SEGURANÇA DA INFORMAÇÃO: PRIVACIDADE, EDUCAÇÃO E RESPONSABILIDADE NA ERA DIGITAL

Karolayne Cunha Barboza[1]
Faculdade de Direito de Cachoeiro de Itapemirim

Kryscila Ferreira Bessa Oliveira[2]
Faculdade de Direito de Cachoeiro de Itapemirim

Maria Deuceny da Silva Lopes Bravo Pinheiro[3]
Faculdade de Direito de Cachoeiro de Itapemirim

RESUMO
O objeto do presente artigo é a segurança da informação, com foco na importância da criptografia, do uso responsável de senhas e da educação digital como instrumentos de proteção no ambiente virtual. No contexto contemporâneo, o registro crescimento das ameaças cibernéticas e a falta de conscientização dos usuários quanto aos riscos de exposição de dados pessoais e institucionais. Nesse sentido, torna-se necessário compreender como as práticas de segurança digital e a formação de uma cultura voltada à proteção da informação podem contribuir para a preservação da privacidade, da integridade e da confiança nas interações online. O artigo busca demonstrar a relevância da educação digital na prevenção de ataques virtuais e na construção de uma sociedade mais consciente e segura. A metodologia foi conduzida com base na análise do corpus teórico-científico, incluindo artigos especializados, legislações e estudos que abordam a temática da segurança da informação, da criptografia e da responsabilidade digital. Os resultados indicam que práticas estruturadas de segurança digital, aliadas à educação digital, reduzem vulnerabilidades no ambiente virtual.

[1] Graduanda do Curso de Direito da Faculdade de Direito de Cachoeiro de Itapemirim (FDCI). Correio eletrônico: karolaynecunhabarboza@gamil.com
[2] Graduanda do Curso de Direito da Faculdade de Direito de Cachoeiro de Itapemirim (FDCI). Correio eletrônico: Kferreirabessaoliveira@gmail.com
[3] Doutora e Pós-doutora em Ciências da Educação pela Universidade de Coimbra. Investigadora do CEIS 20 da Universidade de Coimbra. Professora da Faculdade de Direito de Cachoeiro de Itapemirim. Correio eletrônico: deuceny@fdci.edu.br

Palavras-chave: Segurança da informação; Privacidade; LGPD; Marco Civil da Internet; Senhas.

ABSTRACT
The object of the present article is information security, with an emphasis on the importance of cryptography, the responsible use of passwords, and digital education as instruments of protection in the virtual environment. In the contemporary context, there has been a notable increase in cyber threats and a lack of user awareness regarding the risks associated with the exposure of personal and institutional data. In this regard, it becomes essential to understand how digital security practices and the development of a culture focused on information protection can contribute to the preservation of privacy, integrity, and trust in online interactions. This study aims to demonstrate the relevance of digital education in preventing cyberattacks and in building a more aware and secure society. The research was conducted through an analysis of theoretical and scientific literature, including specialized articles, legislation, and studies addressing information security, cryptography, and digital responsibility. The results indicate that structured digital security practices, combined with digital education, significantly reduce vulnerabilities within the virtual environment.

Key-words: Information Security; Privacy; General Data Protection Law (LGPD); Brazilian Internet Civil Framework; Passwords.

1. INTRODUÇÃO

A segurança da informação constitui um dos pilares para o funcionamento das instituições e para a proteção dos direitos fundamentais na sociedade digital. Em um contexto em que a informação se consolidou como ativo estratégico, a preservação de sua confidencialidade, integridade e disponibilidade tornou-se indispensável para o desenvolvimento de atividades pessoais, corporativas e governamentais. Assim, compreender os mecanismos que garantem a proteção dos dados e das comunicações é um imperativo diante da crescente dependência tecnológica e da complexidade dos sistemas informacionais.

A problemática que circunda a segurança da informação decorre, sobretudo, da ampliação das ameaças cibernéticas e da vulnerabilidade dos usuários e instituições diante de ataques e falhas de proteção. Vazamentos de dados, invasões a sistemas e fraudes eletrônicas evidenciam a fragilidade das práticas de segurança e a necessidade de políticas eficazes de prevenção e conscientização. Essa realidade demonstra que a

proteção informacional não se restringe ao âmbito técnico, mas envolve também dimensões éticas, comportamentais e jurídicas, exigindo uma abordagem interdisciplinar para garantir a confiança e a estabilidade do ambiente digital.

Diante desse cenário, o presente artigo pretende geral analisar os principais instrumentos e práticas voltados à segurança da informação, enfatizando a importância da encriptação, da gestão responsável de senhas, da educação dos usuários, do uso de programas antivíruse *antispywares,* da realização de cópias de segurança e da criação de senhas fortes e distintas. Busca-se, assim, demonstrar como tais medidas, articuladas entre si, contribuem para a consolidação de um ambiente digital mais seguro e alinhado às exigências legais de proteção de dados.

No que se refere aos aspectos metodológicos, trata-se de uma pesquisa de natureza qualitativa e exploratória, fundamentada em revisão bibliográfica de obras, artigos científicos e legislações pertinentes ao tema, incluindo a Constituição Federal de 1988, o Marco Civil da Internet, Lei n.º 12.965/2014 (Brasil, 2014) e a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (Brasil, 2018).

Desse modo, a análise desses referenciais permitiu estabelecer uma compreensão integrada entre os aspectos técnicos, jurídicos e educativos que envolvem a proteção das informações. Com base nessa perspectiva, a estrutura do presente artigo organiza-se em sete seções, além desta introdução. Inicialmente, aborda-se a encriptação da informação, destacando sua função na proteção da confidencialidade e autenticidade dos dados. Em seguida, trata-se da partilha de senhas, evidenciando os riscos e as responsabilidades legais decorrentes dessa prática. Na sequência, discute-se a educação dos usuários, ressaltando sua importância na prevenção de incidentes cibernéticos. Posteriormente, são analisados os programas antivírus, antimalwares e antispywares como barreiras essenciais à invasão e à captura de dados. Adiante, apresentam-se as cópias de segurança como estratégia de preservação e recuperação da informação. Por fim, examina-se a relevância do uso de senhas fortes e distintas,

relacionando-o aos princípios de proteção de dados e aos métodos modernos de autenticação.

Espera-se que o texto contribua para o fortalecimento da cultura de segurança digital, evidenciando que a proteção informacional resulta da integração entre tecnologia, conscientização e responsabilidade jurídica — elementos indispensáveis à consolidação de uma sociedade digital segura, ética e confiável.

2 A CRIPTOGRAFIA COMO FUNDAMENTO DA SEGURANÇA DA INFORMAÇÃO

Na era digital, a informação tornou-se um dos bens mais valiosos da sociedade. Mensagens, transações financeiras e dados pessoais circulam em rede a cada segundo, conectando indivíduos e instituições em escala global. Essa realidade, embora traga praticidade e dinamismo, também expõe vulnerabilidade: o que aconteceria se tais informações fossem interceptadas ou manipuladas no percurso? É diante dessa ameaça que a encriptação se afirmar como instrumento essencial para a proteção da privacidade e da segurança no mundo contemporâneo.

Conforme Teixeira (2023, p. 19), a encriptação, também denominada criptografia consiste em uma técnica de comunicação segura que tem por objetivo proteger dados contra acessos não autorizados. Por meio dela, uma informação legível é transformada em um código indecifrável, utilizando-se um algoritmo matemático e uma chave criptográfica. Assim, apenas quem possui a chave correta pode reverter o processo e acessar o conteúdo original.

Por séculos, a criptografia, uma disciplina com raízes profundas na matemática e na engenharia, foi um domínio estrito do Estado-Nação. Apenas atores estatais tinham acesso a versões robustas, virtualmente inquebráveis. Essa realidade, contudo, foi radicalmente alterada. A partir da década de 1970, quando o surgimento da computação digital, juntamente com a invenção crucial da “encriptação de chave pública”, impulsionou esta tecnologia para fora dos círculos governamentais. Dessa forma, a

criptografia tornou-se mais amplamente disponível em nossa sociedade, demonstrando uma adaptação excepcional aos ambientes digitais. Nesse contexto, essa evolução levou à implantação generalizada de técnicas criptográficas, as quais se consolidaram como uma ferramenta essencial para indivíduos, o setor comercial e o setor público, protegendo informações, comunicações e, fundamentalmente, garantindo o anonimato e a privacidade (Schulz; Van Hoboken, 2016).

A partir dessa transformação, compreender a relevância da criptografia implica reconhecê-la não apenas como um instrumento de proteção da privacidade de dados e comunicações, mas também como um mecanismo essencial para assegurar a autenticidade das mensagens, resguardando-as contra alterações de terceiros e garantindo a identificação do emissor de uma comunicação criptografada. (Gill et al., 2018, *apud* Teixeira, 2023).

Nesse sentido, a confiabilidade das comunicações digitais apoia-se em uma arquitetura técnica fundamentada na classificação dos sistemas criptográficos, que se subdividem em simétricos e assimétricos. Enquanto o simétrico se caracteriza pelo uso de uma única chave para cifrar e decifrar mensagens, o assimétrico apresenta uma estrutura mais avançada, baseada em um par de chaves distintas e matematicamente relacionadas: uma pública, destinada à encriptação, e outra privada, utilizada exclusivamente pelo destinatário para a decriptação. (Teixeira, 2023, p. 20). Esse modelo, conhecido como criptografia assimétrica, não apenas mitiga riscos de intercepção e acesso indevido, como também viabiliza mecanismos de autenticação e assinatura digital, garantindo a integridade e a origem das informações transmitidas. Dessa forma, constitui um dos pilares técnicos da segurança da informação na contemporaneidade, assegurando confiabilidade às transações digitais e à proteção de dados sensíveis. (Teixeira, 2023).

Outro aspecto relevante da criptografia assimétrica, pertinente ao presente estudo, manifesta-se na encriptação de ponta a ponta, amplamente empregada em

aplicações e serviços de comunicação pela internet. Conforme esclarece Linguori, (2022, *apud* Teixeira, 2023):

> A ideia desse mecanismo é, de forma simplificada, cifrar o conteúdo da mensagem no dispositivo do emissor a partir da chave pública do receptor e ela só pode ser decifrada no dispositivo do receptor a partir de sua chave privada. Nessa lógica, mesmo se houver um servidor central que encaminhe a mensagem a um usuário do sistema, ele não conseguirá acessar o conteúdo da mensagem, uma vez que não possui a chave para tanto.

Além disso, constata-se a aplicação de um modelo criptográfico híbrido, que integra o uso de chaves simétricas e assimétricas, em conjunto com funções *hash,* frequentemente empregadas em mecanismos de certificação digital. Nesse contexto, para que um agente mal-intencionado consiga decifrar uma informação protegida, seria necessário obter a chave privada correspondente, seja por meio de subtração indevida, seja pela tentativa de força bruta, isto é, pela exploração exaustiva das inúmeras combinações possíveis dentro do universo de chaves existentes. (Garbe, 2021, *apud* Teixeira, 2023).

Desse modo, o aumento do comprimento das chaves criptográficas, medidos em bits, eleva exponencialmente a complexidade computacional exigida para a sua quebra, consolidando-se como um mecanismo de reforço à segurança digital. Sob essa perspectiva, a ampliação das chaves configura um recurso de dissuasão tecnológica, uma vez que torna inviável ou economicamente desvantajoso o esforço de agentes maliciosos para violar sistemas de proteção informacional. Em consequência, observa-se o fortalecimento da confiabilidade e da integridade dos ambientes digitais, assegurando que a criptografia de alta complexidade permaneça como elemento essencial à preservação da confidencialidade e da autenticidade das comunicações no cenário cibernético contemporâneo (Teixeira, 2023, p. 21).

Diante desse panorama técnico, torna-se evidente que a criptografia não se limita a um instrumento matemático de segurança, mas representa também um mecanismo jurídico e social de proteção de direitos fundamentais, em especial o direito à privacidade e à inviolabilidade das comunicações. A consolidação dessa tecnologia impôs novos desafios ao campo jurídico, exigindo adequações normativas capazes de compatibilizar o avanço tecnológico com a efetiva tutela das informações.

No ordenamento jurídico brasileiro, a proteção das comunicações encontra respaldo direto na Constituição Federal de 1988, em seus artigos 5°, incisos X e XII. O inciso X assegura que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrentes de sua violação", enquanto o inciso XII dispõe que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer" (Brasil, 1988). Esses dispositivos conferem à criptografia um fundamento constitucional implícito, legitimando-a como meio técnico de resguardar a confidencialidade das interações e comunicações digitais.

Ademais, o Marco Civil da Internet, Lei n° 12.965 (Brasil, 2014) atua de forma complementar à Constituição Federal, reforçando a proteção das comunicações no ambiente digital. Conforme estabelece o artigo 7°, inciso II, "a inviolabilidade e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial", a legislação não apenas consagra o direito ao sigilo, mas também reconhece a necessidade de medidas técnicas que assegurem sua efetividade. Logo, a criptografia garante que as informações trocadas permaneçam protegidas, concretizando a segurança da comunicação.

Dessa forma, percebe-se que o marco normativo relativo à criptografia não apenas legitima seu uso, mas também a consolida como elemento essencial da segurança jurídica e tecnológica contemporânea. Ao tutelar a integridade das informações e das interações digitais, o Direito reconhece na criptografia um instrumento indispensável

para a efetividade da proteção de dados e da liberdade informacional.

3. PARTILHA DE SENHAS: ENTRE O COMODISMO E O RISCO: A VULNERABILIDADE HUMANA NA SEGURANÇA DIGITAL

O uso de logins, senhas e e-mails tornaram-se rotina no cotidiano digital, envolvendo redes sociais, plataformas de ensino e sites de compras. No entanto, a repetição de senhas entre diferentes contas e o compartilhamento dessas credenciais com terceiros têm se mostrado práticas comuns e perigosas. Uma pesquisa realizada no ano de 2022 pela Netfive aponta que 60% dos gaúchos utilizam a mesma senha para contas diferentes, além disso, cerca de 25% compartilham suas senhas com colegas, familiares ou amigos. Embora essas ações facilitem o dia a dia, elas comprometem a proteção de dados pessoais e institucionais, expondo informações sensíveis a riscos de acesso não autorizado (Pontifícia Universidade Católica do Rio Grande do Sul, Tecnopuc, 2022).

Além da prática de reutilização ou compartilhamento de senhas, o estudo evidencia a relevância do fator humano na segurança digital. O usuário é frequentemente o ponto de entrada para ataques cibernéticos, sendo o comportamento inadequado, como a partilha de senhas, um fator de vulnerabilidade crítico. A pesquisa da Netfive também aponta que, mesmo entre pessoas conscientes, há grande subestimação do risco: 43% dos respondentes acreditam que perceberam se uma conta foi hackeada, o que nem sempre ocorre. (PUC-RS, Tecnopuc, 2022).

Para mitigar esses riscos, a implementação de medidas administrativas de segurança da informação é essencial. Entre elas, destaca-se a Política de Segurança da Informação (PSI), definida como um conjunto de diretrizes e regras que permitem planejar, implementar e controlar ações relacionadas à proteção de dados em uma organização. Embora não seja obrigatória, sua adoção, mesmo que simplificada,

demonstra boa-fé e diligência, orientando práticas seguras, como cópias de segurança, atualização de softwares, controle de acesso e, especialmente, não compartilhar logins e senhas (Autoridade Nacional de Proteção de Dados, 2021).

Além da PSI, a conscientização e o treinamento dos funcionários são cruciais. Segundo a ANPD (2021), os colaboradores devem ser informados sobre suas responsabilidades legais no tratamento de dados pessoais, receber orientações sobre o uso correto dos sistemas de TI, sobre prevenção contra-ataques de *phishing* e sobre medidas básicas de proteção, como bloquear computadores ao se afastar ou manter documentos físicos seguros. Essas práticas reforçam que a segurança da informação não depende apenas de tecnologia, mas também da conduta ética e consciente dos usuários.

Diante dos riscos crescentes da partilha de senhas, torna-se essencial compreender como o ordenamento jurídico brasileiro protege a segurança da informação e os dados pessoais. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709 (Brasil, 2018) estabelece que os agentes de tratamento devem adotar medidas técnicas e administrativas para garantir a segurança, integridade e confidencialidade de dados pessoais, conforme descrito em seu artigo 6º, que trata dos princípios da proteção de dados, incluindo a necessidade de segurança adequada. A lei ainda reforça, em seu artigo 46°, que os controladores e operadores de dados têm o dever de implementar medidas de segurança, técnicas e administrativas, capazes de prevenir acessos não autorizados, incidentes de segurança e compartilhamento indevido de credenciais.

Além disso, o artigo 48° da LGPD prevê que os agentes de tratamento devem manter registros de operações de tratamento e demonstrar a adoção de medidas de segurança, especialmente em ambientes digitais onde senhas e credenciais são compartilhadas ou reutilizadas de forma imprópria. Dessa maneira, a partilha negligente de senhas não é apenas uma falha operacional: ela se enquadra diretamente em descumprimento da legislação, uma vez que expõe dados pessoais de clientes,

colaboradores e parceiros a riscos de acesso indevido.

Complementando, a Lei nº 12.737 (Brasil, 2012), conhecida como Lei "Carolina Dieckmann", criminaliza o acesso não autorizado a dispositivos e sistemas de informação. O compartilhamento de credenciais facilita a prática de crimes cibernéticos, tornando os responsáveis civil e penalmente responsabilizados, reforçando a necessidade de políticas internas e conscientização sobre boas práticas de segurança.

À luz do exposto, evidencia-se que a partilha de senhas constitui um desafio crítico, envolvendo aspectos técnicos, comportamentais e jurídicos. Nesse cenário, a adoção de políticas de segurança da informação robustas, a conscientização contínua dos colaboradores e a utilização de mecanismos de autenticação multifatorial não apenas mitigam riscos, mas também concretizam a proteção de dados pessoais prevista na LGPD. Assim, práticas antes vulneráveis podem ser convertidas em estratégias efetivas de segurança digital, promovendo a integridade das informações e consolidando a confiança nas operações em ambientes virtuais.

4. O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO: ESTRATÉGIAS DE EDUCAÇÃO CONTÍNUA PARA MITIGAR O RISCO HUMANO.

Conforme Freitas e Araújo (apud Bauer, 2006, p. 42), a educação contínua dos usuários representa um componente essencial para a gestão da segurança da informação, visto que grande parte dos incidentes e vulnerabilidades encontram origem na própria rede interna das organizações. Frequentemente, falhas decorrentes do desconhecimento de procedimentos básicos ou da utilização inadequada de recursos tecnológicos podem gerar riscos significativos, comprometendo a integridade, confidencialidade e disponibilidade das informações. Diante desse cenário, a implementação de práticas educativas constantes torna-se imprescindível, assegurando que todos os colaboradores compreendam a relevância de suas ações na proteção de

dados e sistemas corporativos.

Além disso, situações recorrentes evidenciam a relevância desse processo educativo. Por exemplo, a má configuração de programas de leitura de e-mails pode permitir que arquivos anexados sejam executados automaticamente, favorecendo a instalação de *backdoors*, cavalos de Tróia e a disseminação de vírus. Tais incidentes demonstram que, mesmo com tecnologias avançadas e sistemas de proteção sofisticados, a atuação inadequada dos usuários permanece como um dos vetores críticos de risco. Nesse sentido, a conscientização insuficiente pode potencializar os impactos de ataques cibernéticos, aumentando a probabilidade de comprometimento de informações sensíveis e a propagação de ameaças internas (Bauer, 2006).

Dessa forma, o estabelecimento de políticas de segurança e normas de uso aceitável revela-se fundamental para a criação de um ambiente corporativo seguro. Para que essas diretrizes sejam eficazes, é imprescindível serem claras, objetivas e amplamente compreendidas, evitando ambiguidades e promovendo a adoção de práticas seguras no dia a dia da organização. Incluem-se nesse contexto orientações sobre senhas, compartilhamento de dados, uso de e-mails e sistemas internos, bem como instruções relativas à atualização de softwares e à implementação de medidas preventivas. A efetividade dessas políticas depende, portanto, de um esforço contínuo de comunicação e treinamento, garantindo que todos os colaboradores conheçam suas responsabilidades e consigam aplicar corretamente os procedimentos definidos (Freitas & Araújo, apud Bauer, 2006).

Adicionalmente, a criação de canais de comunicação internos, como boletins informativos, listas de e-mails e comunicados periódicos, constitui uma estratégia eficaz para disseminar informações sobre segurança. Tais canais permitem informar os usuários sobre novos vírus, vulnerabilidades detectadas e métodos de prevenção. Embora algumas vulnerabilidades não afetem diretamente os usuários, o compartilhamento de conhecimento sobre ameaças e medidas protetivas assegura que

todos estejam preparados para adotar condutas seguras. Com isso, os usuários tornam-se agentes ativos da segurança, fortalecendo a cultura organizacional e reduzindo consideravelmente o risco de incidentes internos (Bauer, 2006). Nesse cenário, o Decreto nº 10.474/2020, que institui a Política Nacional de Segurança da Informação e Comunicações (PNSIC), estabelece diretrizes para a capacitação e conscientização dos usuários quanto a protocolos de segurança e procedimentos de acesso seguro em órgãos públicos e empresas reguladas. Sob essa ótica, políticas internas de empresas, como controles rigorosos de senhas, autenticação de múltiplos fatores e restrições de acesso, funcionam como instrumentos concretos de operacionalização do decreto, garantindo que os colaboradores compreendam e cumpram suas responsabilidades na preservação da segurança da informação.

Assim, a integração entre a capacitação dos usuários e as normas estabelecidas pelo PNSIC evidencia que a proteção da informação depende não apenas de tecnologia, mas também do engajamento e conscientização de todos os envolvidos. Dessa forma, a educação contínua dos colaboradores constitui um pilar indispensável para a redução de riscos, a prevenção de incidentes e a consolidação de uma cultura organizacional voltada à segurança da informação.

5. *MALWARES, SPYWARES* E LGPD: PROTEÇÃO CIBERNÉTICA COMO PILAR DA PRIVACIDADE EM UM MUNDO CONECTADO

Em uma sociedade amplamente conectada, na qual o fluxo de informações se intensifica a cada instante, torna-se inevitável refletir sobre os mecanismos de proteção que garantem a segurança dos dados digitais. A exposição constante a ambientes virtuais, somada à ausência de práticas preventivas, favorece a ação de *softwares* maliciosos capazes de comprometer a integridade de dispositivos e informações pessoais. Desse modo, compreender a relevância de ferramentas voltadas à detecção e à neutralização

dessas ameaças é essencial para a preservação da privacidade e da confiabilidade no uso das tecnologias contemporâneas.

A informação é gerada a partir do processamento de dados. Por exemplo, os dados provenientes de uma transação de compra, quando processados, transformam-se em informações de alto valor para áreas como finanças, bancos de dados, contabilidade e outros setores (Barbosa; Silva; Sousa, 2017). Nesse sentido, a aceitação de termos de uso muitas vezes marcada como "lida" sem uma leitura atenta por parte do usuário pode resultar no compartilhamento de dados pessoais com diversas empresas. A não leitura desses termos leva, frequentemente, à aceitação da divulgação desses dados. Neste contexto, a aceitação de termos ou o *download* de aplicativos sem o devido conhecimento podem inadvertidamente abrir a porta para *malwares.* Estes são programas desenvolvidos visando "roubar informações sigilosas, senhas de bancos, cartões de crédito, pois, tudo que o usuário faz dentro do sistema fica nos registros e quem tem conhecimento no assunto consegue rastrear cada passo" (Barbosa; Silva; Sousa, 2017, p. 5). A infecção pode ocorrer de forma imperceptível, com códigos maliciosos ocultos em aplicativos ou mesmo em websites visitados, dado que o vírus consiste em programas ou códigos infecciosos que se anexam a outras partes de *software* e, subsequentemente, se replicam quando esse software é executado (Barbosa; Silva; Sousa, 2017). Como exemplo, pode-se citar a notificação que surge em um dispositivo após a visita a um site, alertando sobre a presença de vírus.

Ademais, existem variados tipos de *malwares*, como o adware, considerado o menos nocivo e o mais rentável, que se limita a exibir anúncios no computador do usuário. Em contrapartida, o *spyware* é classificado como o tipo mais grave, uma vez que se trata de um *software* que espiona o indivíduo, monitorando suas atividades online e sendo utilizado para enviar publicidade (*adware*) de volta ao sistema (Barbosa; Silva; Sousa, 2017). Assim, os *malwares* podem causar danos ao equipamento e vazar dados pessoais, o que contraria os princípios da LGPD, legislação criada justamente para

proteger os dados dos cidadãos no ambiente virtual.

Há também os *keyloggers*, que podem estar integrados a *spywares* ou mesmo a aplicativos de teclado legítimos. Estes são definidos como componentes de pacotes de *spyware* instalados em smartphones sem o consentimento do usuário. A maioria desses aplicativos é capaz de capturar dados digitados no teclado, permitindo que as informações sejam armazenadas localmente ou transmitidas automaticamente pela rede a um computador, ou servidor remoto (Nasaka, 2011 *apud* Alonso, Martinez, Santos, Cunha, Amaral, 2015).

Contudo, existem *softwares* destinados a combater esses códigos maliciosos, como os antivírus e os *antispywares*. No entanto, a atualização de suas definições é, frequentemente, mais lenta do que a criação de novas variantes de *malwares*. Dentre as diversas técnicas empregadas por aplicativos antivírus, a mais comum baseia-se na detecção da assinatura do arquivo suspeito por meio da comparação com um banco de dados previamente atualizado (Silva, Silva, 2018). Dessa forma, o usuário pode instalar aplicativos antivírus e *antispywares* como medida preventiva contra-ataques de *malwares*. Caso essas ferramentas não sejam suficientes, ainda existem outros meios para intervir e evitar o roubo ou a contaminação de dados, como a busca por auxílio de um profissional especializado.

Com a crescente interconexão mundial, a proteção contra *malwares* e *spywares* transcende a recomendação, configurando-se como uma medida essencial para a salvaguarda da privacidade e segurança dos dados pessoais, em estrita observância à LGPD. A adoção de práticas como a leitura minuciosa dos termos de uso, a prudência em relação a *downloads* duvidosos e a utilização de *softwares* de proteção devidamente atualizados permite aos usuários mitigarem significativamente os riscos e navegar com maior segurança no ambiente digital. Desse modo, o investimento contínuo em conscientização e em ferramentas de segurança apropriadas estabelece o mecanismo de defesa mais eficaz contra essas ameaças em constante mutação

6. CÓPIAS DE SEGURANÇA PARA A PRESERVAÇÃO E RESTAURAÇÃO DE DADOS NA ERA DIGITAL

A segurança e a durabilidade dos dados adquirem relevância central, particularmente porque falhas técnicas ou eventos imprevistos que podem gerar perdas consideráveis. Assim, é fundamental estabelecer práticas que assegurem a integridade e a disponibilidade das informações, mesmo diante dos riscos inerentes ao ambiente virtual.

As cópias de segurança (ou *backups*) constituem uma medida primordial, dada a sua capacidade de preservar informações digitais de maneira segura. Tais informações englobam dados de valor inestimável para o usuário, como fotografias pessoais, trabalhos de conclusão de curso (TCCs), arquivos profissionais e documentos diversos, cuja perda é indesejada. Frequentemente, o processo de seleção e armazenamento dos dados é percebido como tedioso e excessivamente demorado; contudo, a verdadeira importância dessas cópias é reconhecida apenas em momentos de necessidade, quando, muitas vezes, é tardio para a sua criação.

Atualmente, o avanço tecnológico simplificou significativamente a realização de *backups.* É possível, por exemplo, programar a execução dessas cópias em dispositivos móveis (*smartphones*) em horários que melhor se ajustem à rotina do usuário. Ademais, conforme diretrizes governamentais (Brasil, 2023), a frequência dos *backups* de serviços pode ser ajustada, sendo exemplos as periodicidades diária, semanal, mensal ou anual. A escolha da frequência mais adequada deve ser pautada na intensidade com que os dados são modificados. Dessa forma, em situações como o roubo de um dispositivo móvel, o usuário pode recuperar suas informações por meio dos backups previamente realizados, mesmo utilizando um aparelho distinto.

Existem diversas metodologias para a realização de cópias de segurança, sendo as mais empregadas: o *backup* completo, que "representa a cópia de todo o banco de

dados, sendo este um novo banco de dados" (Microsoft Corporation, 2012 *apud* Viana, 2020, p. 15); o *backup* incremental, que consiste na "cópia somente dos dados que foram modificados após o último *backup*" (Dong, et al., 2010, *apud* Viana, 2020, p. 16); e o *backup* diferencial, que "tem como base o *backup* completo, contendo apenas as modificações feitas após o último backup completo realizado e a soma dos *backups* diferenciais que forem realizados anteriormente" (Microsoft Corporation, 2012 *apud* Viana, 2020, p. 17). Assim, a escolha do método mais adequado de cópia de segurança deve considerar a quantidade de dados a serem armazenados, os custos envolvidos (se aplicável) e o nível de confiabilidade depositado nos recursos disponíveis.

Logo, as cópias de segurança são instrumentos inerentes no contexto digital, atuando na proteção de dados valiosos contra perdas. Embora possam parecer complexas, as tecnologias contemporâneas facilitaram o processo, oferecendo opções de agendamento personalizado e diversas alternativas de armazenamento. A seleção do método ideal de backup deve levar em conta as necessidades específicas de cada indivíduo, ponderando a volumetria dos dados, os custos e a confiabilidade das soluções. Seja por meio de mídias físicas, cartões de memória ou serviços em nuvem (online), a prática do *backup* assegura a integridade e a facilidade na recuperação das informações, reforçando a necessidade de priorizar essa ação preventiva para evitar perdas potencialmente irreparáveis.

7. PRÁTICAS CONSCIENTES NA GESTÃO DE SENHAS E MÉTODOS DE AUTENTICAÇÃO.

Em um contexto de acelerada intensificação da conectividade e da exposição digital, a proteção das informações pessoais configura-se como um desafio permanente. Desse modo, a atenção voltada à segurança de acessos e credenciais torna-se indispensável, uma vez que pequenas falhas podem gerar consequências expressivas no âmbito virtual. Portanto, ao abordar o cuidado com senhas e métodos de autenticação,

destaca-se a necessidade de adoção de práticas conscientes que fortaleçam a privacidade e a confiança nas interações digitais.

A utilização de credenciais de acesso robustas e distintas é um imperativo na prevenção de violações de segurança cibernética em contas digitais. A adoção de senhas de baixa complexidade eleva a vulnerabilidade dos usuários, uma vez que a fragilidade das credenciais e a carência de protocolos de segurança adequados podem culminar em severas consequências negativas. Estes riscos incluem a exposição a fraudes financeiras, prejuízos à reputação, ofensas à honra e potencial chantagem, facilitados pelo acesso indevido de agentes mal-intencionados a informações sensíveis e de caráter pessoal (Inglesant et al. 2010 apud Gonçalves, Christino, Chang, Martini, 2021). Esta situação, por sua vez, contraria os princípios estabelecidos pela LGPD.

Neste panorama, torna-se vital a não partilha de senhas ou IDs, e a manifestação de ceticismo diante de solicitações de credenciais ou direcionamentos para links suspeitos, dado o risco de tentativas de ataques de engenharia social. Golpes disseminados em plataformas de redes sociais frequentemente se valem de comunicações fraudulentas que visam a obtenção de dados pessoais, como senhas ou informações de cartões de crédito. Com o avanço tecnológico, a sofisticação dessas estratégias tem aumentado, com criminosos se passando por representantes de entidades confiáveis ou simulando interações de contatos próximos para adquirir informações destinadas a fins ilícitos (Almeida, 2023). Desse modo, a notificação de tentativas de fraude é recomendada como medida de proteção à coletividade.

Não obstante, a busca pela conveniência no cotidiano frequentemente conduz à escolha pela repetição de uma mesma senha em múltiplas aplicações. Embora facilite a memorização e o gerenciamento, acarreta uma exposição a riscos consideráveis, incluindo o comprometimento de dados e perdas financeiras. Por conseguinte, preconiza-se o emprego de credenciais singulares para cada plataforma, visando mitigar a probabilidade de acesso não autorizado a contas diversas.

Adicionalmente, conforme assinalado por Mitnick (2017 apud Almeida, 2023), a incorporação de dados de cunho pessoal, como datas de nascimento ou nomes de animais de estimação, na composição das senhas, compromete a sua robustez. Apesar que as informações facilitem a memorização, elas introduzem um vetor de risco. Recomenda-se, assim, que a criação de novas credenciais priorize a complexidade em detrimento da mera conveniência, optando por combinações estruturadas que preservem a praticidade para o uso diário. Muitos serviços online atualmente implementam requisitos mínimos de segurança para senhas, como a inclusão de caracteres em caixa alta e baixa, algarismos, e um comprimento mínimo de, tipicamente, oito caracteres, o que contribui para o fortalecimento da segurança.

Neste sentido, é pertinente a integração das senhas com métodos biométricos, como a identificação facial, ou a adoção exclusiva destes como mecanismos de autenticação. Contudo, há três pilares de autenticação: conhecimento, posse e característica. A autenticação baseada no conhecimento (ex. senhas) é a mais ubíqua e menos segura, dado o risco de descoberta por terceiros ou por ataques de força bruta. Em contraste, a autenticação baseada na posse requer um artefato físico, como um *token* que gera códigos variáveis temporalmente. Por fim, a autenticação baseada em características intrínsecas ao indivíduo, que utiliza tecnologias biométricas para a verificação de identidade, é considerada o método mais rigoroso (Rountree et al. 2013 apud Gonçalves, Christino, Chang, Martini, 2021).

Em face dos riscos inerentes ao ecossistema digital, a adoção de protocolos de autenticação segura transcende a mera comodidade, configurando-se como uma defesa proativa contra ameaças cibernéticas. A integração de senhas complexas com camadas multifatoriais, como a biometria e a identificação facial, eleva significativamente o nível de proteção pessoal dos usuários. Adicionalmente, a vigilância contra comunicações suspeitas, a salvaguarda das credenciais de acesso e a formalização de denúncias são ações complementares que contribuem para a tranquilidade e a segurança das contas

digitais.

8. CONCLUÇÃO

O presente estudo explorou a relação entre os fundamentos da segurança da informação, abrangendo desde a encriptação sustentada pela matemática e legitimada pelo direito até as práticas comportamentais dos usuários, a defesa contra *malwares* e a importância das rotinas de preservação de dados. O objetivo central de analisar a criptografia como alicerce da segurança e de correlacionar aspectos técnicos, comportamentais e jurídicos da proteção da informação.

Iniciando pela encriptação, demonstrou-se seu papel essencial na proteção da privacidade e da segurança, evoluindo de um domínio estatal para uma ferramenta universal, baseada em sistemas criptográficos simétricos e, predominantemente, assimétricos. Essa tecnologia não é apenas um instrumento técnico, mas um mecanismo de tutela de direitos fundamentais, com respaldo explícito no ordenamento jurídico brasileiro, notadamente na Constituição Federal e no Marco Civil da Internet.

Em contraste, o estudo confrontou a solidez da criptografia com a vulnerabilidade inerente ao fator humano, especificamente na seção sobre partilha de senhas. Evidenciou-se que a reutilização e o compartilhamento de credenciais constituem falhas críticas de segurança, sendo um desafio que transcende a tecnologia e demanda medidas administrativas, como a PSI, além de estar diretamente ligada ao cumprimento da LGPD.

A formação dos usuários foi, destacada como um aspecto essencial, voltado a minimizar ocorrências resultantes da ausência de informações e das práticas impróprias. A capacitação contínua, em consonância com o Decreto nº 10.474/2020, configura-se como um pilar que transforma o colaborador em agente ativo da segurança.

Em um plano de defesa reativa, a análise dos programas antivírus e antispywares sublinhou a necessidade de mecanismos de proteção contra códigos maliciosos

(*malwares*), cujo surgimento e sofisticação estão em constante ascensão, violando princípios da LGPD. Complementarmente, a abordagem das cópias de segurança (*backups*) consolidou essa prática como uma medida fundamental para garantir a integridade e a disponibilidade dos dados, independentemente de incidentes.

Por fim, a seção sobre senhas fortes e diferentes amarrou a temática da segurança comportamental, reforçando o imperativo de credenciais robustas e singulares e a adoção de métodos de autenticação multifatorial.

Logo, os resultados alcançados demonstram a segurança da informação como um ecossistema complexo, no qual a criptografia fornece a base técnica e jurídica, mas cuja efetividade final é determinada pela conduta humana, pela capacitação e pela adoção de medidas preventivas e de recuperação. A interconexão desses elementos revela que a proteção de dados na era digital é uma responsabilidade compartilhada, exigindo tanto o avanço tecnológico quanto a conscientização contínua, para que os direitos e a confiabilidade sejam plenamente assegurados no ambiente virtual.

REFERÊNCIAS

ALMEIDA, R. N. de. **Estelionato Virtual no Direito brasileiro.** 2023. 51 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/6205/1/Artigo%20-%20Ruanh%20Neres%20de%20Almeida.pdf.

ALONSO, C. de M. et al. **Estudo sobre spywares.** Uma proposta de solução para o controle de dispositivos móveis. 2015. Disponível em: file:///C:/Users/delle/Downloads/rdazzi,+46.+137925%20(1).pdf.

BARBOSA, M. V. H.; SILVA, B. R. de A. e; SOUSA, J. F. de. **Prevenção de ataques causados por malwares**. 2017. Disponível em: https://www.unibalsas.edu.br/wp-content/uploads/2017/01/ARTIGO-MARCOS-HERES.pdf.

BAUER, César Adriano. **Política de segurança da informação para redes corporativas.** Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro

Universitário Feevale, Novo Hamburgo, 2006

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.** Versão 1.0. Brasília, DF: ANPD, 2021. 19. p. Disponível em: https://www.gov.br/anpd/pt-br/centrais-deconteudo/materiais-educativos-e-publicacoes/guia-vf.pdf.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2025]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Modelo de Política de Backup**. Versão 2.0. Brasília, DF, mar. 2023. 17 p. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_backup.pdf.

GONÇALVES, E. et al. **Usabilidade e Segurança nos Métodos de Geração de Senhas**. 2021. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/34dc3a36-df7f 4f0c-817d-4238c53f7bc7/content .

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL. TECNOPUC. **Segurança da Informação: compartilhamento de senhas ainda é uma prática comum entre as pessoas.** Tecnopuc, [S. l.], 23 mar. 2022. Disponível em: https://tecnopuc.pucrs.br/seguranca-da-informacao-compartilhamento-de-senhas-ainda-e uma-pratica-comum-entre-as-pessoas/.

SCHULZ, Wolfgang; HOBOKEN, Joris van. **Direitos humanos e criptografia**. Tradução brasileira por Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Paris: UNESCO, 2016.

(Série da UNESCO sobre Liberdade na Internet). Disponível em: https://itsrio.org/wp content/uploads/2018/10/direitos-humanos-e-criptografia-1.pdf.

SILVA, Johan Matos Coelho da; SILVA, Philipe Matos Coelho da. **Técnicas de detecção e classificação de malwe classificaçãovisualização de binários**. 2018. 61 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Redes de Comunicação) – Departamento de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2018.

TEIXEIRA, Pedro Mazalotti. **Escolhas político regulatórias envolvendo o uso de criptografia**. 2023. 97 f. Dissertação (Mestrado Profissional em Direito e Tecnologia) – Escola de Direito de São Paulo, Fundação Getúlio Vargas, São Paulo, 2023.

VIANA, Frank Jonh Soares. **O processo de backup:** uma análise em prefeituras do Rio Grande do Norte. Angicos/RN: Universidade Federal Rural do Semi-Árido, 2020.