REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

CRIMES CIBERNÉTICOS NA PREVIDÊNCIA SOCIAL – INSS

Tamires do Nascimento Sá
https://orcid.org/0009-0001-3065-000X
E-mail: tamiresdonascimentosa@gmail.com

DOI-Geral: http://dx.doi.org/10.47538/RA-2026.V5N2
DOI-Individual: http://dx.doi.org/10.47538/RA-2026.V5N2-43

RESUMO: O presente artigo analisa os crimes cibernéticos na Previdência Social, com foco no Instituto Nacional do Seguro Social (INSS), identificando os principais métodos utilizados por criminosos digitais, como roubo de identidade, phishing, falsificação de documentos e ataques a sistemas informatizados. A pesquisa destaca os impactos econômicos e sociais dessas fraudes, evidenciando prejuízos ao erário e à confiança dos beneficiários, além de riscos à integridade dos dados pessoais e à sustentabilidade do sistema previdenciário. São discutidas medidas de prevenção e proteção digital, incluindo o uso de inteligência artificial, autenticação multifatorial, auditorias, monitoramento contínuo e capacitação de servidores, reforçando a necessidade de políticas públicas voltadas à segurança cibernética. O estudo contribui para o entendimento dos desafios enfrentados pelo INSS frente à digitalização dos serviços e à sofisticação crescente das fraudes, propondo estratégias para mitigação dos crimes cibernéticos e proteção de dados.
PALAVRAS-CHAVE: Crimes Cibernéticos. INSS. Segurança Digital. Fraudes Previdenciárias. Proteção de Dados.

CYBER CRIMES IN SOCIAL SECURITY – INSS

ABSTRACT: This article examines cybercrimes affecting the Brazilian Social Security system, focusing on the National Institute of Social Security (INSS). It identifies the main methods used by digital criminals, including identity theft, phishing, document forgery, and attacks on computerized systems. The study highlights the economic and social impacts of these frauds, showing financial losses, reduced trust from beneficiaries, risks to personal data, and threats to the sustainability of the social security system. Prevention and digital protection measures, such as artificial intelligence, multi-factor authentication, auditing, continuous monitoring, and staff training, are discussed, emphasizing the need for public policies aimed at cybersecurity. The research contributes to understanding the challenges faced by the INSS amidst service digitalization and increasingly sophisticated frauds, proposing strategies for mitigating cybercrimes and safeguarding data.

KEYWORDS: Cybercrime. INSS. Digital Security. Social Security Fraud. Data Protection.

INTRODUÇÃO

A transformação digital tem modificado significativamente a forma como os serviços públicos são oferecidos, trazendo eficiência e acessibilidade, mas também expondo vulnerabilidades que podem ser exploradas por agentes mal-intencionados

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

(Silva Júnior; Pimenta Júnior, 2007; Schall, 2010). No âmbito da Previdência Social, essas mudanças permitiram a digitalização de processos e o acesso remoto a informações sensíveis, mas aumentaram a exposição a crimes cibernéticos, como fraudes em benefícios, invasão de sistemas e roubo de identidade (Filatoff, 2019; Santos; Bizzo, 2009). Tais práticas ilícitas comprometem tanto a integridade dos recursos públicos quanto a segurança das informações pessoais dos beneficiários, tornando necessário analisar o fenômeno de forma detalhada.

O INSS, responsável pela gestão de benefícios previdenciários, enfrenta desafios crescentes diante do uso da tecnologia por criminosos digitais. Phishing, malware, ransomwares e engenharia social são algumas das técnicas mais comuns utilizadas para obtenção indevida de benefícios e manipulação de dados (Silva Júnior; Pimenta Júnior, 2007; Schall, 2010). Além disso, a expansão de plataformas digitais e aplicativos voltados ao atendimento dos segurados, embora facilite o acesso, também abre portas para ataques sofisticados, exigindo políticas de segurança cada vez mais robustas e a conscientização dos usuários.

O contexto atual da sociedade brasileira evidencia que a digitalização do setor previdenciário ocorre em paralelo ao aumento da criminalidade digital, impactando diretamente a sustentabilidade financeira do sistema e a confiança dos cidadãos (Filatoff, 2019; Santos; Bizzo, 2009). Beneficiários idosos e grupos vulneráveis são especialmente afetados, já que possuem menor familiaridade com práticas de segurança digital, tornando-os alvos frequentes de golpes e fraudes. Esses elementos reforçam a necessidade de estudos que abordem a prevenção, detecção e mitigação dos crimes cibernéticos dentro do INSS.

A evolução das tecnologias digitais e a complexidade das fraudes exigem uma análise crítica da legislação vigente, dos mecanismos de proteção existentes e da capacidade do sistema em reagir a ataques cibernéticos (Silva Júnior; Pimenta Júnior, 2007; Schall, 2010). Apesar dos avanços promovidos pelo INSS, como autenticação multifatorial e monitoramento de acessos, ainda existem lacunas que permitem a ocorrência de fraudes e desvios de recursos, evidenciando que a proteção digital é um processo contínuo e dinâmico.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

A relevância deste estudo reside na necessidade de compreender como os crimes cibernéticos impactam o INSS, tanto em termos econômicos quanto sociais, bem como identificar práticas que aumentem a segurança dos beneficiários. Considerando os desafios enfrentados pelo sistema previdenciário e a sofisticação dos ataques digitais, como garantir a integridade dos dados e a confiabilidade dos serviços prestados?

O objetivo geral deste artigo é analisar os crimes cibernéticos na Previdência Social, destacando seus impactos para o INSS e seus beneficiários, e propor estratégias de prevenção e segurança digital. Especificamente, busca-se mapear as vulnerabilidades existentes, os métodos de fraude mais utilizados e as medidas tecnológicas e administrativas que podem mitigar riscos.

A metodologia utilizada consiste em pesquisa bibliográfica, abrangendo livros, artigos científicos, relatórios oficiais e legislações pertinentes, priorizando estudos publicados nos últimos dez anos. Foram aplicados critérios de inclusão, contemplando materiais que abordam especificamente crimes digitais no INSS, e critérios de exclusão, descartando textos genéricos sobre cibercrime sem relação direta com a Previdência Social. A abordagem adotada permite uma compreensão aprofundada do tema e sustenta a proposição de medidas de proteção eficientes.

REFERENCIAL TEÓRICO

CRIMES CIBERNÉTICOS NO INSS

Os crimes cibernéticos passaram a ocupar espaço relevante nas discussões jurídicas e administrativas em razão da ampliação do uso de tecnologias digitais nos serviços públicos. No caso do Instituto Nacional do Seguro Social, essa realidade ganha maior gravidade porque o órgão trabalha diariamente com grande volume de dados pessoais, financeiros e previdenciários de segurados, aposentados, pensionistas e demais beneficiários. Lopes e Lopes (2023) explicam que os crimes virtuais se relacionam ao uso indevido de sistemas informatizados para a prática de condutas ilícitas, enquanto Oliveira (2023) ressalta que o ambiente digital exige nova compreensão dos direitos fundamentais, especialmente quando envolve privacidade, segurança e proteção de dados. No INSS, tais condutas não se limitam ao acesso indevido a informações, pois também alcançam

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

fraudes em benefícios, manipulação cadastral, falsificação documental, golpes contra idosos e obtenção indevida de valores públicos.

A digitalização dos serviços previdenciários representou avanço importante para a administração pública, sobretudo por facilitar o atendimento remoto e reduzir deslocamentos dos segurados. Entretanto, essa modernização também expôs novas fragilidades, pois criminosos passaram a explorar falhas tecnológicas e comportamentais para alcançar vantagens ilícitas. Naspolini e Cestari (2022) observam que a sociedade da informação alterou profundamente a atuação do Estado e do Direito, exigindo respostas mais rápidas diante de conflitos surgidos no meio digital. No mesmo sentido, Laudon e Laudon (2022) destacam que os sistemas de informação, embora essenciais para a gestão moderna, dependem de controle, segurança e monitoramento contínuo. Assim, o INSS precisa conciliar acessibilidade digital com mecanismos capazes de impedir que dados sensíveis sejam usados por terceiros de maneira fraudulenta.

Entre as práticas mais frequentes contra o sistema previdenciário, destaca-se o roubo de identidade, modalidade em que dados pessoais de segurados são utilizados para solicitar benefícios, alterar informações bancárias ou acessar plataformas oficiais. Silva e Oliveira (2024) chamam atenção para a vulnerabilidade dos idosos diante dos crimes cibernéticos, pois esse público costuma ser alvo preferencial de golpes digitais, ligações falsas, mensagens enganosas e promessas de liberação de valores. Bonini et al. (2021) também apontam que a proteção financeira das pessoas idosas deve ser observada à luz da Lei Geral de Proteção de Dados, uma vez que o uso indevido de informações pessoais pode gerar danos patrimoniais e emocionais. No contexto do INSS, a fraude não atinge apenas o sistema público, mas também interfere diretamente na vida de pessoas que dependem do benefício para sua subsistência.

No phishing o criminoso simula uma comunicação oficial por e-mail, mensagem de texto, aplicativo ou ligação telefônica, com a finalidade de convencer a vítima a fornecer CPF, senha, dados bancários ou informações de acesso. Costa e Abrantes (2023) relacionam o crescimento do estelionato digital ao aumento do uso de meios eletrônicos, especialmente em períodos de maior dependência de serviços remotos. Silva e Rezende (2024) explicam que a internet ampliou as formas de violação de direitos, pois conteúdos, imagens, dados e informações pessoais podem ser usados de maneira ilícita em diferentes

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

contextos. No caso previdenciário, o phishing permite que fraudadores acessem contas vinculadas ao segurado, modifiquem cadastros ou obtenham empréstimos e benefícios sem autorização.

O uso de malwares, spywares e outros programas maliciosos capazes de capturar informações digitadas, monitorar dispositivos ou permitir acesso remoto a sistemas. Malheiro (2020) observa que os cibercrimes exigem novas formas de enfrentamento jurídico e social, pois o criminoso digital pode agir de modo oculto, rápido e muitas vezes distante da vítima. Mello (2021) acrescenta que a cibersegurança precisa ser compreendida como prática permanente de gestão, especialmente em instituições que lidam com acervos de informações sensíveis. No INSS, essas ferramentas podem ser usadas para capturar senhas, acessar dados previdenciários, modificar informações de pagamento ou interferir em processos administrativos. Esse cenário demonstra que a segurança digital não depende apenas de sistemas fortes, mas também da prevenção de condutas que facilitem a entrada de agentes mal-intencionados.

Documentos como laudos médicos, comprovantes de vínculo, certidões, procurações e registros de contribuição podem ser adulterados para simular o preenchimento de requisitos legais. Siqueira (2023) aponta que a perícia digital possui papel relevante na apuração de crimes praticados em ambientes virtuais, pois permite identificar rastros, alterações e evidências eletrônicas. Pereira e Carvalho (2023) reforçam que a investigação de crimes complexos depende de métodos técnicos, análise de dados e atuação especializada das autoridades. No INSS, a falsificação documental pode gerar concessões indevidas de aposentadorias, pensões, auxílios e benefícios assistenciais, causando prejuízo ao erário e sobrecarga aos mecanismos de controle.

Essa prática pode ocorrer por meio de acessos indevidos, uso de credenciais comprometidas ou inserção de informações falsas em cadastros. Fernandes (2021) destaca que tecnologias como blockchain têm sido discutidas na administração pública justamente pela necessidade de proteger informações e evitar adulterações. Balbino e Silva (2024) ressaltam que o tratamento de dados sensíveis pela administração pública exige procedimentos adequados, pois falhas de gestão podem ampliar riscos ao cidadão. No INSS, a manipulação de dados pode alterar vínculos, tempo de contribuição, condição

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

de dependente, informações bancárias ou situação de benefícios, produzindo efeitos graves tanto para a instituição quanto para o segurado legítimo.

Em muitos casos, não se trata de condutas isoladas, mas de esquemas que envolvem coleta ilegal de dados, falsificação de documentos, abertura de contas bancárias e uso de tecnologia para dificultar a identificação dos responsáveis. Rosa (2023) afirma que os crimes digitais desafiam a atuação tradicional do Direito, pois exigem integração entre conhecimento jurídico e domínio técnico. Wendt e Wendt (2022) defendem que a atividade policial precisa estar preparada para lidar com problemas contemporâneos, nos quais a prova e a autoria podem estar dispersas em ambientes digitais. No âmbito do INSS, a organização dessas fraudes demonstra que o combate ao crime cibernético deve envolver prevenção, investigação, cooperação institucional e atualização constante dos instrumentos de controle.

Os golpes direcionados a aposentados e pensionistas merecem atenção especial, pois exploram não apenas vulnerabilidades tecnológicas, mas também relações de confiança. Criminosos costumam se apresentar como servidores, representantes de bancos, advogados ou intermediários de benefícios, criando situações de urgência para convencer a vítima a fornecer dados. Coutinho e Domingues (2023) analisam como a exclusão digital dos idosos dificulta o acesso seguro a serviços e amplia a exposição a práticas abusivas. Bonini et al. (2021) reforçam que a proteção financeira desse grupo deve ser tratada com prioridade, já que muitos aposentados dependem exclusivamente da renda previdenciária. Assim, os crimes cibernéticos no INSS possuem dimensão social relevante, pois atingem pessoas em situação de maior dependência econômica e menor familiaridade com tecnologias digitais.

A Lei Geral de Proteção de Dados também se relaciona diretamente com o tema, pois o INSS realiza tratamento constante de informações pessoais e sensíveis. Pereira e Stakoviak (2022) explicam que a LGPD impõe obrigações quanto à finalidade, necessidade, transparência, segurança e responsabilização no tratamento de dados. Sousa et al. (2024) destacam que a proteção de dados exige adequação institucional, principalmente em setores que lidam com informações de natureza sensível. No campo previdenciário, dados sobre renda, saúde, idade, dependência econômica e histórico

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

contributivo precisam ser preservados com rigor, pois sua exposição pode facilitar fraudes, discriminações, golpes financeiros e violações à privacidade dos segurados.

A legislação penal brasileira passou por alterações para alcançar condutas cometidas por meio eletrônico, especialmente com o fortalecimento da punição para fraudes digitais. Avanço (s.d.) observa que os crimes cibernéticos exigem análise jurídica específica, uma vez que o meio digital modifica a forma de execução do delito. Moreira e Pereira (2023) discutem a necessidade de compatibilizar respostas penais com a proteção de grupos vulneráveis diante de crimes praticados em ambiente virtual. No caso do INSS, essa discussão é essencial porque muitas fraudes combinam estelionato, falsidade documental, invasão de dispositivo, uso indevido de dados e organização criminosa. A resposta jurídica, portanto, precisa considerar a complexidade dos atos e os danos produzidos contra o Estado e contra os beneficiários.

Bergamin (2023) observa que a inteligência artificial tem provocado transformações importantes nas relações sociais e institucionais, inclusive na forma como atividades são monitoradas e executadas. Laudon e Laudon (2022) ressaltam que sistemas bem estruturados permitem identificar padrões, cruzar informações e detectar inconsistências. No INSS, recursos como análise automatizada, autenticação em múltiplos fatores, biometria, cruzamento de bases de dados e monitoramento de acessos podem reduzir a incidência de fraudes. Contudo, tais ferramentas precisam ser aplicadas com responsabilidade, transparência e respeito à proteção de dados, para que a prevenção não resulte em violação de direitos.

Figueiredo et al. (2021) defendem que o uso da tecnologia precisa estar associado à responsabilidade ética, jurídica e educacional. Rossetti e Silva (2021) também indicam que a educação digital contribui para o enfrentamento de práticas danosas no ambiente virtual. Dessa forma, o combate às fraudes previdenciárias não depende apenas de sistemas técnicos, mas também de orientação aos usuários, capacitação de servidores e comunicação clara sobre canais oficiais. Quanto mais informados estiverem os segurados, menor será a chance de caírem em golpes que simulam procedimentos do INSS.

Balbino e Santos (2024) demonstram que as redes digitais podem facilitar práticas ilícitas quando não há controle adequado, enquanto Fernandes (2021) ressalta a importância de mecanismos tecnológicos voltados à proteção das informações públicas.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

No ambiente previdenciário, servidores precisam reconhecer tentativas de engenharia social, proteger credenciais, evitar compartilhamento indevido de informações e seguir protocolos de acesso. Ao mesmo tempo, a administração pública deve investir em auditorias, atualização de sistemas, resposta rápida a incidentes e canais seguros de denúncia. Essas medidas fortalecem a integridade dos serviços e reduzem a possibilidade de exploração criminosa.

IMPACTOS PARA O ESTADO E PARA OS SEGURADOS

Os crimes cibernéticos no âmbito da Previdência Social exercem efeitos diretos e indiretos sobre a gestão pública e sobre os beneficiários do INSS. O desvio de recursos, resultante de fraudes e manipulação de dados, gera prejuízos financeiros significativos ao erário, reduzindo a capacidade de investimento em políticas sociais e comprometendo a sustentabilidade do sistema previdenciário (Silva; Oliveira, 2024; Bonini et al., 2021). Esses prejuízos não se limitam a valores monetários, pois afetam a distribuição de benefícios legítimos e podem aumentar a desigualdade social ao desviar recursos de pessoas vulneráveis.

Sousa et al. (2024) destacam que a insegurança no tratamento de informações sensíveis afeta diretamente a percepção de credibilidade da instituição, enquanto Figueiredo et al. (2021) reforçam que a proteção digital é essencial para a manutenção da legitimidade e da confiança social. Segurados cujos dados foram comprometidos enfrentam dificuldades para comprovar elegibilidade, corrigir cadastros ou contestar pagamentos irregulares, o que gera transtornos financeiros, administrativos e emocionais.

Os impactos financeiros se manifestam também em custos indiretos, como investimentos em auditorias, monitoramento de sistemas, recuperação de informações e capacitação de servidores (Balbino; Silva, 2024; Pereira; Carvalho, 2023). Tais recursos, que poderiam ser aplicados na ampliação de benefícios ou na melhoria do atendimento, passam a ser destinados à mitigação de fraudes, refletindo diretamente na eficiência administrativa do INSS. Essa necessidade de alocação extra de recursos cria uma pressão sobre o orçamento público, potencializando riscos de descontinuidade de programas sociais ou ajuste em alíquotas previdenciárias.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

Costa e Abrantes (2023) explicam que idosos e pessoas em situação de vulnerabilidade são frequentemente alvos de golpes que exploram sua confiança e desconhecimento tecnológico. Bonini et al. (2021) ressaltam que essa população enfrenta maior dificuldade para se proteger, o que aumenta a exposição a fraudes, atrasos nos pagamentos e prejuízos patrimoniais. A sensação de insegurança, além de comprometer o acesso a benefícios, gera estresse psicológico e desconfiança no sistema.

A manipulação de dados cadastrais e a criação de perfis fictícios comprometem a integridade do sistema previdenciário, levando a situações em que benefícios são concedidos a pessoas inexistentes ou cujas informações foram alteradas indevidamente (Silva; Rezende, 2024; Lopes; Lopes, 2023). Tais práticas não apenas sobrecarregam a gestão administrativa, mas também aumentam o risco de decisões equivocadas em processos de concessão, revisão ou cancelamento de benefícios. A consequência é um aumento na burocracia e no tempo de resposta aos segurados legítimos.

O impacto social dessas fraudes é evidenciado pela redução da confiança no Estado e pelo aumento da sensação de vulnerabilidade entre os cidadãos (Alcântara; Cruz, 2024; Bergamin, 2023). Beneficiários que já dependem da Previdência Social para sua subsistência podem sofrer atrasos críticos em pagamentos ou enfrentar dificuldades para acessar recursos essenciais. Além disso, golpes direcionados a aposentados, como empréstimos consignados irregulares ou solicitações fraudulentas de prova de vida, revelam a complexidade do problema, pois combinam vulnerabilidades tecnológicas, comportamentais e sociais.

Silva e Oliveira (2024) destacam que, quanto mais sofisticadas as técnicas de ataque, maior a necessidade de monitoramento contínuo e de implementação de mecanismos preventivos. Almeida et al. (2023) ressaltam que a segurança cibernética deve ser abordada de forma integrada, contemplando infraestrutura tecnológica, legislação, processos internos e educação dos usuários. O impacto sobre o Estado e sobre os segurados não se limita a prejuízos imediatos, mas se estende a longo prazo, afetando a confiabilidade, eficiência e sustentabilidade do sistema previdenciário.

Pereira e Stakoviak (2022) indicam que a aplicação da Lei Geral de Proteção de Dados, combinada com medidas penais e civis, contribui para a mitigação de riscos. No entanto, a efetividade dessas normas depende do fortalecimento da fiscalização, da

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

capacitação dos servidores e da atualização tecnológica contínua. Dessa forma, os impactos para o Estado e para os segurados estão diretamente relacionados à capacidade institucional de prevenir, identificar e responder rapidamente às ameaças digitais.

PREVENÇÃO E SEGURANÇA DIGITAL

A proteção digital na Previdência Social emerge como um elemento essencial para mitigar os impactos dos crimes cibernéticos e preservar tanto os recursos públicos quanto a integridade dos beneficiários. Silva e Oliveira (2024) destacam que a segurança digital exige abordagens integradas que combinam tecnologia, gestão de processos e conscientização dos usuários, enquanto Bonini et al. (2021) reforçam que medidas preventivas contribuem para reduzir a vulnerabilidade de grupos mais frágeis, como idosos e pessoas com menor familiaridade tecnológica. No contexto do INSS, a prevenção abrange estratégias técnicas, normativas e educativas, todas voltadas para a minimização de riscos.

Bergamin (2023) observa que algoritmos de IA podem identificar padrões atípicos em solicitações de benefícios, possibilitando a atuação proativa antes que a fraude se concretize. Balbino e Silva (2024) acrescentam que a criptografia garante que dados sensíveis sejam protegidos durante transmissão e armazenamento, impedindo acessos não autorizados e assegurando a confidencialidade das informações. Esses mecanismos são fundamentais para impedir que criminosos digitais manipulem registros ou acessem benefícios indevidamente.

Figueiredo et al. (2021) destacam que treinamento em segurança digital permite que os colaboradores reconheçam tentativas de phishing, engenharia social e outros métodos de fraude, promovendo respostas rápidas e eficazes. Rossetti e Silva (2021) enfatizam que a educação digital se estende também aos beneficiários, que precisam compreender os riscos associados a plataformas online e adotar boas práticas de proteção, como senhas fortes e verificação em múltiplos fatores. A conscientização cria uma camada adicional de defesa, tornando menos eficazes as ações de agentes mal-intencionados.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

A Estratégia Nacional de Segurança Cibernética (E-Ciber) e a Política Nacional de Cibersegurança (PNCiber) estabelecem diretrizes para proteger infraestruturas críticas, coordenar ações entre órgãos governamentais e estimular a cultura de segurança (Alcântara; Vieira, 2024; Silva Júnior; Pimenta Júnior, 2007). Costa e Abrantes (2023) afirmam que a regulamentação também define responsabilidades sobre tratamento de dados, impondo medidas preventivas e corretivas em caso de incidentes, enquanto Pereira e Stakoviak (2022) reforçam a necessidade de integração entre dispositivos legais e ferramentas tecnológicas para fortalecer a resiliência do sistema.

Malheiro (2020) explica que sistemas de auditoria e análise de comportamento podem identificar padrões suspeitos, permitindo ações preventivas antes que os danos ocorram. Almeida et al. (2023) ressaltam que a combinação de auditoria, monitoramento de acessos e análise de risco garante que qualquer alteração indevida nos dados seja detectada rapidamente, protegendo tanto o INSS quanto os beneficiários de fraudes complexas. A capacidade de resposta rápida é determinante para limitar prejuízos financeiros e preservar a confiança da população.

Silva e Rezende (2024) destacam que a atuação conjunta de órgãos como Polícia Federal, Ministério da Justiça, Dataprev e instituições financeiras permite rastrear criminosos, compartilhar informações sobre ameaças e coordenar medidas de proteção. Lopes e Lopes (2023) acrescentam que a integração entre setores público e privado amplia a capacidade de detecção de ataques e fortalece a proteção das infraestruturas críticas, criando barreiras mais efetivas contra práticas ilícitas. No INSS, essa cooperação assegura que fraudes complexas, que envolvem múltiplos atores e plataformas digitais, sejam combatidas de forma coordenada.

Laudon e Laudon (2022) enfatizam que tecnologias defasadas aumentam a exposição a ataques e comprometem a eficiência das estratégias de segurança. Silva e Oliveira (2024) reforçam que a manutenção regular, a aplicação de patches e a evolução tecnológica são essenciais para prevenir vulnerabilidades exploráveis por criminosos. No INSS, o aprimoramento contínuo das plataformas digitais garante maior confiabilidade no processamento de benefícios e na proteção de dados sensíveis.

As medidas de prevenção e segurança digital não se limitam à tecnologia ou à legislação; incluem também a promoção de cultura de segurança entre os servidores e

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

beneficiários. Bergamin (2023) observa que, sem conscientização, mesmo os sistemas mais robustos podem ser comprometidos por falhas humanas, enquanto Figueiredo et al. (2021) afirmam que treinamento constante reduz riscos e fortalece a postura preventiva da instituição. Balbino e Santos (2024) indicam que a educação digital amplia a percepção de segurança entre os usuários, tornando-os menos suscetíveis a golpes e mais aptos a adotar medidas de proteção pessoal.

DESAFIOS JURÍDICOS E INSTITUCIONAIS NO ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS NO INSS

O enfrentamento dos crimes cibernéticos no âmbito do INSS exige uma análise que considere não apenas os recursos tecnológicos utilizados para prevenção e detecção de fraudes, mas também o conjunto de normas jurídicas que orientam a proteção dos dados, a responsabilização dos infratores e a atuação da administração pública. A digitalização dos serviços previdenciários ampliou o acesso dos segurados a requerimentos, consultas e acompanhamento de benefícios, porém também tornou mais complexa a proteção das informações pessoais e financeiras armazenadas em sistemas digitais. Lopes e Lopes (2023) destacam que os crimes virtuais desafiam o ordenamento jurídico porque se adaptam rapidamente às mudanças tecnológicas, enquanto Laudon e Laudon (2022) indicam que sistemas de informação precisam de controles internos, gestão de riscos e monitoramento constante para garantir segurança e eficiência. No caso do INSS, esses desafios são ainda mais sensíveis, pois envolvem dados de aposentados, pensionistas, trabalhadores e pessoas em situação de vulnerabilidade.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representa um marco importante no combate aos crimes informáticos no Brasil, ao alterar o Código Penal para tipificar a invasão de dispositivo informático. Essa norma tornou possível responsabilizar condutas relacionadas ao acesso indevido a computadores, celulares e sistemas, especialmente quando há violação de mecanismo de segurança para obtenção, adulteração ou destruição de dados. No contexto previdenciário, essa lei se relaciona diretamente com situações em que criminosos buscam acessar indevidamente dados de segurados, capturar senhas ou manipular informações vinculadas a benefícios. Malheiro (2020) ressalta que os cibercrimes exigem respostas jurídicas compatíveis com a

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

dinâmica da sociedade da informação, enquanto Mello (2021) reforça que a cibersegurança deve integrar a gestão de instituições que lidam com dados sensíveis. Assim, a proteção do sistema do INSS depende tanto da tecnologia quanto da responsabilização penal de quem utiliza meios digitais para praticar ilícitos.

Outro instrumento relevante é a Lei nº 12.965/2014, conhecida como Marco Civil da Internet. Essa lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção da privacidade, dos dados pessoais e da guarda de registros. No caso dos crimes cibernéticos contra segurados do INSS, o Marco Civil contribui para orientar a atuação dos provedores, a preservação de registros e a responsabilização em situações que envolvem uso indevido de plataformas digitais. Naspolini e Cestari (2022) apontam que a sociedade da informação alterou a relação entre Estado, cidadãos e tecnologia, exigindo novas formas de regulação. Silva e Rezende (2024) também observam que o ambiente virtual amplia os riscos de violação de direitos quando informações pessoais são compartilhadas ou utilizadas de forma ilícita. Nesse sentido, o Marco Civil fornece base jurídica importante para investigar condutas digitais e proteger usuários em ambientes conectados.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, possui relação direta com o tema, pois regula o tratamento de dados pessoais em meios físicos e digitais, inclusive por órgãos públicos. O INSS, por administrar informações como CPF, dados bancários, vínculos de trabalho, histórico contributivo, idade, dependentes e informações relacionadas à saúde, deve observar princípios como finalidade, necessidade, segurança, transparência e responsabilização. Balbino e Silva (2024) afirmam que o tratamento de dados sensíveis pela administração pública exige procedimentos adequados, pois falhas de gestão podem ampliar riscos aos cidadãos. Bonini et al. (2021) reforçam que a proteção financeira dos idosos demanda cuidado especial, sobretudo quando dados pessoais podem ser usados para empréstimos fraudulentos, golpes e alterações indevidas em benefícios. Portanto, a LGPD fortalece a obrigação do INSS de proteger dados e adotar medidas técnicas e administrativas contra acessos não autorizados.

A Lei nº 13.853/2019, ao alterar a LGPD e criar a Autoridade Nacional de Proteção de Dados, também possui importância para o enfrentamento das fraudes digitais. A existência de uma autoridade voltada à proteção de dados contribui para orientar,

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

fiscalizar e consolidar práticas mais seguras no tratamento de informações pessoais. Sousa et al. (2024) destacam que a proteção de dados exige adequação institucional constante, principalmente em setores que lidam com informações sensíveis. Pereira e Stakoviak (2022) reforçam que a aplicação da LGPD depende de medidas efetivas de conformidade, e não apenas de previsão normativa. No âmbito previdenciário, isso significa que o INSS precisa manter protocolos de segurança, revisar permissões de acesso, registrar operações realizadas nos sistemas e responder de maneira eficiente a incidentes envolvendo dados de segurados.

A Lei nº 14.155/2021 também é essencial para a discussão, pois alterou o Código Penal e agravou penas para crimes cometidos por meio eletrônico, como furto mediante fraude eletrônica e estelionato praticado com uso de redes sociais, contatos telefônicos, e-mails fraudulentos ou outros meios digitais. Essa norma dialoga diretamente com golpes aplicados contra aposentados e pensionistas, especialmente quando criminosos simulam atendimento oficial, enviam links falsos, solicitam atualização cadastral ou induzem a vítima a fornecer informações bancárias. Costa e Abrantes (2023) observam que o estelionato digital ganhou força com a maior dependência das tecnologias de comunicação, enquanto Silva e Oliveira (2024) ressaltam que idosos são mais vulneráveis a crimes cibernéticos por dificuldades de acesso seguro e menor familiaridade com ferramentas digitais. Desse modo, a Lei nº 14.155/2021 amplia a resposta penal para condutas que afetam diretamente segurados do INSS.

O Código Penal brasileiro, Decreto-Lei nº 2.848/1940, também continua sendo base para a responsabilização de condutas relacionadas às fraudes previdenciárias, sobretudo quando se verificam crimes como estelionato, falsidade ideológica, uso de documento falso, invasão de dispositivo informático e associação criminosa, conforme o caso concreto. No ambiente previdenciário, uma fraude pode envolver várias condutas ao mesmo tempo, como obtenção indevida de dados, falsificação de documentos, abertura de contas, alteração cadastral e recebimento irregular de benefícios. Lopes e Lopes (2023) explicam que os crimes virtuais não se apresentam de forma isolada, pois muitas vezes combinam práticas tradicionais com novos meios tecnológicos. Malheiro (2020) acrescenta que o enfrentamento dos cibercrimes exige interpretação jurídica adequada às novas formas de execução do delito. Por isso, a aplicação do Código Penal deve

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

considerar a complexidade das fraudes digitais e seus efeitos contra o patrimônio público e os segurados.

Mesmo com a existência dessas normas, o combate aos crimes cibernéticos no INSS enfrenta dificuldades práticas. Uma delas é a identificação dos autores, pois os criminosos podem utilizar perfis falsos, dados de terceiros, redes privadas, contas bancárias intermediárias e servidores localizados fora do país. Mello (2021) destaca que a cibersegurança requer monitoramento constante e articulação entre diferentes instituições, enquanto Laudon e Laudon (2022) afirmam que sistemas digitais dependem de controles capazes de detectar acessos indevidos e comportamentos fora do padrão. No INSS, essa realidade exige cooperação entre órgãos como Polícia Federal, Dataprev, instituições financeiras, Ministério da Previdência, órgãos de controle e canais de atendimento ao cidadão. Sem integração, a resposta institucional pode ser lenta e insuficiente para impedir novos prejuízos.

A legislação penal pode punir o criminoso, mas a prevenção depende de medidas educativas e administrativas que reduzam a exposição das vítimas. Coutinho e Domingues (2023) destacam que a exclusão digital dos idosos dificulta o acesso seguro a direitos, enquanto Bonini et al. (2021) apontam que a proteção financeira desse público deve ser prioridade diante do crescimento de golpes digitais. No caso do INSS, muitos segurados recebem mensagens falsas sobre prova de vida, bloqueio de benefício, revisão cadastral, liberação de valores ou empréstimos consignados. Quando a vítima acredita na comunicação fraudulenta, fornece dados pessoais e abre caminho para prejuízos financeiros. Assim, a efetividade das leis depende também de campanhas claras, linguagem acessível e orientação permanente sobre canais oficiais.

A LGPD exige medidas técnicas e administrativas aptas a proteger dados pessoais, mas sua aplicação prática depende de estrutura institucional. Bergamin (2023) observa que a inteligência artificial vem transformando os processos de trabalho e pode auxiliar na identificação de padrões suspeitos. Figueiredo et al. (2021) defendem que a tecnologia precisa estar associada à responsabilidade ética, jurídica e educacional. No INSS, ferramentas como autenticação multifatorial, biometria, cruzamento de bases de dados, auditorias automatizadas e análise de comportamento podem reduzir fraudes. Contudo,

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

tais instrumentos devem ser aplicados com equilíbrio, para proteger o sistema sem dificultar indevidamente o acesso de beneficiários legítimos.

O Marco Civil da Internet e a LGPD também reforçam a importância da transparência no uso de dados e da proteção da privacidade. O segurado precisa compreender como seus dados são tratados, quais canais são oficiais e quais práticas podem colocar suas informações em risco. Rossetti e Silva (2021) apontam que a educação digital contribui para prevenir danos no ambiente virtual, ao permitir que o cidadão reconheça ameaças e adote condutas mais seguras. Silva e Rezende (2024) acrescentam que violações no ambiente digital podem afetar não apenas o patrimônio, mas também a intimidade e a dignidade da vítima. Por essa razão, o INSS deve aliar tecnologia e comunicação pública, orientando os beneficiários a não compartilhar senhas, não clicar em links suspeitos e não enviar documentos por canais não oficiais.

Balbino e Silva (2024) afirmam que o tratamento de dados sensíveis exige gestão responsável e procedimentos seguros, especialmente no setor público. Malheiro (2020) ressalta que a repressão penal, embora importante, não substitui a prevenção. No INSS, auditorias podem identificar alterações cadastrais repetidas, concessões atípicas, acessos incomuns, documentos inconsistentes e pagamentos direcionados a contas suspeitas. Essas medidas dialogam com a LGPD, pois demonstram responsabilidade institucional no tratamento de dados e ajudam a reduzir danos ao erário e aos segurados.

CONSIDERAÇÕES FINAIS

O presente artigo permitiu compreender que os crimes cibernéticos no âmbito do INSS representam um desafio relevante para a administração pública, especialmente diante da crescente digitalização dos serviços previdenciários. A modernização dos canais de atendimento trouxe avanços importantes, como maior agilidade, facilidade de acesso e redução de deslocamentos para os segurados. No entanto, essa mesma transformação também ampliou os riscos de fraudes digitais, invasões, uso indevido de dados, falsificação documental e golpes direcionados a aposentados, pensionistas e demais beneficiários.

Verificou-se que os impactos dessas práticas ilícitas atingem tanto o Estado quanto os segurados. Para o poder público, as fraudes provocam prejuízos ao erário,

aumento dos custos administrativos, necessidade de auditorias constantes e comprometimento da eficiência dos serviços. Para os beneficiários, os danos podem envolver perda financeira, exposição de dados pessoais, bloqueio de benefícios, contratação indevida de empréstimos e insegurança quanto à proteção de suas informações. Esse cenário mostra que a proteção previdenciária não depende apenas da concessão correta dos benefícios, mas também da garantia de um ambiente digital seguro e confiável.

A análise também demonstrou que o enfrentamento dos crimes cibernéticos exige a integração entre tecnologia, legislação e educação digital. Leis como a Lei Carolina Dieckmann, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei nº 14.155/2021 oferecem instrumentos importantes para responsabilizar condutas ilícitas e orientar a proteção das informações pessoais. Entretanto, a existência de normas legais precisa ser acompanhada de medidas práticas, como autenticação multifatorial, monitoramento contínuo, capacitação de servidores, auditorias internas, cooperação entre órgãos públicos e orientação acessível aos segurados.

Conclui-se que a prevenção dos crimes cibernéticos no INSS deve ser tratada como uma responsabilidade contínua e compartilhada. O Estado precisa investir em sistemas seguros, fiscalização eficiente e atualização tecnológica permanente, enquanto os segurados devem ser orientados sobre os riscos digitais e os canais oficiais de atendimento. Dessa forma, torna-se possível reduzir fraudes, proteger os recursos públicos, preservar os dados pessoais dos beneficiários e fortalecer a confiança da população na Previdência Social.

REFERÊNCIAS

BALBINO, Michelle; SILVA, Flavia Oliveira Guedes. O tratamento de dados sensíveis da população coletados pela administração pública municipal: **a necessária alteração nos procedimentos de gestão para o tratamento de dados sensíveis no Alto Paranaíba em Minas Gerais.** LexLab – Revista Eletrônica de Direito, v. 1, n. 1, p. 184-197, 2024.

BERGAMIN, Marta. Trabalho e inteligência artificial: **consequências psicossociais das transformações sociotécnicas do trabalho.** Aurora: Revista de Arte, Mídia e Política, v. 16, n. 48, p. 93-113, 2023.

BONINI, Deise Mara Soares et al. **Proteção financeira dos idosos à luz da Lei Geral de Proteção de Dados.** Research, Society and Development, v. 10, n. 12, p. e575101220973-e575101220973, 2021.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

BRASIL. **Decreto-Lei nº 2.848,** de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Rio de Janeiro, 31 dez. 1940.

BRASIL. **Lei nº 12.737,** de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União: Brasília, DF, 3 dez. 2012.

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.

BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. **Lei nº 13.853,** de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. Diário Oficial da União: Brasília, DF, 9 jul. 2019.

BRASIL. **Lei nº 14.155,** de 27 de maio de 2021. Altera o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Diário Oficial da União: Brasília, DF, 28 maio 2021.

COSTA, Vanessa Barbosa; ABRANTES, Joselito Santos. A influência da pandemia da COVID-19 nos crimes de estelionato digital ocorridos no município de Santana-Amapá. **Revista Científica Multidisciplinar do CEAP,** v. 5, n. 1, 2023.

COUTINHO, Weverton; DOMINGUES, Sana Gimenes Alvarenga. A exclusão digital dos idosos e o acesso à justiça. **Revista Científica Multidisciplinar UNIFLU,** v. 8, n. 2, p. 22-33, 2023.

FIGUEIREDO, Adriana et al. Tecnologia e responsabilidade: **reflexões éticas, jurídicas e educacionais.** Curitiba: Editora BAGAI, 2021.

LAUDON, Kenneth C.; LAUDON, Jane P. Sistemas de informação gerenciais: **administrando a empresa digital.** Porto Alegre: Bookman Editora, 2022.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. Crimes virtuais no ordenamento jurídico brasileiro. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** v. 9, n. 8, p. 462-472, 2023.

MALHEIRO, Emerson Penha. **O trabalho do preso como forma de ressocialização em face da prática de cibercrimes na sociedade da informação.** Revista dos Tribunais, São Paulo, v. 1014, p. 209-227, 2020.

MELLO, Janaina Cardoso. Cibersegurança em gestão de museus no século 21 nas humanidades digitais. **Boletim do Tempo Presente,** v. 10, n. 7, p. 12-28, 2021.

NASPOLINI, Samyra Haydêe Dal Farra; CESTARI, Ricardo Yunes**. O futuro do direito e do estado na sociedade da informação.** Revista Direito UFMS, v. 8, n. 1, p. 66-82, 2022.

PEREIRA, Muniz Araújo; STAKOVIAK, Paulo Beli Moura. **A Lei Geral de Proteção de Dados no ensino superior.** Humanidades & Inovação, v. 9, n. 20, p. 166-181, 2022.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.2 abr/jun. 2026 DOI: 10.47538/RA-2026.V5N2
ISSN: 2965-0003

ROSSETTI, Regina; SILVA, Ciro Ferreira. **Educação digital no enfrentamento do ciberbullying e a Lei Geral de Proteção de Dados.** ECCOM: Educação, Cultura e Comunicação, v. 12, n. 24, 2021.

SILVA, João Antonio Maciel; REZENDE, Paulo Izidio. Crimes cibernéticos: **o compartilhamento de fotos, vídeos e conteúdos íntimos por motivo de vingança.** Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 1727-1743, 2024.

SILVA, Uênis Pereira; OLIVEIRA, Marcela Cordeiro. **Os crimes cibernéticos e a vulnerabilidade dos idosos.** LexLab – Revista Eletrônica de Direito, v. 1, n. 1, p. 34-55, 2024.

SOUSA, Vanielly Lino et al. **Os impactos da Lei Geral de Proteção de Dados (LGPD) no sistema de saúde brasileiro.** Revista JRG de Estudos Acadêmicos, v. 7, n. 14, p. e141129-e141129, 2024.

Submissão: janeiro de 2026. Aceite: fevereiro de 2026. Publicação: junho de 2026.