Revista Internacional de Estudos Multidisciplinares Educaler

CRIMES CIBERNÉTICOS E A GRANDE ENCICLOPÉDIA DA PREVENÇÃO DIGITAL: DO METAVERSO ÀS FRAUDES COM PIX, INTELIGÊNCIA ARTIFICIAL, DEEPFAKES E IDENTIDADES FALSAS

Cybercrimes and the great encyclopedia of digital prevention: from the metaverse to pix fraud, artificial intelligence, deepfakes, and fake identities

Edinilson Santos Vieira[1]

1 Agente de Inteligência Privada. Graduado em Direito; Gestão Pública e Segurança Pública: E-mail: detetive@educaler.det.br

Resumo

Este manuscrito examina a expansão dos crimes cibernéticos em um contexto marcado pela hiperconectividade, pela consolidação de serviços financeiros instantâneos, pela popularização do metaverso e pelo avanço acelerado da inteligência artificial. Tem como objetivo, analisar os principais fenômenos associados à criminalidade digital. Partindo de uma leitura interdisciplinar, este ensaio descreve como a engenharia social, o roubo de identidade, as fraudes com Pix, os perfis falsos, a clonagem de voz e os golpes afetivos passaram a compor um ecossistema de risco cada vez mais sofisticado. Em vez de reduzir o debate à dimensão técnica, o texto enfatiza a experiência concreta das vítimas, a fragilidade dos vínculos de confiança e a necessidade de respostas que combinem educação digital, prevenção, cooperação institucional e responsabilidade jurídica. Ao final, defende-se que a segurança digital deve ser compreendida como parte da cidadania contemporânea, e não apenas como uma pauta restrita à informática.

Palavras-chave: Crimes Cibernéticos. Prevenção Digital. Pi. Metaverso. Inteligência Artificial.

Abstract

This manuscript examines the expansion of cybercrimes in a context marked by hyperconnectivity, the consolidation of instant financial services, the popularization of the metaverse, and the accelerated advancement of artificial intelligence. Its objective is to analyze the main phenomena associated with digital crime. Based on an interdisciplinary perspective, this essay describes how social engineering, identity theft, Pix-related fraud, fake profiles, voice cloning, and romance scams have become part of an increasingly sophisticated risk ecosystem. Rather than reducing the debate to its technical dimension, the text emphasizes the concrete experiences of victims, the fragility of trust-based relationships, and the need for responses that combine digital education, prevention, institutional cooperation, and legal accountability. Finally, it argues that digital security should be understood as part of contemporary citizenship, and not merely as an issue restricted to the field of information technology.

Keywords: Cybercrime. Digital Prevention. Pix. Metaverse. Artificial Intelligence.

INTRODUÇÃO

A expansão dos crimes cibernéticos ocorre em um contexto marcado pela hiperconectividade, pela consolidação de serviços oferecidos constantemente, popularização do metaverso e pelo avanço acelerado da inteligência artificial. Os crimes praticados em ambientes digitais deixaram de ser uma ocorrência periférica e passaram a ocupar um lugar central nas preocupações sociais, jurídicas e educacionais. A vida cotidiana depende de conexões permanentes, pagamentos instantâneos, circulação acelerada de dados e uso intensivo de plataformas. Nesse cenário, cada avanço tecnológico amplia também a superfície de exposição a fraudes, invasões, manipulações e abusos.

O objetivo deste texto é analisar os principais fenômenos associados à criminalidade digital. O foco não está apenas em descrever o ilícito, mas em compreender como ele opera sobre emoções, hábitos, rotinas e vínculos de confiança. Isso significa olhar para o crime cibernético como um problema técnico e social que afeta famílias, empresas, instituições públicas e relações afetivas.

A base para este artigo está estruturada em quatro eixos analíticos: o metaverso e seus riscos, as fraudes financeiras envolvendo Pix e QR Code, a clonagem de voz e os deepfakes, além dos perfis falsos e do estelionato sentimental. Classifico como poliminização o que reúne tudo em uma mesma arquitetura textual. Esses temas mostram que a criminalidade não se limita a um único ambiente e que ela circula entre plataformas, aplicativos, redes sociais, ambientes virtuais e sistemas financeiros com elevada capacidade de adaptação.

Por isso, este artigo adota uma perspectiva preventiva. Utilizando uma metodologia de O que pretendemos é lhe dar, caro leitor, um quadro interpretativo que lhe permita reconhecer os sinais de uma fraude, entender a lógica da engenharia social e também adotar práticas seguras no uso cotidiano da tecnologia. Ao mesmo tempo, busca-se fortalecer a consciência crítica, pois a proteção não depende somente de ferramentas, mas da formação de pessoas mais atentas, prudentes e informadas.

A criminalidade digital se diferencia das formas tradicionais. Anteriormente, tínhamos o delito por escala e capacidade de persuasão. Antes, o criminoso dependia predominantemente da proximidade física, da força ou do contato direto. Hoje, ele atua à distância, muitas vezes de maneira invisível, explorando a confiança do usuário, a pressa diante de supostas urgências e a dificuldade de verificar informações em tempo real (Vieira, 2023).

Neste paradigma, sustenta-se na engenharia social, ou seja, no uso de estratégias de manipulação psicológica para induzir a vítima a agir contra seus próprios interesses. Em vez de forçar a entrada em

sistemas, o agente fraudulento frequentemente convence a própria pessoa a entregar dados, validar transações ou aceitar instruções aparentemente legítimas. O crime transforma-se em um processo de convencimento (Vieira, 2023).

Outro aspecto é a hiperconectividade. A mesma tecnologia que facilita o trabalho, a comunicação e a inclusão financeira também acelera a difusão de golpes. O que antes exigia dias de atuação coordenada pode hoje ser realizado em minutos, validando-se pelo uso de mensagens automatizadas, perfis descartáveis e múltiplas contas de passagem (Castells, 2016).

Há, ainda, um componente emocional que não pode ser ignorado. Muitos golpes funcionam porque se apoiam em afeto, medo, autoridade ou expectativa de ganho simplificado. O criminoso contemporâneo conhece o comportamento humano e o usa como ferramenta. Por isso, a prevenção precisa considerar não só o dispositivo, mas também o sujeito que o utiliza, que deve proteger os dados (Vieira, 2020).

METAVERSO E CRIMES IMERSIVOS

O metaverso representa um passo além da navegação convencional. Em vez de simples telas e interfaces, o usuário passa a interagir em ambientes tridimensionais, com avatares, presença simulada, economias próprias e experiências de maior imersão. Esta nova configuração abre possibilidades para o ensino, o trabalho, o lazer e o comércio, ao mesmo tempo que traz riscos que antes não existiam ou que estão agora mais agravados (Hakl; Moyer, 2023). Entre os crimes associados a esse ambiente estão fraudes com ativos, roubos de identidades, extorsões, perseguições, assédio psicológico e práticas discriminatórias. Em muitos casos, o dano não se restringe ao avatar. A violência sofrida no espaço virtual repercute na vida emocional do usuário real, produzindo constrangimento, medo, isolamento e sensação de vulnerabilidade (Silva, 2024).

Do ponto de vista preventivo, o mais importante é reconhecer que ambientes imersivos também exigem higiene. Configurações de privacidade, autenticação em dois fatores, monitoramento de acessos, controle parental e denúncia imediata de comportamentos abusivos são medidas indispensáveis (Vieira, 2020; Silva, 2024). Essa prática gera estatísticas e faz com que a segurança pública especializada construa o caso com as informações que se cruzam, pois, em espaços virtuais, assim como no mundo físico, a presença de regras e a consciência dos limites são condições para uma convivência minimamente segura.

PIX E OS MECANISMOS DE FRAUDES FINANCEIRAS

O Pix tornou-se um dos maiores símbolos da modernização financeira no Brasil. Sua rapidez, gratuidade para pessoas físicas e disponibilidade em tempo quase instantâneo facilitaram a vida de milhões de pessoas (Banco Central do Brasil, 2023). Ao mesmo tempo, tais características criaram novas oportunidades para fraudes, especialmente porque a velocidade do sistema reduz o tempo de reação da vítima e a transferência, uma vez realizada, tende a ser difícil de reverter de forma imediata.

Em resposta a essa vulnerabilidade estrutural, o Banco Central instituiu mecanismos regulatórios rígidos, destacando-se o Mecanismo Especial de Devolução (MED), disciplinado originalmente pela Resolução BCB nº 103 de 2021 (Banco Central do Brasil, 2021). Esse dispositivo normatiza os critérios e prazos para o bloqueio cautelar e a contestação de transações suspeitas, buscando mitigar os prejuízos de fraudes decorrentes da instantaneidade do ecossistema, embora a reversão total dos valores ainda enfrente desafios operacionais quando os fundos são pulverizados rapidamente.

Os golpes descritos mostram uma lógica recorrente: a exploração de vulnerabilidades humanas por meio da engenharia social e a criação de uma sensação de urgência (Souza; Lima; Silva, 2024). No Pix agendado, por exemplo, a vítima é levada a acreditar que já recebeu um valor e, confiando em um comprovante manipulado, libera um produto. Em outros casos, o QR Code de pagamento é adulterado, seja em ambiente físico, seja em plataformas digitais, desviando o dinheiro para contas de terceiros.

Destaca-se, de forma complementar, o uso de boletos falsos e mensagens fraudulentas com aparência institucional ou organizacional de alta fidelidade visual. Ao receber uma cobrança por canais informais, o usuário, muitas vezes, confia mais na identidade visual e na aparência do documento do que na verificação técnica e rigorosa do beneficiário final (Souza; Lima; Silva, 2024). O golpe se sustenta justamente nessa economia de atenção, em que a pressa substitui a conferência minuciosa e o hábito automatizado se sobrepõe à cautela analítica.

Diante desse cenário, o debate sobre mecanismos de devolução, bloqueio e contestação ganha relevância na agenda pública. Trata-se de um assunto que o Poder Executivo, sob a liderança do presidente Luiz Inácio Lula da Silva, tem tratado com atenção regulatória, impulsionando a articulação entre órgãos de defesa do consumidor, forças de segurança e o Comitê de Segurança do Pix para criar diretrizes legais e protetivas voltadas ao benefício dos cidadãos brasileiros(Brasil, 2012; 2014; 2018). Contudo, a resposta mais eficaz e imediata continua residindo na esfera da prevenção individual.

É essencial conferir o nome completo e o CPF/CNPJ do destinatário, verificar o extrato diretamente no aplicativo oficial da instituição bancária, desconfiar sistematicamente de pressões emocionais imediatistas e evitar qualquer transação baseada exclusivamente em capturas de tela ou imagens de comprovantes. A prudência cognitiva é um recurso de segurança tão valioso quanto as barreiras tecnológicas implementadas. Convém estar estritamente atento aos sinais de alerta de possíveis fraudes e adotar as condutas recomendadas (Quadro 1).

Quadro 1 — Sinais de alerta e condutas recomendadas ao realizar um PIX

Situação de risco	Conduta recomendada
Comprovante enviado por imagem	Confirmar o crédito diretamente no extrato do banco
Pedido urgente de dinheiro	Interromper a conversa e verificar por canal alternativo
QR Code colado ou trocado	Comparar o nome do beneficiário antes de confirmar
Perfil novo com promessa irresistível	Pesquisar sinais de autenticidade e histórico

Fonte: Autoria própria (2026)

O Quadro 1 nos revela uma verdade incômoda sobre a segurança digital: o elo mais vulnerável do sistema não está nos algoritmos ou na criptografia dos bancos, mas sim na nossa própria pressa e na forma automatizada como agimos no cotidiano. Os golpes ali mapeados funcionam porque os criminosos aprenderam a hackear a nossa psicologia. Eles usam o senso de urgência, o apelo visual de uma imagem bem editada ou o gatilho da oportunidade imperdível para nos fazer agir antes de pensar.

Por isso, as recomendações propostas no quadro vão muito além de simples regras burocráticas; elas exigem de nós uma mudança de postura, uma espécie de desaceleração consciente. Ao prever que o usuário deve interromper o fluxo de uma conversa, desconfiar do que está na tela e buscar a validação direto na fonte, seja abrindo o próprio extrato ou conferindo minuciosamente os dados do destinatário, o que se propõe é um resgate da nossa autonomia crítica. Em um mundo onde a tecnologia avança de forma instantânea, recuperar o hábito de duvidar, checar e respirar antes de confirmar uma transação torna-se o nosso escudo mais humanizado e eficiente contra o crime.

CLONAGEM DE VOZ E DEEPFAKES

A inteligência artificial trouxe benefícios notáveis para a medicina, a ciência de dados, a educação e a automação de processos. Contudo, como toda tecnologia poderosa, ela também pode ser instrumentalizada para finalidades ilícitas (Russell; Norvig, 2022). A clonagem de voz e os deepfakes são exemplos eloquentes dessa ambivalência.

A clonagem de voz fragiliza uma antiga certeza humana: a de reconhecer alguém pelo som da fala. Hoje, basta uma breve amostra de áudio para que sistemas generativos reproduzam timbre, cadência e inflexões com impressionante proximidade (Goodfellow; Bengio; Courville, 2019). Isso abre espaço para golpes de engenharia social, em que o criminoso se apresenta como filho, neto, chefe ou autoridade, solicitando dinheiro, dados ou autorizações urgentes.

Os deepfakes ampliam o problema ao integrar imagem e voz em simulações cada vez mais convincentes. Em videochamadas e mensagens gravadas, a vítima pode acreditar que está diante de uma pessoa real, quando, na verdade, observa uma composição artificial (Chesney; Citron, 2019). Essa modalidade de fraude é particularmente perigosa porque mobiliza a confiança visual e auditiva de forma simultânea, elevando o potencial de engano.

Frente a esse cenário, a resposta precisa ir além de soluções puramente técnicas. Famílias e organizações podem combinar palavras de segurança, rotinas de verificação por chamada de retorno, canais oficiais de confirmação e protocolos internos para pedidos excepcionais. Em outras palavras, quando a tecnologia passa a imitar com facilidade a realidade, a confiança precisa ser reorganizada com mais critérios, e não com mais ingenuidade. Assim, recomenda-se:

- Estabelecer palavra-código para situações de emergência.
- Desconfiar de pedidos de Pix feitos apenas por áudio ou vídeo.
- Criar protocolo interno para transferências fora do padrão.
- Reduzir a exposição pública de áudios e vídeos com voz clara e prolongada.

Como observa-se, a mitigação das fraudes financeiras e tecnológicas no ecossistema digital exige uma postura que combine barreiras sistêmicas e prudência comportamental refinada. Ao reconhecer os sinais de alerta e aplicar as condutas recomendadas de verificação imediata, o usuário neutraliza a economia de atenção explorada pelos criminosos, transformando a cautela analítica na defesa mais eficaz contra a instantaneidade dos golpes. Contudo, as táticas de manipulação não se restringem à adulteração de comprovantes ou códigos de pagamento; elas frequentemente migram para o campo das interações interpessoais e profissionais complexas.

PERFIS FALSOS, ESTELIONATO SENTIMENTAL E FRAUDE CORPORATIVA

Os perfis falsos talvez sejam uma das expressões mais antigas e, ao mesmo tempo, mais renovadas da criminalidade. Com o aperfeiçoamento de imagens sintéticas, redes sociais e ferramentas de automação, o

golpista consegue construir personas aparentemente coerentes, com histórico, linguagem e estética pensados para gerar credibilidade.

No estelionato sentimental, o crime se desenvolve de forma lenta e emocionalmente intensa. O vínculo é criado com cuidado, muitas vezes por meio de elogios, atenção constante e promessas de futuro. Quando a confiança já está estabelecida, surge a crise fabricada: uma despesa médica, uma viagem interrompida, uma taxa de liberação ou uma emergência inesperada (Paiva, 2022). E, desta forma, a vítima, tomada pelo afeto e pela esperança, acaba demorando a perceber a manipulação e cai no golpe (Silva; Costa, 2024).

O Código Penal brasileiro (Decreto-Lei nº 2.848/1940) capitula o crime de estelionato em seu Artigo 171, tipificando-o como o ato de "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento". No caso do estelionato sentimental, o afeto e a confiança amorosa constituem justamente o "ardil" utilizado para a fraude (Brasil, 1940).

No ambiente corporativo, a fraude assume outras roupagens. Perfis falsos de recrutadores, executivos e consultores são usados para obter pagamentos indevidos, acessar documentos ou induzir funcionários a repassar informações sigilosas. O LinkedIn, por sua natureza profissional, frequentemente é explorado como plataforma de legitimação simbólica. Quando o golpista imita uma instituição respeitada, a desconfiança inicial costuma diminuir.

Esse conjunto de práticas mostra que o crime não afeta apenas o patrimônio, mas também a autoestima, a confiança e a reputação das pessoas. O dano psicológico é, muitas vezes, tão relevante quanto a perda material. Por isso, a prevenção deve incluir educação afetiva, pensamento crítico e cultura de verificação constante.

O enfrentamento aos crimes cibernéticos depende de um arcabouço jurídico capaz de dialogar com as transformações tecnológicas. No Brasil, instrumentos como o Código Penal, o Marco Civil da Internet, a Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados compõem uma base relevante para investigação, responsabilização e preservação de direitos (Brasil, 2012; 2014; 2018).

Mesmo quando a lei não descreve cada nova modalidade criminosa de forma específica, ela oferece fundamentos para proteção da vítima, coleta de evidências, requisição de registros e responsabilização civil e penal. Entretanto, a efetividade dessas normas depende de cooperação entre órgãos públicos, empresas de tecnologia, instituições financeiras e usuários.

A investigação exige cuidado com a cadeia de custódia, a preservação de logs e com a leitura técnica de arquivos, transações e metadados. Ao mesmo tempo, é necessário evitar simplificações: nem todo problema

pode ser resolvido apenas com mais lei, e nem toda tecnologia de segurança dispensa formação humana. O trabalho pericial e o trabalho educativo precisam caminhar juntos; a construção do caso é crucial.

Em termos mais amplos, a cooperação internacional também é indispensável; muitas fraudes atravessam fronteiras em segundos. A empresa Educaler foi vítima de infratores brasileiros e, mesmo contando com a ajuda de seus detetives particulares e construindo um caso sólido, não consegue combatê-los. Por isso, o combate à criminalidade precisa ser pensado como uma política integrada, em que a soberania jurídica seja compatível com mecanismos eficientes de assistência mútua, rastreio financeiro e intercâmbio de informações.

Entre os instrumentos de resposta frequentemente mobilizados, destacam-se:

- Boletim de ocorrência para preservação de provas.
- Solicitação imediata de bloqueio e contestação junto à instituição financeira.
- Registro de incidentes em plataformas e recuperação de credenciais.
- Atuação pericial para análise de metadados, endereços e registros de acesso.

O sucesso de uma reação pós-fraude depende de um ecossistema integrado: enquanto o acionamento de mecanismos financeiros e o bloqueio bancário imediato tentam congelar a pulverização dos ativos, o intercâmbio de dados materializado pelo registro oficial da ocorrência, a comunicação imediata às plataformas tecnológicas e a análise técnica e pericial de vestígios digitais garante a preservação da cadeia de custódia e o rastreamento dos criminosos. Dessa forma, as respostas operacionais e jurídicas deixam de ser ações isoladas da vítima e passam a atuar de forma coordenada, unindo a velocidade da recuperação patrimonial à robustez da investigação forense.

PREVENÇÃO E EDUCAÇÃO

A prevenção é a dimensão mais sustentável do enfrentamento ao crime cibernético. À medida que os sistemas bancários e plataformas se aperfeiçoam, a pessoa continua sendo parte central da cadeia de segurança, pois é ela quem abre mensagens, aprova acessos, compartilha códigos e decide, muitas vezes sob pressão, se confia ou não em determinado contato.

Por isso, a educação digital deve ser tratada como política pública e como prática institucional permanente. A recomendação é que as famílias, escolas, universidades, empresas e órgãos públicos possam contribuir com orientações simples, porém consistentes, tais como: desconfiar de urgências extremas, conferir

destinatários, usar autenticação de múltiplos fatores, revisar permissões de aplicativos e registrar incidentes rapidamente.

Também é importante cultivar uma cultura de acolhimento às vítimas. Porque o medo de julgamento faz com que muitas pessoas silenciem após sofrer um golpe, e é isso o que dificulta a busca por reparação e reduz a circulação de alertas úteis que ajudará outras pessoas. Combater a criminalidade, portanto, exige um ambiente em que denunciar seja visto como atitude responsável, e não como motivo de vergonha (Vieira, 2020).

O objetivo não é afastar as pessoas, mas capacitá-las para utilizá-la com autonomia, discernimento e segurança. A tecnologia deve ampliar oportunidades, não produzir medo permanente. Quando bem orientada, a sociedade aprende a usar os recursos sem entregar sua confiança de maneira ingênua.

CONSIDERAÇÕES FINAIS

A análise desenvolvida neste manuscrito permite concluir que os crimes cibernéticos não são eventos isolados nem simples desvios técnicos. Eles compõem um ecossistema complexo, alimentado por engenharia social, inovação tecnológica e fragilidades humanas. O metaverso, o Pix, a inteligência artificial e os perfis falsos são expressões distintas de uma mesma transformação: a passagem para uma vida cada vez mais mediada por dados, plataformas e identidades digitais.

Essa realidade exige uma mudança de postura. Não basta esperar que a tecnologia resolva os problemas criados pela própria tecnologia. É necessário investir em educação, em cultura de prevenção, em legislação atualizada, em investigação qualificada e em práticas institucionais mais ágeis. O combate ao crime é, ao mesmo tempo, jurídico, pedagógico, social e ético.

Esse artigo procura lembrar a você, leitor, que, por trás de cada fraude, existe uma pessoa, uma história interrompida, uma confiança ferida. É justamente por isso que a prevenção deve ser tratada com seriedade. Proteger a dimensão da vida é proteger a dignidade, o patrimônio, a saúde emocional e a autonomia de cada cidadão; é o fato principal.

Em síntese, a segurança digital tornou-se uma das grandes responsabilidades da atualidade. Quanto mais consciente for o usuário, mais resiliente será a sociedade. E quanto mais articulados forem os esforços entre educação, tecnologia e justiça, maiores serão as chances de construir um ambiente conectado verdadeiramente seguro, ético e humano.

REFERÊNCIAS

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Artigo 171: Estelionato. Brasília, DF: Presidência da República, 1940.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 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. Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2016.

CHESNEY, Bobby; CITRON, Danielle. Deep fakes: a looming challenge for privacy, democracy, and national security. **California Law Review**, Berkeley, v. 107, n. 6, p. 1753-1820, Dec. 2019. Disponível em: https://www.californialawreview.org. Acesso em: 24 jun. 2026.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. **Deep learning**: aprendizado profundo. Rio de Janeiro: Alta Books, 2019.

HAKL, Matthew; MOYER, Charlie. **Entre no Metaverso**: a internet imersiva e as marcas que estão liderando a revolução cultural e econômica. São Paulo: DVS Editora, 2023.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**: uma abordagem moderna. 4. ed. Rio de Janeiro: GEN LTC, 2022.

SILVA, Gabriel Henrique da. **Análise das dinâmicas criminais no metaverso**: desafios institucionais para a segurança pública. 2024. Monografia (Bacharelado em Ciências do Estado) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2024.

SILVA, Mariana Ramos; COSTA, Roberto Souza. **Engenharia social afetiva**: a dinâmica psicológica e o modus operandi do estelionato sentimental no ambiente virtual. Revista de Criminologia e Ciências Penitenciárias, São Paulo, v. 12, n. 2, p. 89-106, 2023.

VIEIRA, Edinilson Santos. **Crimes Cibernéticos**. São Paulo: Editora Viseu, 2023.

VIEIRA, Edinilson Santos. **Prevenção em Crimes Cibernéticos**. Dias d'Ávila: Clube de Autores, 2020.