Perspectiva Da Proteção De Dados Pessoais

Digital trust and cyber resilience: Cybersecurity from the perspective of personal data protection

**Nathália Mylena**[1]
ORCID: https://orcid.org/0000-0001-6438-7695
*E-mail:* nathaliamylena1993@gmail.com

**Como citar este artigo:**
MYLENA, Nathália. Confiança Digital e Resiliência Cibernética: Cibersegurança na perspectiva da proteção de dados pessoais. **Revista de Egressos e Acadêmicos de Direito do CEUB**, Brasília, v. 1, nº 1, p. 367- 389, 2026. Disponível em: [...]. Acesso em: [...].

**RESUMO**

Com a promulgação da Lei nº 13.709/2018 e da EC nº 115/2022, tornou-se premente a busca por mecanismos que assegurem o direito fundamental à proteção de dados pessoais. Nesse viés, a cibersegurança se apresenta como uma alternativa à gestão de riscos para evitar incidentes de segurança, onde a confiança digital e a resiliência cibernética são fatores imprescindíveis na promoção da cultura organizacional. Ante o exposto, indaga-se: A cibersegurança é medida obrigatória para assegurar a proteção de dados pessoais, a confiança digital e a resiliência cibernética? Para tanto, objetiva-se averiguar se e como a cibersegurança é apta a assegurar a proteção de dados pessoais, a confiança digital e a resiliência cibernética. E de forma específica: tecer considerações sobre a cibersegurança; demonstrar como a confiança digital e a resiliência cibernética contribuem na cultura organizacional; discutir aspectos da LGPD; expor sobre a gestão de riscos da segurança da informação e, por fim, avaliar os pilares da cibersegurança na consecução da proteção de dados, da confiança digital e da resiliência cibernética. No que pertine à metodologia empregada no presente trabalho, utilizou-se o método de pesquisa qualitativo, tendo em vista a natureza não mensurável do presente estudo, no qual buscou-se, primordialmente, a compreensão do tema. Por sua vez, a técnica de pesquisa utilizada como instrumento para conduzir aos objetivos da pesquisa, destaca-se a pesquisa bibliográfica, em razão da utilização da legislação afeta ao tema, bem como a utilização de materiais já publicados como livros, artigos científicos e periódicos.

**Palavras-chaves**

[1] Mestra em Direito pela Universidade Federal de Sergipe. Especialista em Direito e Planejamento Tributário, em Direito e Planejamento Previdenciário e em LGPD. Possui MBA em Auditoria, Contabilidade e Gestão Tributária. É pesquisadora do Laboratório de Governo da Faculdade de Direito da USP (LabGov-FDUSP) e do Grupo de Pesquisa cadastrado no CNPD intitulado "O protagonismo humano". Integrou a 3ª edição do CEDIS IDP PRIVACY LAB. Certificada em Análise de Dados pela Google e ENAP. É advogada e coordenadora do setor judicial no escritório DRL Advocacia.

Confiança digital; resiliência cibernética; cibersegurança; proteção de dados pessoais.

**Sumário**



**ABSTRACT**

With the promulgation of Law nº 13.709/2018 and EC nº 115/2022, the search for mechanisms that ensure the fundamental right to the protection of personal data has become urgent. In this sense, cybersecurity presents itself as an alternative to risk management to avoid security incidents, where digital trust and cyber resilience are essential factors in promoting organizational culture. In light of the above, the question arises: Is cybersecurity a mandatory measure to ensure the protection of personal data, digital trust and cyber resilience? To this end, the objective is to find out whether and how cybersecurity is capable of ensuring the protection of personal data, digital trust and cyber resilience. And specifically: make considerations about cybersecurity; demonstrate how digital trust and cyber resilience contribute to organizational culture; discuss aspects of the LGPD; explain information security risk management and, finally, evaluate the pillars of cybersecurity in achieving data protection, digital trust and cyber resilience. Regarding the methodology used in this work, the qualitative research method was used, given the non-measurable nature of the present study, in which we primarily sought to understand the topic. In turn, the research technique used as an instrument to achieve the research objectives, bibliographical research stands out, due to the use of legislation affecting the topic, as well as the use of already published materials such as books, scientific articles and periodicals.

**Keywords**

Digital trust; cyber resilience; cybersecurity; protection of personal data.

**Contents**



## Introdução

Com a promulgação da LGPD, a Lei nº 13.709/2018 e da EC nº 115/2022, primeira norma específica versando sobre a proteção de dados pessoais e a sua consagração enquanto

direito fundamental, respectivamente, tornou-se premente a busca por mecanismos que assegurem o direito fundamental à proteção de dados pessoais.

Nesse viés, a cibersegurança, como o próprio nome sugere, busca garantir a segurança no ambiente digital a fim de se evitar incidentes de segurança, tais como vazamento de dados, cibercrimes e até mesmo o acesso não autorizado por terceiros a sistemas de segurança.

No mesmo sentido, a confiança digital pode ser assegurada mediante a adoção de práticas que reflitam o nível de confiança da Organização entre os *stakeholders*, sopesando-se risco e reputação, buscando, assim, a minimização desses riscos com foco na cibersegurança e no *compliance*, na ética e na responsabilidade social[2].

Por sua vez, a resiliência cibernética está relacionada à "capacidade de continuar a produzir os resultados pretendidos, apesar dos eventos e ataques cibernéticos, catástrofes naturais ou crises econômicas enfrentadas[3]".

Denota-se que essas três medidas: cibersegurança, confiança digital e resiliência cibernética, encontram-se atreladas de modo que a avaliação de riscos, a prevenção destes, o monitoramento de ações, bem como a correção de falhas, são pilares necessários ao bom e regular desenvolvimento das Organizações, sobretudo, para a realização do tratamento de dados pessoais.

Assim, a cibersegurança se apresenta como uma alternativa à gestão de riscos na perspectiva da proteção de dados pessoais, para evitar incidentes de segurança, onde a confiança digital e a resiliência cibernética são fatores imprescindíveis na promoção da cultura organizacional.

Ante o exposto, o presente trabalho visa responder ao seguinte questionamento: A cibersegurança é medida obrigatória para assegurar a proteção de dados pessoais, a confiança digital e a resiliência cibernética?

Para tanto, objetiva-se averiguar se e como, a cibersegurança é apta a assegurar a proteção de dados pessoais, a confiança digital e a resiliência cibernética. E de forma específica: tecer considerações sobre a cibersegurança; demonstrar como a confiança digital e a resiliência cibernética contribuem na cultura organizacional; discutir aspectos da LGPD; expor sobre a gestão de riscos da segurança da informação e, por fim, avaliar os pilares da cibersegurança na consecução da proteção de dados, da confiança digital e da resiliência cibernética.

Justifica-se a relevância do tema em razão da necessidade de adoção de medidas que assegurem o direito fundamental à proteção de dados pessoais contra possíveis incidentes de segurança, levando-se em consideração que os dados pessoais são identificados, hodiernamente, como um ativo intangível, na qual, as Organizações que realizam seu regular tratamento, se destacam com diferencial competitivo frente ao mercado cada vez mais, altamente concorrencial.

---

[2] CARNEIRO, André. Confiança digital: diferencial de negócios em um mundo digital. **Tecmundo**, 30 de junho de 2022. Disponível em: https://www.tecmundo.com.br/mercado/241123-confianca-digital-diferencial-negocios-mundo-digital.htm. Acesso em: 06 maio 2024.

[3] ***International Business Machines Corporation*** **- IBM**. O que é resiliência cibernética. Disponível em: https://www.ibm.com/br-pt/topics/cyber-resilience#:~:text=IBM-,O%20que%20%C3%A9%20resili%C3%AAncia%20cibern%C3%A9tica%3F,de%20incidentes%20de%20seguran%C3%A7a%20cibern%C3%A9tica. Acesso em: 06 maio 2024.

Metodologicamente, o presente trabalho trata-se de uma pesquisa normativa-jurídica, que busca além de analisar as normas, também a interpretação dos julgados sobre o tema, sendo necessário o entendimento da legislação para melhorar a sua aplicação[4]. Quanto ao tipo pesquisa realizou-se uma pesquisa exploratória, com abordagem qualitativa, tendo em vista que a pesquisa exploratória serve de base para fundamentos jurídicos para a construção de argumentos sólidos e convincentes[5]. Quanto às fontes, foram usadas as fontes primárias e secundárias. E por fim, foram utilizadas as técnicas documental e a jurisprudencial[6], pois analisa a norma ISO 27.001, a LGPD, o Manual de Referência do CNJ sobre prevenção e mitigação de ameaças cibernéticas e confiança digital, a Estratégia Nacional de Segurança Cibernética, a Política Nacional de Cibersegurança e a Ação Direta de Inconstitucionalidade nº 6390. Para os procedimentos de análise utilizou-se a Teoria de Análise de Conteúdo agrupa em categorias os resultados coletados, possibilitando a análise por meios jurídicos[7].

## 1. Considerações sobre cibersegurança

A Quarta Revolução Industrial, também conhecida como Revolução Digital ou, até mesmo, Indústria 4.0, trouxe avanços significativos para toda a sociedade, irradiando por todos os setores, a exemplo da educação (ensino *EAD*), da saúde (mapeamento genético para prevenção e tratamento de doenças), da segurança pública (sistemas de monitoramento e reconhecimento biométrico), administração pública (prestação digital de serviços públicos), setor empresarial (vendas *online*).

Nesse cenário, a Indústria 4.0 pode ser compreendida como a fusão entre tecnologias, com interação entre os domínios físicos, digitais e biológicos[8]. É dizer, essa Revolução não se resume à inserção e ao desenvolvimento de novas tecnologias, ora intituladas disruptivas, por ocasionaram uma quebra de paradigmas, rompendo uma ordem até então vigente. Isso porque, o que caracteriza a revolução digital é, justamente, essa interconexão entre domínios de modo que, não mais se discute a (im)possibilidade de uso de tecnologias seja a nível nacional ou internacional, mas sim, como essas tecnologias podem ser utilizadas para melhorar a qualidade de vida dos cidadãos e, sobretudo, assegurando os seus direitos fundamentais.

Desse modo,

> O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso[9].

[4] BITTAR, Eduardo Carlos Bianca. **Metodologia da pesquisa jurídica**: teoria e prática da monografia para os cursos de direito.17 ed. Saraiva, 2022. p 65.
[5] LAMY, Marcelo. **Metodologia da pesquisa jurídica**: Técnicas de investigação, argumentação e redação. 2011 Ed. Elsevier Editora Ltda, 2010. "n.p".
[6] KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro; SOUZA, Carlos Henrique Medeiros. **Metodologia da pesquisa**: um guia prático. Ed. Via Litterarum, 2010. p 28.
[7] BARDIN, Laurence. **Análise de Conteúdo**. 70. Ed. São Paulo: 2016. p. 229.
[8] SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.
[9] CASTELLS, Manuel. **A sociedade em rede (A era da informação, economia, sociedade e cultura)**. 6 ed. São Paulo: Paz e Terra, 1999, p. 69.

Ainda na perspectiva das transformações derivadas da revolução *ciber*, apresenta-se a cibercultura, a qual pode ser definida como:

> A expressão da aspiração de construção de um laço social, que não seria fundado nem sobre *links* territoriais, nem sobre relações institucionais, nem sobre as relações de poder, mas sobre a reunião em torno de centros de interesses comuns, sobre o jogo, sobre o compartilhamento do saber, sobre a aprendizagem cooperativa, sobre processos abertos de colaboração. O apetite para as comunidades virtuais encontra um ideal de relação humana desterritorializada, transversal, livre. As comunidades virtuais são os motores, os atores, a vida diversa e surpreendente do universal por contrato[10].

Desse modo, no ciberespaço onde ocorre a virtualização das relações sociais, o virtual se manifesta e se atualiza, apresentando-se como o domínio da potência, do sentido e da inteligência coletiva. É dizer, no virtual surge a potencialidade simbólica da ação humana.

E essa potencialidade simbólica da ação humana referente à expressão "virtual" é importante pois, na perspectiva da confiança digital e da resiliência cibernética, as comunidades virtuais compostas por sujeitos conectados colaboram, compartilham conhecimento e atualizam boas práticas para a promoção de uma cultura organizacional em proteção de dados pessoais. Do mesmo modo, o fenômeno cultural e social inserto nas comunidades virtuais têm o condão de viabilizar a proteção, a prevenção e a confiança no ecossistema digital.

Na perspectiva jurídica, a desterritorialização do ciberespaço ganha um novo relevo ao ampliar as discussões acerca da competência jurisdicional em âmbito transnacional, da eficácia das decisões judiciais transnacionais e da aplicação de normas locais adequadas a um padrão de Governança global com vistas a adoção de cooperação internacional e acordos multilaterais.

Assim, a expressão "virtual" proposta por Pierry Lévy em sua obra Cibercultura, deve ser compreendida como um meio para a promoção de uma cultura organizacional diante da emergência das comunidades virtuais no ciberespaço que representam a potência, ainda que não concretizada, porém, com possibilidade de atualização, oferecendo uma base sólida para repensar os desafios contemporâneos que permeiam a confiança digital e em resiliência cibernética, especialmente na perspectiva jurídica da promoção do letramento e da inclusão digitais.

Não à toa, o ciberespaço promoveu significativas mudanças nos costumes da sociedade hodierna repercutindo, inclusive, no reconhecimento de novos direitos e deveres bem como, na releitura dos outrora existentes. É o que acontece com a cibertransparência, o direito de acesso à internet, o direito à privacidade digital, a *accountability* digital e o novel direito fundamental à proteção de dados pessoais.

No Brasil, as repercussões na esfera jurídica do ciberespaço tiveram início com a CF de 1988 quando o STF, no julgamento do MS 21.729/DF, pontuou que o âmbito de proteção do inciso XII, do art. 5º da Carta Magna referia-se a comunicação de dados, e não dos dados

[10] LÉVY, Pierre. **Cibercultura**. Tradução por Carlos Irineu da Costa. São Paulo: Ed. 34, 1999, pg. 129-130.

em si[11] com adoção da tese de Tércio Sampaio Ferraz Júnior, dando início às discussões sobre a necessidade de reconhecimento de um direito à proteção de dados pessoais.

No mesmo sentido, o Código de Defesa do Consumidor dispôs sobre a proteção de dados, regulando o acesso às informações constantes em bancos de dados mantidos pelas Instituições de caráter público ou privado. O CDC previu a necessidade de observância ao dever constitucional de acesso à informação, bem como a necessidade de comunicação expressa ao consumidor quando da abertura de qualquer meio que armazene os dados pessoais.

Por seu turno, a Lei no 12.527 de 2011, Lei da Acesso à Informação (LAI) tem por objetivo regular o acesso à informação com vistas à efetivação dos princípios da publicidade e da transparência pela Administração Pública. A norma aduz que a divulgação ou o acesso às informações de caráter pessoal somente poderão ser divulgadas ou acessadas por terceiros mediante previsão legal ou consentimento expresso do titular. Sendo desnecessário o consentimento nas hipóteses expressamente previstas na lei, a exemplo do cumprimento de ordem judicial e as relativas à defesa de direitos humanos.

Em 2014 foi promulgada a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI) que trouxe em seu arcabouço a proteção de dados pessoais com enfoque anteriormente não visto no ordenamento jurídico brasileiro prevendo o desenvolvimento da personalidade como um de seus fundamentos e, dentre seus princípios, a proteção de dados pessoais. Assim, a norma legal, ao dispor expressamente sobre o tema, demonstrou necessária preocupação com os impactos dos dados pessoais na internet.

No que pertine à proteção de dados pessoais, em que pese a promulgação da Lei nº 13.709 em 2018 e da EC nº 115 em 2022, impende esclarecer que as discussões sobre a necessidade de regulamentação de uma norma que reconhecesse os dados pessoais enquanto um direito fundamental em decorrência da vulnerabilidade e da hipossuficiência dos cidadãos ante os incidentes de segurança, remontam desde os anos 80, especificamente em 15/12/1983, ocasião na qual o Tribunal Constitucional Federal alemão reconheceu o direito à autodeterminação informação sobre a Lei do Censo[12].

No Brasil, o direito à autodeterminação informativa e o direito fundamental à proteção de dados pessoais foram expressamente reconhecidos no ano de 2020, por meio da decisão em sede de Ação Direta de Inconstitucionalidade (ADI) julgada sob o nº 6.390 em face da Medida Provisória (MP) nº 954/2020, a qual previa a possibilidade de compartilhamento de dados dos usuários de telefonia fixa e móvel, pelas emprestadas prestadoras desse serviço com o Instituto Brasileiro de Geografia e Estatística (IBGE) para o Pesquisa Nacional por Amostra de Domicílios - PNAD Contínua[13].

---

[11] BRASIL. Supremo Tribunal Federal. **Mandado de Segurança no 21729-4-DF**, Relator: Min. MARCO AURÉLIO, Relator p/ Acórdão: Min. NÉRI DA SILVEIRA, Tribunal Pleno, julgado em 05/10/1995, DJ 19-10-2001 PP-00033 EMENT VOL-02048-01 PP-00067 RTJ VOL-00179-01 PP-00225. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599. Acesso em: 23 abr. 2025.

[12] FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais - LGPD**. Salvador: Editora JusPodivm, 2021, p. 27.

[13] BRASIL. SUPREMO TRIBUNAL FEDERAL (STF). **Ação Direta de Inconstitucionalidade nº 6390 MC-REF / DF**. Brasília: DF. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em 07 maio 2024.

Nessa senda, a autodeterminação informativa "certifica que o titular tenha domínio sobre os seus dados pessoais, ainda que o tratamento dessas informações seja legítimo[14]". Ademais, sua estreita relação com dados pessoais o alçou ao patamar de fundamento na LGPD, conforme dicção expressa do inciso II do art. 2º da supracitada lei.

Ocorre que, a promulgação de um instrumento normativo, por si só, não possui o condão de estimular medidas e coibir práticas pertinentes ao seu objeto de alcance, *in casu*, assegurar a proteção de dados pessoais. E é nesse contexto que se destaca a cibersegurança, a qual consiste em uma prática de usar tecnologia, controles e processos com o objetivo de proteger o ambiente digital, seja por meio de redes, dispositivos e dados armazenados contra os incidentes de segurança, estes, materializados no vazamento de dados, nos ciberataques e, até mesmo, no acesso não autorizado por terceiros. Tudo isso, com vistas a garantir a confidencialidade, a integridade e a disponibilidade das informações[15].

Para além disso, a autodeterminação informativa atua como um propulsor para coibir práticas discriminatórias no ciberespaço repercutindo na esfera ética e social da cibersegurança. Levando-se em consideração que a autodeterminação informativa garante que o titular assuma o controle de seus dados pessoais devendo ser cientificado sobre quaisquer ações que afetem seu direito, inclusive nos casos de alteração da finalidade na coleta dos referidos dados, decerto que a sociedade adota uma postura proativa e questionadora em relação a atuação dos controladores, operadores e encarregados de dados pessoais quanto ao seu regular tratamento.

No mais, não se pode perder de vista que a ausência de uma Política de Cibersegurança voltada à proteção dos sistemas digitais e das informações neles contidas gera implicações éticas e sociais, especialmente no que diz respeito ao risco de vigilância excessiva, além de impactos desproporcionais em grupos marginalizados. No que pertine ao risco de vigilância excessiva esta pode ocorrer por meio do monitoramento de tráfego, do reconhecimento facial, da exigência de biometria e do rastreamento de comportamento *online*, dentre outros, quando desvinculadas de políticas públicas específicas além da necessária regulamentação e da adesão à boas práticas, ao contrário disso, referidas práticas não se coadunam com o Estado democrático de Direito, cuja conduta enseja reparação civil por violação aos direitos fundamentais à intimidade, à vida privada, a honra e a imagem, nos termos do art. 5º, inciso X da CF de 1988.

Por seu turno, no que diz respeito aos impactos desproporcionais em grupos marginalizados destacam-se: (i) Reconhecimento facial e policiamento preditivo os quais tendem a apresentar maior taxa de erro com pessoas negras, indígenas, mulheres e pessoas trans, levando a abordagens injustas ou detenção indevida; (ii) Comunidades periféricas e minorias políticas podem se tornar alvo preferencial de vigilância estatal, especialmente em regimes autoritários ou contextos de criminalização da pobreza, (iii) A exclusão digital agrava a vulnerabilidade onde grupos sem acesso adequado a informação, letramento digital ou recursos de proteção tornam-se mais expostos a abusos, dentre outros.

---

[14] MARIA, Isabela; PICOLO, Cynthia. **Laboratório de Políticas Públicas e Internet (LAPIN),** 2021. Autodeterminação Informativa: Como esse direito surgiu e como ele me afeta? Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em: 07 maio 2024.

[15] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.

Dessa forma, a cibersegurança também se apresenta como um instrumento de justiça social pugnando pela adoção de padrões e princípios éticos baseando-se na proporcionalidade, no interesse legítimo, no livre consentimento informado, na transparência algorítmica e na responsabilização, no mesmo sentido do que dispõe a Lei Geral de Proteção de Dados Pessoais, a LGPD, em seu art. 6º.

Demais disso, a autodeterminação informativa e o controle sobre os dados pessoais constituem elementos essenciais da liberdade pessoal e da participação democrática. Nesse viés, o dever informacional, a transparência de ações e decisões e o letramento digital são instrumentos necessários para a consecução da autodeterminação informativa para que o titular de dados detenha, de fato, controle sobre seus dados pessoais.

Por outro lado, a ausência desses instrumentos propiciam um ambiente de decisões automatizadas com adoção de perfis preditivos como ocorre na discriminação algorítmica, além de corroborar com a desigualdade digital, com a vigilância excessiva. Situações que afetam ainda mais os grupos marginalizados.

Por oportuno, a postura proativa do titular de dados incentiva as organizações que realizam o tratamento de dados pessoais a adotar padrões de segurança mais rígidos e atualizados para prevenção e combate aos cibercrimes, a exemplo de fraudes. Não à toa, os Tribunais de Justiça pátrios, ao analisar demandas que versam sobre proteção de dados pessoais no âmbito da responsabilidade civil por incidentes de segurança, têm decidido pelo dano moral *in re ipsa*, isto é, presumido.

Foi o que restou decidido no processo nº 5000110-18.2020.8.13.0569 que tramitou no Tribunal de Justiça do estado de Minas Gerais (TJMG) cujo autor foi uma pessoa física e a parte requerida, uma pessoa jurídica, versando sobre inclusão de dados pessoais do demandante em cadastro de inadimplentes como devedor de parcelas de contrato de financiamento o qual, acreditava-se terem sido quitadas, prática popularmente conhecida como golpe do falso boleto. Na ocasião, o Juízo deu provimento aos pedidos da parte postulante condenando a parte requerida ao pagamento de indenização por danos morais decorrentes de vazamento de dados sigilosos no valor de R$10.000,00 (dez mil reais), sob o argumento de que o Banco requerido não comprovou excludente de responsabilidade diante do fato de que o autor renegociou uma dívida com terceiro acreditando ter renegociado com o próprio Banco em virtude de informações específicas e detalhadas informadas pelo criminoso[16].

Ademais, o Instituto Brasileiro de Cibersegurança (IBSEC) apresenta os dez principais tipos de segurança, sendo estes: (i) Segurança de aplicativos; (ii) Segurança da nuvem; (iii) Segurança de infraestrutura crítica; (iv) Segurança de dados; (v) Segurança de *endpoint*; (vi) Segurança de *IoT* - Internet das Coisas; (vii) Segurança móvel; (viii) Segurança de rede; (ix) Segurança operacional e a (x) Confiança zero[17].

Em relação à segurança dos aplicativos, esta medida tem o condão de evitar o acesso e o uso não autorizado de aplicativos e dados conectados. Por sua vez, a segurança da nuvem se

---

[16] MINAS GERAIS. Tribunal de Justiça de Minas Gerais -TJMG. **Procedimento Comum Cível 5000110-18.2020.8.13.0569**. Des(A). Octávio de Almeida Neves, 1ª Vara Cível, Criminal e da Infância e da Juventude, julgamento em 23/04/2024, publicação em 23/04/2024.

[17] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.

concentra na proteção de ativos e serviços baseados em nuvem, incluindo aplicativos, dados e infraestrutura; já a segurança de infraestrutura crítica é utilizada para proteger as redes, aplicações, sistemas e ativos digitais dos quais dependem organizações de infraestrutura crítica (por exemplo, comunicações, barragens, energia, setor público e transporte)[18].

Destarte, a segurança de dados integra a segurança da informação, cuja finalidade é proteger a confidencialidade, a integridade e a disponibilidade das informações. A segurança de *endpoint* visa proteger os dispositivos bem como os dados armazenados nestes. Por seu turno, a segurança *IoT* "busca minimizar as vulnerabilidades que esses dispositivos em proliferação trazem para as organizações"[19].

De outra banda, a segurança móvel, de rede e operacional, protege os dispositivos móveis em face do acesso não autorizado; inclui monitorar, detectar e responder a ameaças focadas na rede e estabelece protocolos de acesso e monitoramento para detectar comportamentos incomuns, respectivamente[20].

Por fim, o modelo de confiança zero consiste na adoção de determinadas práticas partindo-se da premissa de que nenhum usuário, tampouco sistema, merece confiança integral. É dizer, a identidade do usuário passa por um processo de verificação contínua[21].

Resta claro que a cibersegurança consiste em um conglomerado de medidas dotadas de certa complexidade e, cujas técnicas exigem habilidades específicas de profissionais para sua implementação nos sistemas dentro das Organizações.

Isso posto, a atuação *multistakeholder* com uma rede de colaboração composta por profissionais das mais diversas áreas, incluindo tecnologia da informação, *marketing*, jurídico, administração, economia, estatística, bem como profissionais designados para atuar como controlador, operador e encarregado de dados, são imprescindíveis para certificar a mudança na cultura organizacional com a implementação da cibersegurança.

## 2. Confiança digital e resiliência cibernética na promoção de uma cultura organizacional

Muito se discute acerca da necessidade de se estimular hábitos nas Organizações que conduzam às boas práticas. Pode-se dizer que, a governança e o *compliance* são, hoje, importantes instrumentos na consecução de uma mudança na cultura organizacional.

A governança, requer transparência nos processos e nos procedimentos adotados por cada Organização[22]. Essa transparência nas ações organizacionais tem o propósito de promover a ética, a responsabilidade e a responsabilização dos agentes envolvidos, repercutindo na imagem da Organização perante toda a sociedade, é dizer, a governança é o meio pelo qual evitam-se crises reputacionais ao tempo em que promovem o diferencial de mercado.

---

[18] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.
[19] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.
[20] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.
[21] QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio 2024.
[22] KASEMIRSKI, André Pedroso. Reflexões sobre segurança, boas práticas, governança e *compliance* na proteção de dados pessoais. In: **Proteção de dados**: fundamentos jurídicos. Coordenadores Tarcísio Teixeira, Américo Ribeiro Magro - Salvador: Editora JusPodivm, 2021, p. 193.

O *compliance* pugna pelo conhecimento das normas pertinentes à Organização bem como, "seguir os procedimentos recomendados, agindo em conformidade e sentir quanto é fundamental à ética e a idoneidade em todas as nossas atitudes[23]".

Com o desenvolvimento do ciberespaço não seria diferente. As relações socioculturais e econômicas ganharam significativo relevo diante da Revolução 4.0. No setor privado e no setor público, dentre os principais impactos das tecnologias, destacam-se o incentivo à inovação e a melhoria na qualidade em produtos e serviços. No que diz respeito ao setor privado, individualmente, destaca-se a redução do preço final dos produtos e serviços. Quanto ao setor público, nota-se a ampliação dos serviços e informações pela internet[24], sobretudo com a emergência da prestação digital de serviços públicos e da cibertransparência.

Ainda no cenário 4.0, é perceptível, os seguintes impactos referentes à estrutura organizacional: (i) sistemas abertos com modelos mais flexíveis de gestão; (ii) adoção da estrutura em rede ou mistas; (iii) redução de níveis hierárquicos; (iv) conhecimento e pessoas como principais recursos; (v) busca pela melhoria contínua; e (vi) cultura do aprendizado e da inovação[25].

Quanto aos impactos referentes às pessoas, destacam-se: (i) substituição de chefias por lideranças; (ii) empregos transitórios; (iii) ampliação de competências; (iv) profissionalização do relacionamento interpessoal; (v) capacitação contínua; (vi) trabalho eletrônico; (vii) trabalho em grupo[26], dentre outros.

Diante das diversas habilidades exigidas, decorrentes da inserção de novas tecnologias disruptivas na sociedade hodierna, impende ressaltar a necessidade de construção de "um novo ecossistema de proteção de dados, pautado na boa-fé, na transparência, na segurança, em boas práticas corporativas e na governança[27]".

Para além disso, assegurar a confidencialidade, a disponibilidade e a integridade das informações é medida que se impõe, para evitar crises reputacionais, sanções previstas na LGPD bem como, para promover excelentes oportunidades de negócios e um diferencial de mercado[28] e, sobretudo, assegurar os direitos fundamentais dos cidadãos.

Para tanto, a confiança digital pode ser assegurada mediante a adoção de práticas que reflitam o nível de confiança da Organização entre os *stakeholders*, sopesando-se risco e reputação, buscando, assim, a minimização desses riscos com foco na cibersegurança e no *compliance*, na ética e na responsabilidade social[29].

---

[23] KASEMIRSKI, André Pedroso. Reflexões sobre segurança, boas práticas, governança e *compliance* na proteção de dados pessoais. In: **Proteção de dados**: fundamentos jurídicos. Coordenadores Tarcísio Teixeira, Américo Ribeiro Magro - Salvador: Editora JusPodivm, 2021, p. 192.

[24] PALUDO, Augustinho. **Administração Pública**. 10. ed. rev. ampl. e atual. - São Paulo: Editora JusPodivm, 2022, p. 330.

[25] PALUDO, Augustinho. **Administração Pública**. 10. ed. rev. ampl. e atual. - São Paulo: Editora JusPodivm, 2022, p. 332.

[26] PALUDO, Augustinho. **Administração Pública**. 10. ed. rev. ampl. e atual. - São Paulo: Editora JusPodivm, 2022, p. 333-334.

[27] FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais - LGPD**. Salvador: Editora JusPodivm, 2021, p. 173.

[28] FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais - LGPD**. Salvador: Editora JusPodivm, 2021, p. 173.

[29] CARNEIRO, André. Confiança digital: diferencial de negócios em um mundo digital. **Tecmundo**, 30 de junho de 2022. Disponível em: https://www.tecmundo.com.br/mercado/241123-confianca-digital-diferencial-negocios-mundo-digital.htm. Acesso em: 06 maio 2024.

Por conseguinte, a resiliência cibernética está relacionada à "capacidade de continuar a produzir os resultados pretendidos, apesar dos eventos e ataques cibernéticos, catástrofes naturais ou crises econômicas enfrentados[30]".

Assim, o que determina a efetividade desse novo ecossistema de proteção de dados pessoais é o nível de confiança que os *stakeholders* possuem em relação ao tratamento de dados pessoais realizado pelas Organizações assim como, a capacidade que cada Organização detém, para lidar, superar e, se reinventar diante das demandas relacionadas à gestão de riscos digitais.

Portanto, a confiança digital e a resiliência cibernética apresentam-se como premissas necessárias para o fortalecimento e o respeito aos direitos fundamentais da sociedade no ambiente digital.

## 3. Lei geral de proteção de dados pessoais

A Lei nº 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais, ou simplesmente, LGPD, trouxe avanços significativos em relação ao necessário tratamento de dados pessoais. Isso é dito, pois, esse importante instrumento normativo, o primeiro a dispor sobre o tema de forma específica, propõe uma mudança na cultura da proteção de dados pessoais por meio de uma abordagem responsiva, da governança nodal e da autorregulação regulada.

A abordagem responsiva, também denominada, autorresponsabilidade, pugna pela consciência de que, cada agente integrante da Organização, é responsável pela implementação da cultura na proteção de dados pessoais. Não à toa, o acesso não autorizado por terceiros e as situações acidentais são tratados como incidentes de segurança, os quais devem ser evitados, tal qual prevê a LGPD no *caput* do art. 46, disposto no capítulo VII sobre segurança e boas práticas, mais adiante analisado.

Assim, a mudança na cultura da proteção de dados pessoais deve ter como ponto de partida, a estrutura interna organizacional, com foco na gestão de pessoas, onde o treinamento e o aperfeiçoamento contínuos são primordiais para se estabelecer condutas positivas e negativas com aplicação de sanções em virtude de descumprimento.

Por sua vez, no que pertine às estratégias de governança nodal:

> Incentivam a participação efetiva de indivíduos e instituições variadas, principalmente do setor privado, que possuem um conjunto de tecnologias, conhecimentos e modos de pensar variados, para buscar contornar o déficit de capacidade regulatória de alguns dos países, desonerando a estrutura estatal do ônus de implementar todas as medidas de incentivo à conformidade normativa do regulado[31].

A autorregulação regulada ou corregulação parte da premissa de que as próprias Organizações dispõem de maior capacidade para regular suas atividades em detrimento do

---

[30] ***International Business Machines Corporation*** **- IBM**. O que é resiliência cibernética. Disponível em: https://www.ibm.com/br-pt/topics/cyber-resilience#:~:text=IBM-,O%20que%20%C3%A9%20resili%C3%AAncia%20cibern%C3%A9tica%3F,de%20incidentes%20de%20seguran%C3%A7a%20cibern%C3%A9tica. Acesso em: 06 maio 2024.

[31] IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020, p. 108.

governo[32]. Assim, as Organizações regulam suas atividades de acordo com seu porte e suas condições financeiras criando normas internas que assegurem o seu bom e regular funcionamento. Todavia, na autorregulação regulada, como o próprio nome sugere, em que pese a adoção de normas internas, estas não excluem a atuação estatal, apenas desonera em parte a regulação governamental.

Desse modo, a LGPD se mostra como uma legislação inovadora e incentivadora de uma mudança na cultura organizacional em relação ao tratamento de dados pessoais, cuja violação expõe seus titulares a diversas vulnerabilidades, como os ciberataques.

### *3.1 O direito fundamental à proteção de dados pessoais*

A EC nº 115 de 2022 firmou expressamente o entendimento de que a proteção de dados pessoais constitui um direito fundamental, bem como fixou a competência privativa da União para legislar sobre o tema. Contudo, antes mesmo da promulgação da referida emenda, autores já defendiam esse posicionamento.

Isso pois, "os dados pessoais, assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização[33]".

Não obstante, os dados pessoais passam por uma etapa de processamento durante seu tratamento, o que pode ser feito com o auxílio de algoritmos, os quais, por sua vez, são determinantes para a tomada de decisão.

Nessa senda, o uso de algoritmos pode otimizar o tempo de processamento de dados e apresentar projeções para subsidiar a tomada de decisão estratégica em tempo célere. Porém, é necessário que os algoritmos sejam "alimentados" com instruções sem vieses, sob pena de incorrer em discriminação algorítmica.

Até porque:

> Quanto maiores os incentivos para o uso de processamento de dados por meio de algoritmos como base para tomadas de decisão e quanto mais prontamente disponíveis e baratas as tecnologias para tornar isso possível, mais urgente se torna a discussão acerca das consequências de tais procedimentos para os indivíduos e os riscos a eles associados[34].

Ademais, sobre o direito fundamental à proteção de dados pessoais, assevera Ingo Sarlet:

---

[32] IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020, p. 106.

[33]BASTOS, Caroline Ayala de Carvalho; SPOSATO, Karyna Batista. Direito fundamental à proteção de dados pessoais: o reconhecimento constitucional da vulnerabilidade do titular no contexto da sociedade informacional. In: **Temas de Direito Constitucional**: estudos em homenagem ao Professor José Lima Santana. Aracaju: Editor Ubirajara Coelho Neto, 2022, p. 120.

[34] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: **Tratado de Proteção de Dados Pessoais**. Coordenadores Bruno Bioni, Danilo Doneda, Ingo Wolfgang Sarlet, Laura Schertel Mendes, Otavio Luiz Rodrigues Junior. Rio de Janeiro: Forense, 2021.

> A condição de direito fundamental vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional.
> Nesse contexto, nunca é demais lembrar que levar à sério a proteção de dados pessoais é sempre também render homenagem à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à liberdade pessoal como autodeterminação[35].

Assim, a positivação da proteção de dados pessoais enquanto direito fundamental não se esvazia ante a sua inserção expressa no ordenamento jurídico pátrio. Muito pelo contrário, a positivação é a lembrança de que os dados pessoais são partes integrantes de cada indivíduo, repercutindo na forma como os titulares se identificam perante a si mesmos e perante a sociedade, razão pela qual, no tratamento de dados pessoais deve-se primar sempre, pela melhoria contínua, identificando vulnerabilidades, corrigindo falhas, monitorando todas as etapas do tratamento de dados e implementando as melhorias necessárias.

### *3.2 Da segurança e das boas práticas*

A LGPD, no seu capítulo VII, aduz pela segurança e boas práticas. Logo no art. 46, *caput*, o legislador previu que: "Os agentes de tratamento devem adotar 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".

Em relação às medidas de segurança e técnicas previstas na norma, destaca-se a cibersegurança, a qual, reveste-se de uma importante ferramenta, haja vista que um dos seus tipos é a segurança de dados, cujo objetivo é assegurar a confidencialidade, a integridade e a disponibilidade das informações, conforme anteriormente mencionado.

Por conseguinte, dentre as medidas administrativas, as boas práticas e a governança destacam-se, com amparo legal no art. 50 da LGPD, assim dispondo:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.[36]

---

[35] SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista de Direitos Fundamentais & Justiça** | Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875/985. Acesso em: 03 maio 2024, p. 214.

[36] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

O dispositivo supra é claro quanto à necessidade de implementação de regras que estimulem a mudança na cultura organizacional da proteção de dados pessoais através da abordagem responsiva, da governança nodal e da autorregulação regulada, conceitos anteriormente elucidados.

Nesse mesmo sentido, o art. 46 da LGPD, outrora mencionado, aborda os incidentes de segurança na medida em que os discrimina da seguinte maneira: (i) acessos não autorizados; (ii) situações acidentais; (iii) situações ilícitas; e (iv) qualquer forma de tratamento inadequado ou ilícito.

Em suma, incidente de segurança trata-se de "qualquer fato que possa comprometer a integridade dos dados pessoais, inclusive os provenientes de falhas nos sistemas ou erros humanos[37]".

Não se pode perder de vista a importância da Autoridade Nacional de Proteção de Dados, a ANPD, a qual dispõe de poderes regulatórios, fiscalizatórios e sancionatórios, conforme se depreende do art. 55-J da LGPD. Um exemplo dos poderes fiscalizatórios e sancionatórios da referida autoridade administrativa encontra-se previsto no inciso IV do dispositivo ora discutido, nestes termos: "fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso[38]". No que pertine ao poder regulatório, cita-se o inciso III, assim disposto: "elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade[39]".

Todavia, em relação a sua competência regulamentar é imprescindível que a edição de normas e de regulamentos seja precedida de consultas e audiências públicas, além da análise do impacto regulatório[40], demonstrando-se a importância de uma ação articulada, integrada e multissetorial no que diz respeito à proteção de dados pessoais.

Dessa forma, nota-se que a competência da ANPD deve estar alinhada com os *multistakeholders*, isto é, com as múltiplas partes interessadas na promoção de uma cultura organizacional da proteção de dados pessoais, aqui abrangidos, a sociedade civil, governos, poderes, empresas, e, em especial, cada cidadão individualmente, ora titular de dados pessoais.

## 4. Gestão de riscos da segurança da informação

Quando se fala em proteção de dados pessoais, a LGPD é um dos diversos instrumentos que devem ser observados para assegurar esse direito fundamental. Nessa

---

[37] KASEMIRSKI, André Pedroso. Reflexões sobre segurança, boas práticas, governança e *compliance* na proteção de dados pessoais. In: **Proteção de dados**: fundamentos jurídicos. Coordenadores Tarcísio Teixeira, Américo Ribeiro Magro - Salvador: Editora JusPodivm, 2021, p. 185.

[38] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

[39] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

[40] FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais** - LGPD. Salvador: Editora JusPodivm, 2021, p. 205.

conjuntura, a segurança da informação, a qual incorpora a segurança de dados, é medida que se impõe nas Organizações, onde a gestão de riscos deve ser pormenorizadamente avaliada. Para tanto, vejamos o que dispõem alguns instrumentos sobre o tema.

Inicialmente, destaca-se a própria LGPD que, no inciso I do §2º do seu art. 50, recomenda a implementação de um Programa de Governança em Privacidade, com os seguintes requisitos mínimos:

> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas[41].

Em que pese a norma fazer alusão à possibilidade de implementação de tal Programa, ao utilizar o verbo "poderá", nos termos do parágrafo 2º do art. 50, defende-se a necessidade da adoção de um Programa de Governança em Privacidade nas Organizações. Isso porque, esse instituto prevê um conjunto de medidas aptas a assegurar o adequado tratamento de dados pessoais alinhado à governança organizacional. É dizer, o PGP é parte integrante do Programa de Governança nas Organizações, o qual, conforme já elucidado, evita crises reputacionais, apresenta-se como diferencial de mercado, evita sanções pela ANPD, assegura as boas práticas e, ainda, garante o respeito aos direitos fundamentais dos cidadãos.

De outra banda, a ISO 27.001 com foco na *Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação*, defende o modelo de melhoria contínua, também conhecido como ciclo PDCA, por meio do Sistema de Gestão em Segurança da Informação - SGSI, nos seguintes moldes:

**Figura 1 — Modelo PDCA aplicado aos processos do SGSI**

| | |
|---|---|
| ***Plan* (planejar) (estabelecer o SGSI)** | Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização. |

[41] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

| | |
|---|---|
| ***Do* (fazer) (implementar e operar o SGSI)** | Implementar e operar a política, controles, processos e procedimentos do SGSI. |
| ***Check* (checar) (monitorar e analisar criticamente o SGSI)** | Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção. |
| ***Act* (agir) (manter e melhorar o SGSI)** | Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. |

**Fonte: ABNT NBR ISO/IEC 27001:2006**

Essas etapas do ciclo de melhoria contínua são de extrema importância para toda e qualquer Organização que busca manter o alto padrão de qualidade em seus processos e procedimentos, sem que isso implique, necessariamente, em altos custos para sua implementação. Até porque, "O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas[42]".

A gestão de riscos da segurança da informação também alcançou o Poder Judiciário nacional. O Conselho Nacional de Justiça - CNJ, editou, em março de 2021, o Manual de Referência para prevenção e mitigação de ameaças cibernéticas e confiança digital. Referido documento inova ao abordar a confiança digital e a resiliência cibernética como mecanismos necessários para assegurar o melhor desempenho organizacional no que concerne à segurança da informação.

De acordo com o Manual, os requisitos para um ambiente de segurança cibernética resiliente incluem as seguintes etapas:

[42] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006. Disponível em: https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf. Acesso em: 03 maio 2024.

> a) Identificar: ativo crítico e comuns, mapeamento de processo, avaliação de risco e prontidão para resposta; b) Proteger: mecanismos de segurança de primeira linha de defesa; c)Detectar: análise de segurança; verificação de integridade de dados de configuração/reconfiguração de ativos em tempo real; d) Responder: resposta a violações ou falhas de segurança; e, e) Recuperar: mecanismos coordenados de recuperação[43].

Nota-se que as etapas descritas, em muito se assemelham ao ciclo de melhoria contínua, também conhecido como ciclo PDCA, com as fases de planejamento, execução, verificação e ação, anteriormente discutidos, ratificando-se a necessidade de que as Organizações mantenham esses cuidados correspondentes às etapas, de forma contínua, sempre com a finalidade de verificar as suas vulnerabilidades, corrigi-las, aprimorar seus procedimentos, bem como evitar que os erros se repitam.

Por fim, a Autoridade Nacional de Proteção de Dados (ANPD), em outubro de 2021, publicou o *Guia Orientativo sobre segurança da informação para agentes de pequeno porte* sob o argumento de que esse nicho "em razão de seu tamanho e eventuais limitações, muitas vezes não possuem dentre o seu corpo de funcionários, pessoas especializadas em segurança da informação e necessitam aprimorá-la em relação ao tratamento de dados pessoais[44]".

Nessa senda, a ANPD define a Política de Segurança da Informação (PNI) como "um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização[45]".

Para além disso, a autoridade administrativa exemplifica determinadas medidas que devem ser tomadas nas Organizações para evitar incidentes de segurança, tais como: cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de softwares; uso de correio eletrônico; uso de antivírus, entre outros[46].

Portanto, resta claro que a gestão dos riscos de segurança da informação, muito embora exija uma mudança na cultura organizacional com aperfeiçoamento e conscientização dos colaboradores, investimentos financeiros e recursos humanos, não se caracteriza como uma tarefa complexa, na medida em que os direitos e deveres de cada colaborador na execução de suas tarefas estejam bem alinhadas ao objetivo da Organização, bem como, haja o necessário investimento para a consecução dessas tarefas, sobretudo, quando a alta administração for o primeiro setor alinhado à responder suas demandas.

---

[43] BRASIL. Conselho Nacional de Justiça (CNJ). **Manual de Referência**: Prevenção e mitigação de ameaças cibernéticas e confiança digital. Brasília, DF: CNJ, março de 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVManualReferenciaPrevencaoMitigacaoDeAmeacasCiberneticasConfiancaDigitalRevisadoREV.docx.pdf. Acesso em 03 maio 2024, p. 18.

[44] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Segurança da Informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, versão 1.0, outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 03 maio 2024, p. 04.

[45] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Segurança da Informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, versão 1.0, outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 03 maio 2024, p.08.

[46] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Segurança da Informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, versão 1.0, outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 03 maio 2024, p.08.

## 5. Cibersegurança para assegurar o direito fundamental à proteção de dados pessoais, a confiança digital e a resiliência cibernética

Para além da promulgação da LGPD, a cibersegurança também já foi disciplinada no Brasil. À nível governamental, o Decreto nº 10.222, de 05 de fevereiro de 2020, aprovou a Estratégia Nacional de Segurança Cibernética (*E-Ciber*) com o objetivo de "melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais[47]". O Decreto supra constatou que o:

> E-Ciber, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Em terceiro, vê-se a existência de diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema.

Em contrapartida, apresentou as seguintes ações estratégicas: (i) Fortalecer as ações de governança cibernética; (ii) Estabelecer um modelo centralizado de governança no âmbito nacional; (iii) Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; (iv) Elevar o nível de proteção do Governo; (v) Elevar o nível de proteção das Infraestruturas Críticas Nacionais; (vi) Aprimorar o arcabouço legal sobre segurança cibernética; (vii) Incentivar a concepção de soluções inovadoras em segurança cibernética; (viii) Ampliar a cooperação internacional do Brasil em Segurança cibernética; (ix) Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade e (x) Elevar o nível de maturidade da sociedade em segurança cibernética[48].

Depreende-se a necessidade de ações articuladas, integradas e alinhadas não só no âmbito interestatal, mas também, por todos os *multistakeholders* no tocante à segurança cibernética, sob pena de ineficácia das ações que combatam os incidentes de segurança.

Por sua vez, o Decreto nº 11.856, de 26 de dezembro de 2023, instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança (PNCiber) "com a finalidade de orientar a atividade de segurança cibernética no País[49]".

---

[47] BRASIL. **Decreto nº 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 04 maio 2024.

[48] BRASIL. **Decreto nº 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 04 maio 2024.

[49] BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,que%20lhe%20confere%20o%20art. Acesso em: 04 maio 2024.

Dentre os objetivos do PNCiber ilustram-se: garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações (inciso II) e estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos (inciso V)[50], entre outros.

Destarte, dos objetivos acima destacados, é perceptível que a proteção de dados pessoais e a cibersegurança convergem para um mesmo objetivo: proteger direitos fundamentais e evitar incidentes de segurança.

Não se pode perder de vista que a Política Nacional de Cibersegurança precisa estar alinhada ao ordenamento jurídico, especialmente no que toca ao combate e a prevenção de cibercrimes, preenchendo as lacunas existentes e consolidando os avanços até então alcançados. Tal constatação deve-se ao avanço exponencial do uso de tecnologias, o qual nem sempre acompanha o progresso na perspectiva ética e social, conforme se depreende dos incidentes de segurança aqui incluídos: vazamento de dados pessoais, fraudes e acesso não autorizado por terceiros.

Do mesmo modo, a Política Nacional de Cibersegurança com as legislações vigentes como a LGPD e o Marco Civil da Internet e, sobretudo, alinhada à LGPD penal ainda não promulgada, a qual deverá contar com a integração entre o Poder Público, as forças policiais, o Ministério Público, as organizações promotoras dos direitos humanos e da própria sociedade civil organizada.

No que diz respeito à ampliação da cooperação internacional do Brasil em segurança cibernética, defendida pelo *E-Ciber*, Jussara Polesel afirma que esse tipo de cooperação, "em torno da cibersegurança, privacidade e proteção de dados pessoais é crucial, seja nas esferas política, econômica ou jurídica, seja no compartilhamento de dados, ou na implementação de políticas públicas, bem como no aperfeiçoamento do cumprimento da legislação pelos países[51]".

Outrossim, será necessário equilibrar a necessidade de segurança cibernética com a proteção de direitos individuais. Para tanto, a autodeterminação informativa é primordial na medida em que assegura o controle dos dados pessoais pelo titular, estimulando a adoção de boas práticas de segurança pelas Organizações que realizam o tratamento de dados pessoais, incluindo em seus procedimentos rotineiros, avaliação de impacto de riscos, procedimentos de segurança com mecanismos de prevenção e repressão aos incidentes de segurança , além de estimular a adoção de uma Política de Governança eficaz.

Isso porque, o ciberespaço não é dotado de limites territoriais e, sequer, físicos. As relações virtuais ultrapassaram fronteiras onde não é possível precisar o local exato onde essas relações se firmaram, tal qual ocorre com os ciberataques. Desse modo, o estabelecimento de

---

[50] BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,que%20lhe%20confere%20o%20art. Acesso em: 04 maio 2024.

[51] POLESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no Brasil, à luz do direito comparado e dos standards internacionais de regulamentação** [recurso eletrônico]. – Caxias do Sul, RS: Educs, 2021. Disponível em: https://www.ucs.br/educs/arquivo/ebook/ciberseguranca privacidade-e-protecao-de-dados-pessoais/. Acesso em: 04 maio 2024.

cooperação a nível internacional, com a fixação de direitos e deveres entre as partes interessadas, colabora não só, com a possibilidade de compartilhamento de técnicas avançadas de cibersegurança, como também na promoção de um ciberespaço cada vez mais confiante e resiliente frente aos incidentes de segurança e, com vistas ao respeito ao direito fundamental à proteção de dados pessoais.

## Conclusão

Ante o exposto, resta claro que a cibersegurança é medida obrigatória para assegurar a proteção de dados pessoais, a confiança digital e a resiliência cibernética. Isso é dito pois, assegurar o direito fundamental à proteção de dados pessoais, seja no cenário nacional, seja a nível internacional, é tarefa complexa no sentido de que é necessário uma mudança na cultura organizacional onde a abordagem responsiva, a governança nodal e a autorregulação regulada sejam partes integrantes e indispensáveis.

Para além disso, a cibersegurança, pugna pela adoção de uma série de medidas dentre as quais, a segurança de dados engloba a segurança da informação, sendo necessário o alinhamento de todos esses segmentos a fim de evitar incidentes de segurança e, sobretudo, o respeito ao direito fundamental à proteção de dados pessoais.

Ademais, é imprescindível que haja articulação multissetorial, integrada e alinhada entre todos os setores, inclusive pela sociedade. Não obstante a promulgação da LGPD, houve a edição de Decretos pelo governo federal com o intuito de identificar as vulnerabilidades para implementação da cibersegurança, bem como identificar possíveis caminhos para superar esses desafios.

Outrossim, em todos os documentos analisados no presente trabalho, verificou-se a importância do ciclo de melhoria contínua, ou ciclo PDCA nas Organizações, a qual, como aduz o próprio nome, consiste em uma série de medidas cíclicas, ininterruptas, onde o planejamento, a execução, a verificação e a ação, são as etapas para a visualização das vulnerabilidades, suas correções, seu monitoramento e sua posterior avaliação.

Demais disso, é através da cibersegurança que a confiança digital e a resiliência cibernética são alcançadas, seja porque são empreendidos esforços para evitar incidentes de segurança, seja porque as medidas implementadas visam fortalecer a capacidade organizacional de resposta e superação aos incidentes de segurança.

Portanto, defende-se no presente trabalho, que a cibersegurança é medida que se impõe às Organizações, porquanto inclui instrumentos de governança, inclusive a governança em privacidade, a segurança de dados, a gestão de riscos e, ainda, a atuação administrativa da ANPD, com poderes regulatório, fiscalizatório e sancionatório, sem prejuízo da atuação judicial, que também detém programa de medidas de prevenção e mitigação de riscos, no que pertine à sua competência atípica administrativa, regulamentando o tema.

## Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006. Disponível em:

https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf. Acesso em: 03 maio 2024.

BARDIN, Laurence. **Análise de Conteúdo**. 70 ed. São Paulo: 2016. p. 229.

BASTOS, Caroline Ayala de Carvalho; SPOSATO, Karyna Batista. Direito fundamental à proteção de dados pessoais: o reconhecimento constitucional da vulnerabilidade do titular no contexto da sociedade informacional. In: **Temas de Direito Constitucional**: estudos em homenagem ao Professor José Lima Santana. Aracaju: Editor Ubirajara Coelho Neto, 2022, p. 109-127.

BITTAR, Eduardo Carlos Bianca. **Metodologia da pesquisa jurídica**: teoria e prática da monografia para os cursos de direito. 17 ed. Saraiva, 2022. p 65.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Segurança da Informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, versão 1.0, outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 03 maio 2024.

BRASIL. Conselho Nacional de Justiça (CNJ). **Manual de Referência**: Prevenção e mitigação de ameaças cibernéticas e confiança digital. Brasília, DF: CNJ, março de 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVManualReferenciaPrevencaoMitigacaoDeAmeacasCiberneticasConfiancaDigitalRevisadoREV.docx.pdf. Acesso em: 03 maio 2024.

BRASIL. **Decreto nº 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 04 maio 2024.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,que%20lhe%20confere%20o%20art. Acesso em: 04 maio de 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

BRASIL. SUPREMO TRIBUNAL FEDERAL (STF). **Ação Direta de Inconstitucionalidade nº 6390 MC-REF / DF**. Relatora Ministra Rosa Weber, julgada em 07 de maio de 2020. Brasília: DF. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em 07 maio 2024.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança no 21729-4-DF**, Relator: Min. MARCO AURÉLIO, Relator p/ Acórdão: Min. NÉRI DA SILVEIRA, Tribunal Pleno, julgado em 05/10/1995, DJ 19-10-2001 PP-00033 EMENT VOL-02048-01 PP-00067 RTJ VOL-00179-01 PP-00225. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599. Acesso em: 23 abr. 2025.

CARNEIRO, André. Confiança digital: diferencial de negócios em um mundo digital. **Tecmundo**, 30 de junho de 2022. Disponível em: https://www.tecmundo.com.br/mercado/241123-confianca-digital-diferencial-negocios-mundo-digital.htm. Acesso em: 06 maio 2024.

CASTELLS, Manuel. **A sociedade em rede** (A era da informação, economia, sociedade e cultura). 6 ed. São Paulo: Paz e Terra, 1999.

FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais** - LGPD. Salvador: Editora JusPodivm, 2021.

***International Business Machines Corporation*** **- IBM**. O que é resiliência cibernética. Disponível em: https://www.ibm.com/br-pt/topics/cyber-resilience#:~:text=IBM-,O%20que%20%C3%A9%20resili%C3%AAncia%20cibern%C3%A9tica%3F,de%20incidentes%20de%20seguran%C3%A7a%20cibern%C3%A9tica. Acesso em: 06 maio 2024.

IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020.

KASEMIRSKI, André Pedroso. Reflexões sobre segurança, boas práticas, governança e *compliance* na proteção de dados pessoais. In: **Proteção de dados: fundamentos jurídicos**. Coordenadores Tarcísio Teixeira, Américo Ribeiro Magro - Salvador: Editora JusPodivm, 2021.

KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro; SOUZA, Carlos Henrique Medeiros. **Metodologia da pesquisa**: um guia prático. Ed. Via Litterarum, 2010. p 28.

LAMY, Marcelo. **Metodologia da pesquisa jurídica**: Técnicas de investigação, argumentação e redação. 2011. Elsevier Editora Ltda, 2010.

LÉVY, Pierre. **Cibercultura**. Tradução por Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

MARIA, Isabela; PICOLO, Cynthia. **Laboratório de Políticas Públicas e Internet (LAPIN).** Autodeterminação Informativa: Como esse direito surgiu e como ele me afeta? Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em: 07 maio de 2024.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: **Tratado de Proteção**

**de Dados Pessoais**. Coordenadores Bruno Bioni, Danilo Doneda, Ingo Wolfgang Sarlet, Laura Schertel Mendes, Otavio Luiz Rodrigues Junior. Rio de Janeiro: Forense, 2021.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais -TJMG. **Procedimento Comum Cível 5000110-18.2020.8.13.0569**. Des(A). Octávio de Almeida Neves, 1ª Vara Cível, Criminal e da Infância e da Juventude, julgamento em 23/04/2024, publicação em 23/04/2024.

PALUDO, Augustinho. **Administração Pública**. 10. ed. rev. ampl. e atual. - São Paulo: Editora JusPodivm, 2022.

POLESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no Brasil, à luz do direito comparado e dos standards internacionais de regulamentação** [recurso eletrônico]. – Caxias do Sul, RS: Educs, 2021. Disponível em: https://www.ucs.br/educs/arquivo/ebook/cibersegurancaprivacidade-e-protecao-de-dados-pessoais/. Acesso em: 04 maio de 2024.

QUAIS são os tipos de cibersegurança? **Instituto Brasileiro de Cibersegurança (IBSEC)**, 2024. Disponível em: https://ibsec.com.br/quais-sao-os-tipos-de-ciberseguranca/. Acesso em: 08 maio de 2024.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista de Direitos Fundamentais & Justiça** | Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875/985. Acesso em: 03 maio 2024.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

***Submetido em: 12 de maio de 2024.***
***Aprovado em: 09 de fevereiro de 2025.***