PROJETO PEDAGÓGICO DO CURSO DE CAPACITAÇÃO

Curso de Investigação Avançada de Fraudes Eletrônicas e Estelionato Digital

REALIZAÇÃO
Universidade Federal do Pará
Instituto de Ciências Exatas e Naturais
Programa de Pós-Graduação em Segurança Pública
Resolução No 5.983/2025- CONSEPE/UFPA, de 15 de outubro de 2025

PROJETO PEDAGÓGICO DO CURSO DE CAPACITAÇÃO: Curso de Investigação Avançada de Fraudes Eletrônicas e Estelionato Digital.

Belém – PA

2025

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA

AUTORES

Thiago Galvão Sobrinho
Edson Marcos Ramos Leal Soares

COMO REFERENCIAR ESTA OBRA

SOBRINHO, Thiago Galvão; RAMOS, Edson Marcos Leal Soares. Projeto pedagógico do curso de Capacitação: Curso de Investigação Avançada de Fraudes Eletrônicas e Estelionato Digital. Programa de Pós-Graduação em Segurança Pública. Instituto de Ciências Exatas e Naturais. Universidade Federal do Pará, 2025.

SUMÁRIO

APRESENTAÇÃO

O presente curso de capacitação é resultado de uma lacuna identificada na formação de policiais civis em resposta ao crescente crime de fraude eletrônica que ocorre em todo o Brasil. Desenvolvido no âmbito do Programa de Pós-Graduação em Segurança Pública (PPGSP) da Universidade Federal do Pará (UFPA), visando estabelecer um nivelamento de conhecimento nas investigações desta modalidade de crime cibernético e financeiro, com a transferência de conhecimentos e metodologias que possam ser utilizadas tanto no estado do Pará quanto por outros estados da federação.

Com uma carga horária ampliada e foco em estudos práticos, o curso visa preparar todos os policiais civis, de todas as categorias, para se tornarem agentes multiplicadores, assim como, referências no enfrentamento do crime de fraude eletrônica.

1. JUSTIFICATIVA

A constante evolução da sociedade, tanto no uso da tecnologia quanto nos serviços financeiros, que hoje migram para o universo digital transformou a forma que o criminoso age, levando o estelionato também para este ambiente, nascendo a fraude eletrônica. Neste cenário, o policial se depara com um crime sofisticado e complexo que envolve vários conhecimentos e que não respeita fronteiras ou idiomas, exigindo um aperfeiçoamento por parte do estado na busca pelo seu combate e prevenção. A polícia Civil, como órgão de investigação criminal, necessita deste aprimoramento contínuo e especializado no seu corpo técnico.

Este curso se justifica pela necessidade urgente de aperfeiçoamento das investigações policiais com a criação de habilidades para:

a) **Combater a evolução criminosa:** os golpes financeiros e as novas técnicas de engenharia social, com o auxílio da tecnologia, demandam atualização constantes tanto para reprimir como para prevenir o crime.
b) **Recuperação de ativo:** o conhecimento e habilidade de rastrear o produto do crime através de fluxos financeiros (pix e criptoativos) é essencial para garantir a reparação dos danos sofridos pelas vítimas, bem como para descapitalizar organizações criminosas.

2. OBJETIVOS

2.1. Objetivo Geral

Qualificar policiais civis com conhecimentos e habilidades práticas na execução de investigações de baixa ou alta complexibilidade relacionadas ao crime de fraudes eletrônicas e estelionato digital, na busca de maior elucidação de casos e consequente identificação de criminosos e recuperação de ativos.

2.2. Objetivos Específicos

a) Dominar a legislação e os procedimentos necessários para a obtenção e tratamento de dados digitais, garantindo a cadeia de custódia.
b) Implementar técnicas de coleta de dados em fontes abertas (OSINT), bem como compreender e analisar dados telemáticos.
c) Rastrear e analisar fluxos financeiros complexos a partir de transações bancárias (incluindo o pix) e criptoativos, compreendendo formas de rastreio e blockchains.
d) Aplicar investigação policial e análise criminal para o enfrentamento ao crime de estelionato digital.
e) Elaborar relatórios de investigação com foco na identificação dos criminosos e na recuperação de ativos.

3. CARGA HORÁRIA: 180h/aula

4. MODALIDADE: Síncrona (Aulas ao vivo, remotas ou em laboratório integrado)

5. ÁREA DE CONHECIMENTO: Ciências Sociais Aplicadas (CNPQ)

6. INSTITUIÇÃO PROPONENTE: Programa de Pós-Graduação em Segurança Pública da Universidade Federal do Pará (PPGPS/UFPA)

7. SUPERVISÃO: Polícia Civil do Estado do Pará (PCPA)

8. LOCAL: Auditório "Ione Coelho", localizado na Delegacia Geral de Polícia Civil do Estado do Pará. Avenida Magalhães Barata, 209, bloco C, bairro Nazaré, Belém/PA.

9. PÚBLICO-ALVO: Policiais Civis do Estado do Pará (PCPA): Delegados, Investigadores e Escrivães.

10. CLASSIFICAÇÃO: Formação Continuada

11. METODOLOGIA

O curso irá abordar uma metodologia prática, aplicada e orientada para resultados, em ambiente de aulas síncronas.

- **Aulas síncronas:** Utilização de plataformas para aulas teóricas que permitam interação com os instrutores e resolução de dúvidas.
- **Estudos de Casos:** Os módulos finalizam com um caso prático real já investigado pela Polícia Civil do Estado do Pará, onde os alunos poderão compreender e aplicar o que foi ensinado.
- **Avaliação contínua:** Exercícios em formato de desafios durante os módulos para melhor compreensão dos alunos, culminando em um estudo de caso final.

12. CONTEÚDO PROGRAMÁTICO

Quadro 1: Conteúdo programático, carga horária e responsáveis por ministrar os módulos do curso de Capacitação em Investigação Avançada de Fraudes Eletrônicas e Estelionato Digital.

Módulos	Carga Horária	Professores
Módulo 1: Fundamentos Jurídicos e Cenário de Fraudes	30h	Coordenador do Laboratório de Tecnologia contra Lavagem de Dinheiro da Núcleo de Inteligência (NIP) da PCPA
Módulo 2: Engenharia Social, Golpes e OSINT	30h	Policiais Civis lotados no Laboratório de Inteligência Cibernética (CIBERLAB) da PCPA
Módulo 3: Procedimentos Investigativos, Telemática e Cadeia de Custódia	30h	Policiais Civis lotados na Divisão de Sinais e Dados (DISD) e CIBERLAB da PCPA.
Módulo 4: Investigação Financeira, recuperação de ativos e Rastreamento de Criptoativos	30h	Policiais Civis lotados no LAB-LD e no Núcleo de recuperação de Ativos (NRA) da PCPA
Módulo 5: Estratégias de Inteligência e Ambientes Ocultos	30h	Policiais Civis lotados no NIP
Módulo 6: Inteligência Artificial, Enfrentamento e Mitigação de Riscos	30h	Policiais Civis lotados no Laboratório de Inteligência Cibernética (CIBERLAB) da PCPA

Fonte: Elaborado pelos autores, 2025

13. SISTEMA DE AVALIAÇÃO

A avaliação será realizada de forma contínua pelos professores e coordenadores do curso, sendo necessário alcançar um mínimo de frequência de 85%, conforme prevê o Art. 50 do Regimento Interno da Academia de Polícia Civil do Estado do Pará. Ao final, os concluintes receberão um certificado de conclusão do curso, expedido pela ACADEPOL.

14. CONSIDERAÇÕES FINAIS

- O curso de capacitação terá acompanhamento pedagógico e será concluído conforme os seguintes pontos:
- O acompanhamento pedagógico ficará a cargo do setor pedagógico do PPGSP/UFPA e da ACADEPOL/PA com designação de um supervisor de curso.

- Caberá ao supervisor organizar as inscrições, controlar frequências e pontualidade dos docentes e discentes.
- Ao final, os discentes que cumprirem os requisitos de frequência e aproveitamento previstos, receberão certificado de conclusão do curso.
- As indicações dos discentes serão responsabilidade da Diretoria competente, que comunicará aos selecionados o período e forma da inscrição.
- Situações não previstas neste projeto serão analisadas pela Diretoria da ACADEPOL/PA em articulação com a coordenação acadêmica do curso.

15. DAS EMENTAS DOS MÓDULOS

Módulo 1	Fundamentos Jurídicos e Cenário de Fraudes
Carga Horária	30h/aula
Professor	Coordenador do Laboratório de Tecnologia contra Lavagem de Dinheiro da Núcleo de Inteligência (NIP) da PCPA
Ementa	O que são Fraudes Eletrônicas: Conceitos, tipologias e evolução no Brasil e no Pará. Normativos e Regulamentação: Lei nº 14.155/2021, Marco Civil da Internet, LGPD (Lei Geral de Proteção de Dados) e implicações na investigação. Regulamentações Bancárias: Resoluções do Banco Central e normativos específicos sobre PIX e MED (Mecanismo Especial de Devolução).
Conteúdo	Disciplina 1: Conceitos e tipologias de fraudes eletrônicas 1.1. Definição de fraude eletrônica e estelionato digital. 1.2. Tipologias mais recorrentes no contexto nacional e regional. 1.3. Tendências recentes e fatores que favorecem a prática desses delitos. Disciplina 2: Marco jurídico e regulatório 2.1. Código Penal e Lei 14.155/2021. 2.2. Marco Civil da Internet, LGPD e impactos na investigação. 2.3. Normas do Banco Central: PIX, mecanismos de devolução e circulares relevantes. Disciplina 3: Políticas institucionais e articulação interinstitucional 3.1. Atribuições dos órgãos de segurança pública e do Ministério Público. 3.2. Cooperação com instituições financeiras, COAF e órgãos de controle. 3.3. Boas práticas para padronização de procedimentos em fraudes eletrônicas.
Objetivos	Oferecer base conceitual e jurídica sólida sobre fraudes eletrônicas e estelionato digital. Capacitar o profissional a identificar o enquadramento penal e o arcabouço normativo aplicável a cada caso. Desenvolver visão crítica sobre o cenário atual de fraudes e o papel das instituições na prevenção e repressão.
Metodologia	Aulas expositivas, com apoio de recursos audiovisuais e análise de casos reais e jurisprudências. Proposição de atividades avaliativas em grupo.

Módulo 2	Engenharia Social, Golpes e OSINT

Carga Horária	30h/aula
Professor	Policiais Civis lotados no Laboratório de Inteligência Cibernética (CIBERLAB) da PCPA
Ementa	Engenharia Social e Principais Golpes: Phishing, Vishing, Smishing e Ransomware Análise de vetores de ataque e da "psicologia" do golpe. OSINT: Coleta, tratamento e análise de informações em fontes abertas (redes sociais, fóruns, sites, dados públicos).
Conteúdo	Disciplina 1: Fundamentos de engenharia social 1.1. Conceitos, fases e objetivos da engenharia social. 1.2. Técnicas de persuasão e exploração de vieses cognitivos. 1.3. Perfis de vítimas e perfilamento básico de golpistas. Disciplina 2: Principais golpes digitais 2.1. *Phishing, spear phishing* e *smishing*. 2.2. *Vishing*, golpes via aplicativos de mensagens e redes sociais. 2.3. *Ransomware*, sequestro de contas e fraudes em marketplaces. Disciplina 3: OSINT aplicado à investigação de fraudes 3.1. Fontes abertas: redes sociais, bases públicas e sites de anúncios. 3.2. Ferramentas e técnicas de coleta, correlação e verificação. 3.3. Registro, organização e encadeamento das evidências obtidas por OSINT.
Objetivos	Capacitar o aluno a reconhecer padrões de engenharia social e principais golpes eletrônicos. Desenvolver habilidades práticas de coleta e análise de informações em fontes abertas. Apoiar a construção de hipóteses investigativas com base em dados públicos estruturados e não estruturados.
Metodologia	Exposição teórica e prática de golpes nas modalidades de engenharia social. Realização de exercícios guiados de OSINT em ambiente controlado, com estudos de caso reais e roteiros de pesquisa.

Módulo 3	Procedimentos Investigativos, Telemática e Cadeia de Custódia
Carga Horária	30h/aula
Professor	Policiais Civis lotados na Divisão de Sinais e Dados (DISD) e CIBERLAB da PCPA.
Ementa	Ofícios e Dados Cadastrais: Elaboração de ofícios e requisições formais a provedores, aplicativos e redes sociais. Quebra de Sigilo Telemático: Procedimentos legais e fluxogramas para a obtenção de metadados e conteúdo de comunicações. Busca e Cadeia de Custódia de Evidências Digitais: Princípios e procedimentos para coleta de imagens e dados, garantindo validade processual.
Conteúdo	Disciplina 1: Ofícios, requisições e sigilo telemático 1.1. Requisição de dados cadastrais, registros de log e informações de acesso. 1.2. Elaboração de representações para quebra de sigilo telemático. 1.3. Fluxos de resposta de provedores de internet, aplicativos e redes sociais. Disciplina 2: Evidências digitais e procedimentos de coleta 2.1. Tipos de evidências digitais: mensagens, imagens, logs, metadados. 2.2. Técnicas básicas de preservação em dispositivos, mídias e nuvem. 2.3. Cuidados na apreensão e no espelhamento de dados.

	Disciplina 3: Cadeia de custódia na prática 3.1. Conceitos legais e requisitos formais da cadeia de custódia. 3.2. Registro, lacre, transporte, guarda e manipulação de evidências. 3.3. Documentação padronizada e comunicação com a perícia.
Objetivos	Habilitar o profissional a formular ofícios e pedidos de dados digitais de forma clara e juridicamente adequada. Garantir que o aluno compreenda as etapas da cadeia de custódia e sua relevância para a validade da prova. Promover o uso de procedimentos padronizados para tratamento de evidências telemáticas
Metodologia	Aulas expositivas teórico/práticas com modelo de requisições e relatórios. Exercício e roteiro da manutenção da cadeia de custódia digital e preservação da prova.

Módulo 4	Investigação Financeira, Recuperação de Ativos e Rastreamento de Criptoativos
Carga Horária	30h/aula
Professor	Policiais Civis lotados no LAB-LD e no Núcleo de recuperação de Ativos (NRA) da PCPA
Ementa	Inteligência e Investigação Financeira Aplicada: Análise de dados bancários e Relatórios de Inteligência Financeira (RIF) elaborados pelo COAF. Criptoativos e Rastreio: Fundamentos de Blockchain, carteiras e Exchange. Utilização de Exploradores de Blockchain para rastreio. Técnicas iniciais de rastreamento e identificação de bens para apoiar a recuperação de ativos e o bloqueio patrimonial.
Conteúdo	Disciplina 1: Fundamentos de investigação financeira 1.1. Conceitos de fluxo financeiro e camadas de movimentação. 1.2. Leitura de extratos, comprovantes de transferência e relatórios bancários. 1.3. Indicadores de operações suspeitas e sinais de ocultação de valores. Disciplina 2: Inteligência financeira e cooperação 2.1. Relatórios de inteligência financeira e comunicações de operações atípicas. 2.2. Interação com instituições financeiras e órgãos de inteligência. 2.3. Estratégias de bloqueio, sequestro e recuperação de ativos. Disciplina 3: Criptoativos e rastreamento 3.1. Conceitos básicos de blockchain, tokens e criptoativos. 3.2. Carteiras, exchanges e tipos de transações. 3.3. Uso de exploradores de blockchain e noções de análise de trilhas de criptoativos. Disciplina 4: Recuperação de Ativos 4.1. Identificação de contas de origem, passagem e destino em fraudes eletrônicas. 4.2. Elaboração de representações para bloqueio e sequestro de valores. 4.3. Fluxos de cooperação com instituições financeiras e órgãos parceiros. 4.4. Consolidação de informações financeiras em relatórios de rastreamento de ativos.
Objetivos	Desenvolver a capacidade de leitura crítica de documentos financeiros vinculados a fraudes eletrônicas. Instrumentalizar o aluno para identificar fluxos suspeitos e adotar medidas de bloqueio e recuperação de ativos. Introduzir o raciocínio investigativo voltado ao rastreamento de criptoativos e à descapitalização de grupos criminosos.
Metodologia	Aulas expositivas com muita prática em manuseio de planilhas e dashboard de

	análise. Demonstração guiada de uso de exploradores de blockchain, bem como elaboração de relatórios.

Módulo 5	Estratégias de Inteligência e Ambientes Ocultos
Carga Horária	30h/aula
Professor	Policiais Civis lotados no NIP
Ementa	Inteligência Policial: Construção de Redes Criminosas e Análise de Vínculos. Criação de Avatar e monitoramento de redes. Deep e Dark Web: Diferenciação, acesso seguro (VPN, TOR) e técnicas de coleta de informações em ambientes ocultos.
Conteúdo	Disciplina 1: Inteligência policial aplicada a fraudes eletrônicas 1.1. Ciclo de inteligência e produção de conhecimento. 1.2. Análise de vínculos, redes e fluxos de comunicação. 1.3. Identificação de funções e papéis dentro de grupos criminosos. Disciplina 2: Atuação velada e perfis encobertos 2.1. Construção e manutenção de avatares investigativos. 2.2. Monitoramento de grupos, canais e perfis em plataformas digitais. 2.3. Registro seguro das interações e coleta de evidências. Disciplina 3: Deep web, dark web e segurança operacional 3.1. Diferenças entre surface web, deep web e dark web. 3.2. Ferramentas de acesso seguro (TOR, VPN) e riscos envolvidos. 3.3. Técnicas de coleta e documentação de informações em ambientes ocultos.
Objetivos	Capacitar o profissional a empregar métodos de inteligência na investigação de fraudes eletrônicas. Desenvolver habilidades para atuação controlada em ambientes virtuais e perfis encobertos. Fornecer noções práticas sobre uso seguro e investigativo de deep e dark web
Metodologia	Aulas expositivas de análise de vínculo e estudo de inteligência policial e redes criminosas. Demonstração em ambiente controlado da criação de avatar e acesso a ambientes controlados.

Módulo 6	Inteligência Artificial, Enfrentamento e Mitigação de Riscos
Carga Horária	30h/aula
Professor	Policiais Civis lotados no NIP
Ementa	Inteligência Artificial e Enfrentamento: Uso da IA por criminosos (Deepfakes, textos automáticos) e como ferramenta de apoio à investigação policial (análise de grandes volumes de dados). Mitigação de Riscos: Identificação de vulnerabilidades em sistemas de pagamento e em ambientes da PCPA. Estratégias de prevenção e conscientização. Elaboração de Relatórios Técnicos Finais.
Conteúdo	Disciplina 1: Uso da IA por criminosos 1.1. Deepfakes, clonagem de voz e falsificação de documentos. 1.2. Automação de contatos fraudulentos e chatbots maliciosos. 1.3. IA generativa aplicada à criação de golpes personalizados. Disciplina 2: IA como ferramenta de apoio à investigação 2.1. Noções de análise de dados em larga escala. 2.2. Ferramentas de correlação, agrupamento e detecção de padrões. 2.3. Limites éticos e jurídicos no uso de IA pelo poder público.

	Disciplina 3: Mitigação de riscos e resposta a incidentes 3.1. Mapeamento de vulnerabilidades em sistemas de pagamento e ambientes institucionais. 3.2. Planos de resposta a incidentes e comunicação com vítimas e parceiros. 3.3. Campanhas de prevenção, conscientização e produção de relatórios técnicos finais.
Objetivos	Sensibilizar o aluno sobre o impacto da IA na ampliação e sofisticação das fraudes eletrônicas. Demonstrar possibilidades de uso de ferramentas baseadas em IA para apoiar a atividade investigativa. Desenvolver visão orientada à gestão de riscos, prevenção de incidentes e fortalecimento de controles institucionais.
Metodologia	Aulas expositivas com exemplos de casos envolvendo IA e fraude com demonstração de ferramentas de análise de dados. Elaboração de relatório técnico/prático sobre fraude eletrônica.

REFERÊNCIAS

Módulo 1 – Fundamentos Jurídicos e Cenário de Fraudes

BARBOSA, Adriano Mendes, **Curso de Investigação Criminal**, Porto Alegre: Nuria Fabris ed., 2014.

BERMUDEZ, André Luiz, **A investigação criminal orientada pela Teoria dos Jogos,** Florianópolis: Emais, 2020

BRASIL. Lei n. 9.613, de 03 de março de 1998. **Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9613.htm>. Acesso em 10 de maio de 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para agravar a pena do crime de estelionato cometido mediante fraude eletrônica.** Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2021.

COSTA, R. J. C. C. **Inteligência Policial Judiciária: Os limites doutrinários e legais na assessoria eficaz à repressão ao crime organizado**. Rio de Janeiro: Brasport, 2019.
PARÁ. Decreto nº 1.876/2017 de 03/09/2017. **Homologa a Resolução nº 001, de 3 de agosto de 2017, do Conselho Superior da Polícia Civil do Estado do Pará**. Disponível em: https://sistemas.pa.gov.br/sisleis/legislacao/3456. Acesso em: 18 dez. 2024

Módulo 2 – Engenharia Social, Golpes e OSINT

NASCIMENTO, Guilherme Afonso de Melo; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. A Importância Do Combate À Desinformação E A Atualização Do Código Penal Para Crimes Virtuais De Engenharia Social/Phishing . **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 8, n. 11, p. 2225–2233, 2022. DOI: 10.51891/rease.v8i11.7809. Disponível em: https://periodicorease.pro.br/rease/article/view/7809. Acesso em: 18 mar. 2025.

BARRETO, Alesandro Gonçalves. Fraudes Cometidas na Internet – Uso de Fontes Abertas na Investigação Policial e na Inteligência de Segurança Pública. **Direito & TI**, *[S. l.]*, v. 1, n. 8, p. 4, 2017. DOI: 10.63451/ti.v1i8.81. Disponível em: https://www.direitoeti.com.br/direitoeti/article/view/81. Acesso em: 10 abr. 2025.

Módulo 3 – Procedimentos Investigativos, Telemática e Cadeia de Custódia

CASTRO, Henrique Hoffmann Monteiro de, et al, ***Investigação Criminal pela Polícia Judiciária***, Rio de Janeiro: Lumen Juris, 2016.

COSTA, A. S.; DA SILVA, M. F. de B. M. A prova pericial obtida por meio do DNA à luz da cadeia de custódia. **Brazilian Journal of Health Review**, *[S. l.]*, v. 6, n. 5, p. 20609–20627, 2023. DOI: 10.34119/bjhrv6n5-099. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJHR/article/view/62920. Acesso em: 18

abr. 2025.

COSTA, Melina Even Silva da Costa; DE SÁ, Adriana Abreu; DA COSTA Rebeca Tárcia; SILVA, Gabryella Cunha Nascimento; NEGREIRO, Francisco Vidal. Cibercrimes e fraudes virtuais: o estelionato digital sob a ótica do direito. **Periódicos Brasil. Pesquisa Científica**, Macapá, Brasil, v. 4, n. 1, p. 2802–2818, 2025. DOI: 10.36557/pbpc.v4i1.336. Disponível em: https://periodicosbrasil.emnuvens.com.br/revista/article/view/336. Acesso em: 18 jan. 2025.

FERREIRA VAZ, Millena. A Preservação Da Cadeia De Custódia Como Pressuposto De Admissibilidade Da Prova Digital. **Revista da ESMESC - Publicação contínua**, *[S. l.]*, v. 30, n. 36, p. 323–350, 2023. DOI: 10.14295/revistadaesmesc.v30i36.p323. Disponível em: https://revista.esmesc.org.br/re/article/view/406. Acesso em: 11 jan. 2025.

VALENTE, Manuel Monteiro Guedes. **Cadeia de Custódia da Prova.** 2.ed., Almedina. São Paulo, 2020.

LEAL, Maria dos Reis Borges; SOUSA, Clara Maria da Silva; SILVA, Thayze Vitoria da; SANTOS, Joffreson. A QUEBRA DA CADEIA DE CUSTÓDIA E OS POSSÍVEIS REFLEXOS EM UMA SENTENÇA CRIMINAL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 9, n. 11, p. 2955–2972, 2023. DOI: 10.51891/rease.v9i11.12613. Disponível em: https://periodicorease.pro.br/rease/article/view/12613. Acesso em: 05 abr. 2025

LUIS FERNANDES, André; MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital:: A dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. **Direito & TI**, *[S. l.]*, v. 1, n. 14, p. 59–73, 2023. DOI: 10.63451/ti.v1i14.115. Disponível em: https://www.direitoeti.com.br/direitoeti/article/view/115. Acesso em: 21 jun. 2025.

SILVA, João Espínola da; BEREZOWSKI, Maria Leonice da Silva. CADEIA DE CUSTÓDIA – ATUALIZAÇÕES E DESDOBRAMENTOS TRAZIDOS PELA LEI 13.964/19. **Revista Vertentes do Direito**, *[S. l.]*, v. 10, n. 1, p. 502–520, 2023. DOI: 10.20873/uft.2359-0106.2023.v10n1.p502-520. Disponível em: https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/13451. Acesso em: 03 mar. 2025.

Módulo 4 – Investigação Financeira, recuperação de ativos e Rastreamento de Criptoativos

GAFI. As Recomendações do GAFI. Fevereiro de 2012. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Portuguese-GAFISUD.pdf. Acesso em: 5 out. 2022.

GIANNOTTE, M. V. Cooperação jurídica internacional no combate à corrupção e lavagem de dinheiro. **Revista JRG de Estudos Acadêmicos** , Brasil, São Paulo, v. 8, n. 19, p. e082457, 2025. DOI: 10.55892/jrg.v8i19.2457. Disponível em: https://revistajrg.com/index.php/jrg/article/view/2457. Acesso em: 18 jan. 2025.

TAFURI, L. B., COSTA, A. L. V., LEMES, A. C. R., & Brito, J. M. de O. (2025). O Papel Do

Coaf Como Órgão De Controle Na Prevenção À Lavagem DE DINHEIRO. ***REVISTA FOCO***, *18*(11), e10466. https://doi.org/10.54751/revistafoco.v18n11-088

SVISTALSKI, Marco Aurelio Duarte; BADUR, Nelson Antonio Satto. O laboratório de análise de dados financeiros e o combate à lavagem de dinheiro na corregedoria da PMPR: uma proposta estratégica de controle interno e fortalecimento da polícia judiciária militar. **RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218**, *[S. l.]*, v. 6, n. 9, p. e696760, 2025. DOI: 10.47820/recima21.v6i9.6760. Disponível em: https://recima21.com.br/recima21/article/view/6760. Acesso em: 18 jan. 2025.

SANTOS, Josias Mascarenhas Dos; SILVA, Rêgo Santos Cunha, Roseli. O Uso da Blockchain como ferramenta de combate à lavagem de dinheiro. **Revista Jurídica do Ministério Público do Estado do Tocantins**, *[S. l.]*, v. 16, n. 1, 2024. DOI: 10.65596/revjurmpto.v16.129. Disponível em: https://cesaf.mpto.mp.br/revista/index.php/revistampto/article/view/129. Acesso em: 18 jan. 2025.

SILVA FILHO, Marcos Vinícius Alves e. A investigação financeira e o uso de ferramentas tecnológicas no combate à corrupção e à lavagem de dinheiro. **Revista da Emeron**, Porto Velho, RO, n. 32, p. 508–554, 2023. DOI: 10.62009/Emeron.2764.9679n32/2023/213/p508-554. Disponível em: https://periodicos.emeron.edu.br/index.php/emeron/article/view/213. Acesso em: 18 jan. 2025.

Módulo 5 – Estratégias de Inteligência e Ambientes Ocultos

BRANDÃO, Priscila; Cepik, Marco. **Inteligência de segurança pública: teoria e prática no controle da criminalidade.** Niterói, RJ: Impetus, 2013.

CEPIK, Marco. **Explicando falhas de inteligência governamental: fatores histórico-institucionais, cognitivos e políticos**. In: Varia História, Belo Horizonte, vol. 28, no 47, p.79- 99, jan/jun 2012. Disponível em: <https://www.scielo.br/j/vh/a/JvTGCXX4P3nyjzp8JZpBVmb/?lang=pt#>. Acesso em 05 abril 2024.

DINELLI, Guilherme B. M**. Inteligência de Estado: novos paradigmas para políticas públicas de inteligência no governo do estado de Minas Gerais.** In: Inteligência de Segurança Pública e Cenários Prospectivos da Criminalidade - Série inteligência, estratégia e defesa social – Belo Horizonte: **Editora D'Plácido**, 2016.

GONÇALVES, Joanisval B. **Atividade de Inteligência e legislação correlata.** 6ed. Niterói, RJ: Impetus, 2018.
MINISTÉRIO DA JUSTIÇA. **Doutrina Nacional de Inteligência de Segurança Pública – DNISP. 4. ed. rev. e atual**. Brasília: Secretaria Nacional de Segurança Pública, 2016.

Módulo 6 –Inteligência Artificial, Enfrentamento e Mitigação de Riscos

ALVES, Paulo M.M.R. **O Impacto de Big Data na Atividade de Inteligência. In: Revista Brasileira de Inteligência**. N. 13 (dez 2018) - ISSN 2595-4717 versão online. Brasília: Abin,

2005. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/revista-brasileira-de-inteligencia/copy_of_RBI13.pdf> Acesso em 05 abril 2025.

DE OLIVEIRA, C.; ALEX AVELAR, E. A Era dos Algoritmos de Inteligência Artificial no Controle Gerencial. **Revista Mineira de Contabilidade**, *[S. l.]*, v. 24, n. 2, p. 4–6, 2023. DOI: 10.51320/rmc.v24i2.1543. Disponível em: https://revista.crcmg.org.br/rmc/article/view/1543. Acesso em: 10 jun. 2025.

FELIX, Hiago Marcelo Arruda; MEDEIROS Orione Dantas de. Inteligência Artificial E Teoria Do Risco No Projeto De Lei Nº 2.338/2023 . **RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218**, *[S. l.]*, v. 4, n. 11, p. e4114406, 2023. DOI: 10.47820/recima21.v4i11.4406. Disponível em: https://recima21.com.br/recima21/article/view/4406. Acesso em: 25 mar. 2025.

MAGALHÃES-TIMOTIO, J. G.; E SILVA, R. C. F.; DE OLIVEIRA, R. A.; VIEIRA, V. E. L. Inteligência artificial na produção de economia, econometria e finanças. **OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA**, *[S. l.]*, v. 21, n. 11, p. 21476–21495, 2023. DOI: 10.55905/oelv21n11-157. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/2243. Acesso em: 13 jan. 2025.


UNIVERSIDADE FEDERAL DO PARÁ

UNIVERSIDADE FEDERAL DO PARÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA

CAPES

CNPq