Prevenção de Golpes Digitais: O Papel da Cibersegurança na Proteção do Usuário

Nelcy Renata Silva de Souza [1], Verônica Maria Félix da Silva[2], Amanda Nicole Aguiar de Oliveira[3], Roselma Coelho Santana[4]

[1] Universidade Federal do Amazonas (UFAM) – Manaus, AM – Brazil.

[2 3 4] Universidade do Estado do Amazonas (UEA) – Manaus, AM – Brazil.

nelcy.renata@gmail.com, veronica.mfsjesus@gmail.com,
amanda.nicoleaguiar@outlook.com, roselma_santana@hotmail.com

Abstract. *The growth in connectivity and the use of services has created new vulnerabilities for users, especially in the face of digital scams. In this context, cybersecurity has emerged as an essential field in the protection of personal data and information. A research aims to analyze the role of cybersecurity in preventing digital scams, highlighting user protection practices and strategies. A qualitative methodology was used, based on a bibliographical review and document analysis of technical reports. It was found that effective prevention requires not only the use of technological tools, but also the digital education of users in the virtual environment.*

Resumo. *O crescimento da conectividade e do uso de serviços digitais tem gerado novas vulnerabilidades para os usuários, principalmente frente aos golpes digitais. Neste contexto, a cibersegurança surge como um campo essencial na proteção de dados e informações pessoais. A pesquisa tem como objetivo analisar o papel da cibersegurança na prevenção de golpes digitais, destacando práticas e estratégias de proteção ao usuário. Utilizou-se a metodologia qualitativa com base em revisão bibliográfica e análise documental de relatórios técnicos. Constatou-se que a prevenção eficaz requer não apenas o uso de ferramentas tecnológicas, mas também a educação digital dos usuários no ambiente virtual.*

1. Introdução

Nas últimas décadas, o uso da *internet* e das tecnologias digitais se tornou parte essencial da vida cotidiana, cujo impacto atinge desde a comunicação interpessoal até como se realizam transações financeiras, compras, estudos e acesso a serviços públicos. Tais transformações digitais trouxeram inúmeros benefícios, mas também abriram espaço para novas formas de criminalidade, especialmente os golpes digitais.

As fraudes, geralmente, estão baseadas na manipulação de usuários ou em falhas na proteção de sistemas, têm causado prejuízos financeiros, vazamento de dados e danos

à reputação de indivíduos e organizações. No Brasil, a ocorrência de crimes virtuais tem crescido de forma alarmante. Segundo dados da Federação Brasileira de Bancos (Febraban, 2023, p. *online*), os casos de fraudes eletrônicas aumentaram mais de 70% nos últimos anos.

Neste sentido, é importante discutir e propor ferramentas de prevenção e de educação digital para diversos usos, como: compras *online*, redes sociais, entre outros. Os ataques mais comuns envolvem táticas de *phishing, smishing*, engenharia social e, recentemente, golpes vinculados ao uso indevido de inteligência artificial e *deepfakes*.

A pesquisa tem como objetivo geral analisar a importância da cibersegurança na prevenção de golpes digitais e a atuação na proteção do usuário. Delinearam-se, também, como objetivos específicos: 1. Abordar os principais tipos de golpes digitais e 2. Avaliar políticas e ações educativas sobre o tema como pilar estratégico na luta contra os crimes cibernéticos. Para isso, usou-se da metodologia de pesquisa bibliográfica e documental, de natureza qualitativa e caráter descritivo.

Assim, discutir a prevenção de golpes digitais requer uma abordagem multidisciplinar que considere aspectos técnicos, sociais, educacionais e comportamentais. A proteção do usuário não depende apenas das instituições e da legislação, mas também da própria capacidade de reconhecer ameaças, adotar boas práticas e tomar decisões seguras no ambiente *online*.

2. O Papel da Cibersegurança na Proteção do Usuário

O Direito Digital é fruto da evolução social e das mudanças ocorridas na sociedade com o surgimento da internet e também do próprio Direito (Vieira, 2018). E parte dos crimes digitais estão tipificados no Código Penal Brasileiro (CPB), ainda que cometidos por mecanismos tradicionais ou por meio da *internet*.

A cibersegurança, entendida como o conjunto de práticas, políticas e tecnologias voltadas para a proteção de sistemas, redes e dados digitais, tornou-se um elemento indispensável na era da informação. Com o aumento da conectividade e da digitalização de serviços, proteger o usuário final contra ameaças virtuais passou a ser um dos maiores desafios da sociedade contemporânea.

A função da cibersegurança vai além da simples implementação de soluções técnicas, como antivírus ou *firewalls*. O papel estratégico da cibersegurança envolve a criação de um ecossistema seguro, que considera desde a arquitetura de sistemas até o comportamento dos usuários.

De acordo com Stallings (2018), a segurança eficaz deve atender a quatro pilares fundamentais: confidencialidade, integridade, disponibilidade e autenticidade das informações. Quando esses princípios são comprometidos, os riscos à privacidade, à segurança financeira e à confiança digital se intensificam.

Nesse sentido, a cibersegurança compreende um conjunto de medidas que buscam proteger sistemas, redes e dados contra-ataques, danos ou acessos não autorizados (Stallings, 2018). Os golpes digitais mais comuns incluem: a) *Phishing*: uso de mensagens falsas para obter dados pessoais; b) *Ransomware*: sequestro de dados mediante criptografia e pedido de resgate; c) Engenharia social: manipulação do

comportamento humano para enganar vítimas; d) *Smishing* e *Vishing*: variantes do phishing por SMS (mensagens de texto) e ligações telefônicas.

Explica Silva (2021), que a falta de educação digital é um fator crítico para a disseminação de golpes, ferramentas como autenticação multifator, atualização constante de sistemas e uso de senhas fortes são práticas essenciais. Porém, a vulnerabilidade do usuário, especialmente diante de golpes digitais, como: *phishing, ransomware*, *spoofing* e fraudes via redes sociais, é amplamente explorada por cibercriminosos que se aproveitam de técnicas de engenharia social.

O papel da cibersegurança é promover a cultura da segurança digital. Isso inclui orientar usuários sobre a criação de senhas fortes, identificação de links maliciosos, verificação de autenticidade de comunicações e uso de autenticação multifator. E, também, desenvolver sistemas mais intuitivos e seguros, que minimizem o impacto de erros humanos.

Os ataques exploram falhas humanas — curiosidade, distração ou desconhecimento — para obter acesso a dados sensíveis. Assim, a proteção eficaz depende não apenas de ferramentas automatizadas, mas da consciência crítica e da educação digital do usuário (Silva, 2021).

De acordo com Souza (2024), a "cibersegurança surge como uma necessidade crítica para garantir a integridade, a confidencialidade e a disponibilidade das informações. " Parte dos ataques cibernéticos envolve certo grau de erro humano, e Souza (2024) afirma que a tecnologia intrinsecamente não é suficiente para garantir a segurança.

Além disso, a proteção ao usuário requer ações coordenadas entre setor público, empresas privadas e sociedade civil. Os Estados devem investir em políticas públicas de segurança da informação, promover legislações atualizadas — como o Marco Civil da Internet - MCI (Lei n° 12.965/2014) e a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) no Brasil — e criar canais de denúncia acessíveis. As empresas, por sua vez, precisam garantir que os sistemas estejam protegidos e que seus clientes sejam educados sobre como se proteger no ambiente digital.

Com isso, é necessário compreender que a cibersegurança não é uma solução pontual, mas um processo contínuo de adaptação, resposta e resiliência frente às ameaças em constante evolução. O usuário precisa ser visto como parte ativa da estratégia de proteção, e não apenas como um agente passivo que deve ser defendido. Empoderá-lo com informação, ferramentas e autonomia é um dos maiores desafios — e também uma das maiores responsabilidades — da cibersegurança contemporânea.

3. Incidentes de Segurança Digital- Infrações no ciberespaço

Com o crescimento exponencial da digitalização de serviços, o número de incidentes de segurança digital tem se multiplicado, afetando indivíduos, empresas e governos. Estes incidentes, também conhecidos como infrações no ciberespaço, referem-se a qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade das informações e dos sistemas computacionais (Stallings, 2018).

Entre os tipos mais comuns de infrações estão os acessos não autorizados a sistemas, roubo de dados pessoais, vazamentos de senhas, ataques de negação de serviço

(DDoS) e *ransomware*. Em muitos casos, as ações têm motivação financeira, mas também podem estar ligadas ao ativismo digital, espionagem corporativa ou sabotagem (Franco; Araújo, 2023).

A segurança digital tornou-se um desafio com o aumento dos crimes cibernéticos, e o direito eletrônico desempenha papel essencial na proteção dos direitos no espaço virtual, com a necessária proteção das informações pessoais para não ocorrer uso indevido (Franco; Araújo, 2023).

Segundo o relatório do Cert.br (2023), o país registrou mais de 900 (novecentos) mil notificações de incidentes de segurança relacionados a tentativas de invasão, fraudes por *phishing* e distribuição de códigos maliciosos. O crescimento dessas infrações revela não apenas a sofisticação dos cibercriminosos, mas também a fragilidade de muitos ambientes digitais.

Tais crimes são frequentemente facilitados por vulnerabilidades técnicas, como sistemas desatualizados, ausência de autenticação robusta e má configuração de servidores. No entanto, o fator humano continua sendo uma das principais portas de entrada para os ataques. Usuários que clicam em *links* suspeitos, fornecem dados pessoais inadvertidamente ou utilizam senhas fracas tornam-se alvos fáceis para cibercriminosos (Silva, 2021).

Os crimes cibernéticos, também conhecidos como delitos informáticos, são infrações penais praticadas por meio da internet ou de dispositivos conectados em rede, que têm como alvo dados, sistemas ou usuários digitais. Tais crimes representam ameaças à segurança digital contemporânea, atingindo desde usuários comuns até grandes corporações e governos. A sofisticação e a diversidade dos métodos utilizados tornam esses crimes difíceis de prevenir, investigar e punir.

De acordo com a Convenção de Budapeste (Decreto n° 11.491/2023) sobre o Crime Cibernético (2001), ratificada por diversos países, incluindo o Brasil, os crimes cibernéticos podem ser classificados em três categorias principais:

> Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas, como invasão de dispositivos, sequestro de dados *(ransomware*) e sabotagem digital; crimes informáticos propriamente ditos, como fraude eletrônica, clonagem de cartões, falsificação de identidade virtual e desvio de criptomoedas; crimes tradicionais adaptados ao meio digital, como calúnia, difamação, extorsão, assédio e tráfico de conteúdo ilícito por meio da internet (Brasil, 2023).

No Brasil, a legislação sobre crimes cibernéticos começou a ser sistematizada a partir da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou delitos como invasão de dispositivo informático, e da Lei do Marco Civil da Internet, que estabeleceu princípios e garantias para o uso da internet no país. Posteriormente, a Lei Geral de Proteção de Dados, reforça a responsabilidade sobre o tratamento de dados e a proteção da privacidade do cidadão digital.

Um dos desafios mais relevantes no combate aos crimes cibernéticos é sua natureza transnacional e anônima. Na maioria dos casos, os ataques são orquestrados por redes internacionais, dificultando a identificação de seus autores e a aplicação das leis locais. Além disso, a velocidade com que novas tecnologias e técnicas de ataque

surgem frequentemente supera a capacidade das instituições em se atualizar e responder com eficácia.

Segundo o Relatório de Ameaças Digitais da Norton (2023), mais de 75% dos usuários brasileiros afirmam já ter sido expostos a tentativas de fraude *online*, e estima-se que os prejuízos econômicos causados por crimes cibernéticos no Brasil ultrapassem R$ 15 bilhões ao ano. O cenário reforça a necessidade de ações preventivas, políticas públicas, cooperação internacional e educação digital para mitigar os impactos dessas infrações.

Em 2024, o Panorama de Ameaças da Kaspersky identificou mais de 3,9 milhões de tentativas de golpes móveis (celulares e tablets), em que o Brasil é um dos países mais afetados da América Latina, conjuntamente com o México, o Equador, o Chile e o Panamá. Na comparação dos dados entre 2020 e 2024 demonstrou-se um progressivo aumento de 70% de ataques virtuais, o que corresponde a 7,46 bloqueios por minuto (Kaspersky, 2024).

De acordo com a direção da Equipe Global de Pesquisa e Análise da Kaspersky, há uma importância no uso do celular na América Latina, pois constitui um papel social, em que o dispositivo móvel é o principal responsável pela inclusão digital da população para o acesso à internet, pagamentos, comunicação, informação, entre outros.

A informação acima é corroborada pelas pesquisas do Centro Regional de Estudos para o Desenvolvimento da Informação sobre o uso das Tecnologias de Informação e Comunicação (TIC) nos domicílios do Brasil (Cetic.br, 2023), em que 2022 havia 60 milhões de lares com acesso à internet.

O dispositivo mais utilizado pela população brasileira é o celular, com 99% de usuários, seguido pela televisão, com 55% (Cetic.br, 2023), o que significa um número expressivo de pessoas que acessam à internet. Logo, o espaço virtual é um espaço público em que devem ser preservados os direitos fundamentais de cada pessoa, a privacidade, a intimidade, a liberdade e os dados pessoais.

O Brasil é líder regional em inovação e desempenho na América Latina, pelo Índice e de Inovação Global (2023), e de que o país está conquistando melhorias na tecnologia e modernização. No âmbito da Administração Pública, tem-se o governo como plataforma que utiliza *software livre* para atender a população em bens e serviços (Lei n° 14.129/2021), e mais de 110 milhões de pessoas utilizam os serviços públicos por meio da plataforma “Gov.br” (Brasil, 2023).

Os crimes cibernéticos representam uma ameaça crescente à sociedade digital e exigem uma abordagem multidisciplinar que envolva direito, tecnologia, educação e políticas públicas. O enfrentamento eficaz passa pela modernização das leis, fortalecimento da infraestrutura de cibersegurança, investimentos em investigação digital e promoção de uma cultura de proteção da informação.

A legislação brasileira reconhece a gravidade das infrações digitais. Para tanto, a Lei Carolina Dieckmann tipificou crimes informáticos, porém, ainda há desafios na aplicação efetiva dessas normas e na resposta rápida às ocorrências.

Portanto, compreender os tipos de incidentes mais comuns e suas implicações é essencial para a elaboração de políticas públicas, planos corporativos de segurança da

informação e programas educativos voltados à conscientização dos usuários. A redução das infrações no ciberespaço depende tanto da adoção de soluções técnicas quanto da formação de uma cultura de segurança digital.

4. Estratégias e Medidas para Segurança Digital- Educação Digital

Em um cenário de crescente dependência tecnológica, a implementação de estratégias e medidas eficazes de segurança digital é indispensável para garantir a proteção dos dados, sistemas e usuários.

A segurança digital é um campo dinâmico, que requer abordagens integradas envolvendo aspectos técnicos, organizacionais e humanos. O objetivo é reduzir vulnerabilidades, mitigar riscos e criar ambientes virtuais resilientes frente às ameaças cibernéticas.

Além do ambiente corporativo, é responsabilidade dos governos promover legislações atualizadas, fiscalização efetiva e campanhas públicas de orientação digital. A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) é um marco importante nesse sentido, ao estabelecer padrões legais para coleta, armazenamento e tratamento de dados pessoais, impondo sanções em caso de negligência com a segurança.

Entre as principais estratégias técnicas, destacam-se: autenticação multifator (MFA): adiciona camadas de verificação para garantir que apenas usuários autorizados acessem sistemas; criptografia de dados: protege informações em trânsito e em repouso contra interceptações e acessos indevidos.

As atualizações regulares de software corrigem vulnerabilidades conhecidas e evitam a exploração por *malwares*; *firewalls* e antivírus atuam como barreiras iniciais para impedir o acesso não autorizado ou a entrada de códigos maliciosos; *backup* periódico garante a recuperação de dados em casos de ataques, como *ransomware* ou falhas técnicas.

No entanto, as medidas organizacionais e educativas são igualmente cruciais, pois, segundo Silva (2021), a maioria dos incidentes de segurança tem origem no comportamento humano, como o uso de senhas fracas, o clique em *links* suspeitos ou a negligência com atualizações. Por isso, programas de educação digital e conscientização em cibersegurança devem fazer parte da rotina institucional, com treinamentos regulares e políticas claras de uso seguro de recursos tecnológicos.

Há diferenças regionais no que diz respeito ao acesso à internet e também à educação digital para uso consciente, responsável e seguro no ciberespaço. “A ligação de computadores em rede expandiu-se com o uso de programas que viabilizaram uma teia mundial voltada para o usuário. E assim por diante” (Castells, 2002).

Há a necessidade de educação digital para manusear a tecnologia, pois parte da sociedade é vulnerável digitalmente, com agravamento para idosos, crianças e adolescentes. A vulnerabilidade digital se caracteriza no espaço tecnológico-informacional, que transpõe a vida sociocultural com diversos saberes e experiências, e não basta apenas a alfabetização, é necessário saber a utilização e exploração das tecnologias de informação (Ferreira et al., 2024).

Segundo Castells (2002), a sociedade em rede é resultante do desenvolvimento de novas tecnologias da informação e do reaparelhamento da sociedade com uso do poder da tecnologia. Os conteúdos veiculados nos meios virtuais exercem forte influência sobre os usuários, e dada a realidade de conectividade, a maior parte do tempo estão sujeitos a crimes eletrônicos.

Ainda explica Castells (2002), que uma das características do paradigma tecnológico é a "*penetrabilidade dos efeitos das novas tecnologias",* a informação é parte integrante de toda atividade humana (individual e coletiva) é moldada pelo meio tecnológico. As novas tecnologias compõem o processo de alfabetização, e com isso a necessidade de políticas públicas em letramento digital (Ferreira et al., 2024).

No cenário brasileiro, a fragilidade digital está vinculada às desigualdades socioeconômicas, que excluem parte da população (em sua maioria a periférica) do acesso à internet e às tecnologias, o que as compromete de exercerem o direito à cidadania digital. A educação digital é um caminho para mitigar a debilidade digital (Ferreira et al., 2024).

No âmbito escolar, a Base Nacional Comum Curricular - BNCC (2018) dispõe a compreensão para os termos "cultura digital" e "mundo digital":

> **Cultura digital**: envolve aprendizagens voltadas a uma participação mais consciente e democrática por meio das tecnologias digitais, o que supõe a compreensão dos impactos da revolução digital e dos avanços do mundo digital na sociedade contemporânea, a construção de uma atitude crítica, ética e responsável em relação à multiplicidade de ofertas midiáticas e digitais, aos usos possíveis das diferentes tecnologias e aos conteúdos por elas veiculados, e, também, à fluência no uso da tecnologia digital para expressão de soluções e manifestações culturais de forma contextualizada e crítica. (Destaque nosso).
>
> **Mundo digital:** envolve as aprendizagens relativas às formas de processar, transmitir e distribuir a informação de maneira segura e confiável em diferentes artefatos digitais – tanto físicos (computadores, celulares, tablets etc.) como virtuais (internet, redes sociais e nuvens de dados, entre outros) –, compreendendo a importância contemporânea de codificar, armazenar e proteger a informação. (Destaque nosso).

A juventude é um dos protagonistas da cultura digital nas formas de interação multimidiática e multimodal nas redes. Porém, há desafios a considerar na formação das novas gerações, de que no campo da escolarização haja o estímulo à reflexão crítica e aprofundada diante das ofertas das mídias digitais (BNCC, 2018), a educação digital.

O Instituto Nacional de Propriedade Industrial (INPI) está desenvolvendo um índice nacional que agrega 74 (setenta e quatro) indicadores estatísticos (Inpi, 2024), com intuito de identificar as potencialidades e os desafios de cada estado brasileiro para o campo da inovação, o que representa avanço tecnológico a agregar informações relevantes para a produção de políticas públicas digitais.

No âmbito federal, já existem diretrizes nacionais para a inclusão digital, com a Lei n° 14.533/2023, que estabelece a Política Nacional de Educação Digital, com 04 (quatro) eixos/ objetivos estruturantes, com destaque para a "educação digital escolar".

O eixo que trata da "educação digital escolar" tem por objetivo garantir a inserção da educação digital nos ambientes escolares, em todos os níveis e modalidades,

a partir do estímulo ao letramento digital e informacional e outras competências digitais (artigo 3º, da Lei n° 14.533/2023).

Os direitos digitais na acepção da referida lei, tratam da conscientização dos direitos sobre o uso e o tratamento de dados pessoais (LGPD) e da promoção da conectividade segura e da proteção dos dados da população mais vulnerável, em especial crianças e adolescentes. Logo, há uma preocupação de educar os mais jovens para os riscos da internet e também a atuação responsável na sociedade conectada e nos ambientes digitais.

Dessa forma, as estratégias para segurança digital devem ser amplas, envolvendo tecnologia, processos, legislação e, sobretudo, o fator humano. A prevenção de fraudes e invasões requer uma postura proativa e contínua, voltada à criação de uma cultura organizacional de segurança e à capacitação dos usuários frente aos riscos digitais.

5. Políticas de Inclusão Digital no Amazonas e o Panorama das Punições por Crimes Digitais no Brasil

A inclusão digital tem se consolidado como uma prioridade nas políticas públicas brasileiras, especialmente em regiões de grande extensão territorial e desafios socioeconômicos, como o Amazonas. A política nacional de inclusão digital busca promover o acesso às tecnologias de informação e comunicação (TIC), visando reduzir desigualdades sociais e promover o desenvolvimento sustentável (Brasil, 2014).

No contexto do Amazonas, diversas iniciativas têm sido implementadas para ampliar o acesso à internet e às ferramentas digitais, reconhecendo a importância de conectar comunidades ribeirinhas e rurais às oportunidades do mundo digital (Seplan-Am, 2020; Silva, 2019).

No ano de 2023, foi instituída a lei estadual de inclusão digital em áreas rurais do Estado do Amazonas (Lei nº 6.593/2023), com intuito de almejar dentre os objetivos, o combate ao analfabetismo tecnológico e a redução da desigualdade digital. As características físicas e geográficas representam um desafio à região, cumuladas com outros problemas historicamente visíveis, como: precariedade no saneamento básico, acesso à água, energia, educação, etc.

No âmbito legislativo brasileiro, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no país, sendo uma peça fundamental na regulamentação do ambiente digital (Brasil, 2014). Ademais, o Código Penal Brasileiro prevê punições específicas para crimes cibernéticos, como invasão de dispositivos, difamação, ameaça e crimes contra a honra, com penas que variam de meses a anos de prisão, dependendo da gravidade do delito (Brasil, 1940).

De acordo com o Ministério da Justiça, o número de punições por crimes digitais tem crescido nos últimos anos, refletindo tanto o aumento na incidência desses delitos quanto a maior capacidade de investigação e repressão por parte das autoridades (Ministério da Justiça, 2023; Oliveira, 2022).

Em 2022, foram registrados aproximadamente 15.000 (quinze mil) casos de crimes cibernéticos, incluindo invasões de sistemas, fraudes e crimes contra a honra na internet (Ministério da Justiça, 2023). Essa crescente incidência evidencia a necessidade de uma legislação robusta e de ações educativas para prevenir e combater tais delitos.

As ferramentas como o *phishing*, plataforma de monitoramento de crimes digitais, têm contribuído para a análise e o combate às infrações na rede, fornecendo dados importantes para a formulação de políticas públicas mais eficazes (Silva et al., 2021; Pereira, 2020).

A legislação brasileira evoluiu para acompanhar as novas formas de criminalidade digital, com leis específicas como a Lei Carolina Dieckmann, que criminaliza a invasão de dispositivos eletrônicos (Brasil, 2012), e a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que regula o uso de dados pessoais, reforçando a proteção do cidadão na era digital (Brasil, 2018).

As legislações representam avanços importantes na proteção do ambiente digital e na punição de delitos cibernéticos (Santos, 2020). No âmbito acadêmico, autores como Almeida (2018) destacam a importância de políticas públicas integradas que combinem infraestrutura, educação digital e legislação para promover uma inclusão digital efetiva. Já Costa (2019) enfatiza que o fortalecimento das punições e a conscientização da sociedade são essenciais para criar um ambiente digital mais seguro.

Enfim, a política de inclusão digital no Amazonas é uma estratégia fundamental para promover a inclusão social e o desenvolvimento regional, enquanto o fortalecimento da legislação e das punições por crimes digitais no Brasil é essencial para garantir a segurança dos usuários e a integridade do ambiente digital. A combinação de ações educativas, tecnológicas e jurídicas constitui o caminho para construir uma sociedade digital mais justa, segura e acessível a todos.

6. Considerações Finais

Em um mundo mais interconectado, a proteção do dado é essencial para a privacidade dos usuários, e a cibersegurança constitui um direito digital fundamental individual e coletivo, não apenas com campo técnico, sobretudo é matéria estratégica e humana.

A cibersegurança é mais do que o uso de antivírus e senhas complexas, a cibersegurança envolve práticas, políticas e tecnologias voltadas para garantir a confidencialidade, integridade e disponibilidade das informações no ambiente digital, e a apesar dos avanços tecnológicos, o fator humano continua sendo o elo mais frágil da cadeia de segurança, principalmente pela falta de conhecimento, atenção ou preparo para lidar com os riscos virtuais.

Das informações consultadas, os dados consultados e analisados apontam o *phishing* como o golpe digital mais recorrente no Brasil, em que este tipo de ataque cresce em épocas de crise e datas comemorativas, aproveitando-se da desatenção dos usuários.

A maioria dos usuários desconhece práticas básicas de segurança, como a verificação da autenticidade de links. Apesar dos avanços tecnológicos, a educação digital continua sendo um dos pilares mais eficazes na prevenção.

Iniciativas de bancos e empresas de tecnologia têm se concentrado na proteção de sistemas, mas não investem proporcionalmente na capacitação de seus usuários. Campanhas governamentais são esporádicas e geralmente reativas, não havendo um plano nacional de educação em cibersegurança contínuo.

A cibersegurança desempenha um papel essencial na mitigação dos riscos associados aos golpes digitais. No entanto, os esforços técnicos devem ser complementados com educação digital acessível e contínua. É fundamental que usuários sejam capacitados para reconhecer e evitar ameaças, além de adotar comportamentos seguros online.

Sugere-se o fortalecimento das políticas públicas voltadas para a formação de uma cultura de segurança digital, abrangendo escolas, universidades, empresas e serviços públicos. A prevenção deve ser compreendida como um processo integrado entre tecnologia, informação e comportamento.

7. Referências

Almeida, J. (2018). Políticas públicas de inclusão digital no Brasil: desafios e perspectivas. *Revista Brasileira de Políticas Públicas*, v. 12, n. 3, p. 45-62.

Base Nacional Comum Curricular. (BNCC). (2018). *Base Nacional Comum Curricular Educação é a base*. Brasília, Ministério da Educação. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf.

Brasil. (2023). *Governo Digital, mais de 110 milhões de brasileiros já utilizaram o Gov.br em 2023*. Brasília: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em:https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/outubro/mais-de-110-milhoes-de-brasileiros-ja-utilizaram-o-gov-br-em-2023.

Castells, M. (2002). *A Sociedade em Rede*. Vol. 1. 6ª ed. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra.

Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Decreto n° 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro 2001. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (Cert.br). (2023). *Relatório de Atividades 2023*. Disponível em: https://www.cert.br.

Cetic. br. (2023). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: *TIC Domicílios 2022 [livro eletrônico]*. Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: Comitê Gestor da Internet no Brasil. Disponível em: https://cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf.

Ferreira, K. et al. (2024). Vulnerabilidade Sócio Digital em Questão: Uma experiência em inclusão e letramento digital na comunidade e na Universidade. v. 9 n. 1 (2024). *Anais da Jornada Científica e de Extensão (JCE 2024)*. Disponível em: https://www.upecaruaru.com.br/index.php/jce/article/view/93.

Federação Brasileira de Bancos. (FEBRABAN) (2023). *Relatórios de Fraudes e Segurança Digital 2023*. São Paulo, 2023. Disponível em: https://www.febraban.org.br.

Franco dos Santos, J. V.; Araújo, A. C. (2023). Cibersegurança e a Importância do Direito Digital. *Revista Multidisciplinar do Nordeste Mineiro*, 12(1). Disponível em: https://doi.org/10.61164/rmnm.v12i1.1738.

Índice de Inovação Global. (2023). *GII 2023 at a glance The Global Innovation Index 2023 captures the innovation ecosystem performance of 132 economies and tracks the most recent global innovation trends*. Disponível em:

https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-section1-en-gii-2023-at-a-glance-global-innovation-index-2023.pdf.

Inpi. Instituto Nacional da Propriedade Industrial. (2024). Presidência. Diretoria Executiva. Assessoria de Assuntos Econômicos (AECON). Índice Brasil de Inovação e Desenvolvimento: *IBID: 2024. 1ª edição*. / Rodrigo Ventura [et al.]. Rio de Janeiro: INPI. Disponível em: https://www.gov.br/inpi/pt-br/inpi-data/estudos/indice-brasil-de-inovacao-e-desenvolvimento-ibid/IBID_2024_PT.BRfinal.pdf/.

Kaspersky. (2024). *Panorama de Ameaças Cibernéticas no Brasil em 2024*. Disponível em: https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2024/22888/.

Lei nº 12.737, de 2 de dezembro de 2012. Lei Carolina Dieckmann. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Lei n° 14. 129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm.

Lei n° 14. 533, de 11 de janeiro de 2023. Institui a Política Nacional de Educação Digital e altera as Leis n°s 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), 9.448, de 14 de março de 199, 10.260, de 12 de julho de 2001, e 10.753, de 30 de outubro de 2003. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm.

Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br.

Lei nº 6.593, de 27 de novembro de 2023. Dispõe sobre diretrizes para ações de Incentivo à Inclusão Digital e Tecnológica em Áreas Rurais, visando promover a erradicação do analfabetismo digital, no âmbito do Estado do Amazonas. Manaus, AM, Assembleia Legislativa do Estado Amazonas. Disponível em: https://sapl.al.am.leg.br/media/sapl/public/normajuridica/2023/12846/6593.pdf.

Ministério da Justiça. (2022). *Relatório de Crimes Cibernéticos no Brasil*. Brasília: Ministério da Justiça, 2022.

Norton. (2023). *Relatório de Ameaças Cibernéticas 2023 – Brasil*. Disponível em: https://us.norton.com/blog/emerging-threats/pulse-report-september-2023.

Oliveira, L. (2022). Crimes digitais no Brasil: análise das punições e desafios. *Revista de Direito Digital*, v. 5, n. 2, p. 89-105.

Pereira, A. (2020). Ferramentas de monitoramento de crimes cibernéticos: o caso do Phichig. *Revista de Segurança Digital*, v. 7, n. 1, p. 23-37.

Santos, M. (2020). Legislação e proteção de dados na era digital. *Revista Jurídica Digital*, v. 4, n. 4, p. 112-130.

Secretaria de Planejamento do Amazonas. (SEPLAN-AM). (2020). *Iniciativas de inclusão digital no Amazonas.* Manaus, 2020.

Silva, A. (2019). Inclusão digital no Amazonas: avanços e desafios. *Revista de Políticas Públicas Regionais*, v. 15, n. 1, p. 78-92.

Silva, J. L. da. Educação digital como estratégia de combate à desinformação e fraudes. (2021). *Revista Brasileira de Educação Tecnológica*, Curitiba, v. 14, n. 2, p. 115-127, 2021.

Silva, P. et al. (2021). Monitoramento de crimes digitais e políticas públicas. *Revista de Tecnologia e Sociedade*, v. 9, n. 2, p. 55-70.

Souza, L. P. de. (2024). O papel da cibersegurança na era digital: desafios, tendências e soluções globais: The role of cybersecurity in the digital age: global challenges, trends and solutions. RCMOS - *Revista Científica Multidisciplinar O Saber*, 1(2). Disponível em: https://doi.org/10.51473/rcmos.v1i1.2025.1036.

Stallings, W. (2018). *Segurança de Redes: Princípios e Práticas*. 7. ed. São Paulo: Pearson.

Viera, A. P. (2018). *Direito autoral na Sociedade Digital*. 2ª ed. São Paulo: Montecristo Editora.