CENTRO UNIVERSITÁRIO PROCESSUS
Prática Extensionista

PROJETO (1º semestre/2025)

1. Identificação do Objeto

Atividade Extensionista:

PROGRAMA ( ) PROJETO (**X**) CURSO ( ) OFICINA ( )

EVENTO ( ) PRESTAÇÃO DE SERVIÇOS ( ) AÇÃO DE EXTENSÃO SOCIAL ( )

Área Temática: Direito Digital e Financeiro

Linha de Extensão:

Local de implementação (Instituição parceira/conveniada): Defensoria Pública do Distrito Federal

Título: Golpes Digitais

2. Identificação dos Autor(es) e Articulador(es)

CURSO: Direito

Coordenador de Curso:

Adalberto Nogueira Aleixo

Articulador(es)/Orientador(es):

Alberto Carvalho Amaral

Alunos(as)/Equipe:

Kanandra Pereira da Paixão Rodrigues - 2323280000153
Eduardo Nobre da Costa – Direito - 2113180000386
Dyana Kelly Monteiro da Silva - 2217200000006
Roberton Pereira Valadão - 2023180000082
Thaíslane Alencar da Silva - 2023180000036
João Marcos Ferreira Damaceno - 2227200000033
Hugo Emanuel Lira Maques - 2310010000084
Aricia Rani Dourado Barbosa - 2423180000019
Elias Nunes de Sousa Junior – 2423180000068
Djalma Torres Laurindo - 2423180000080

3. Desenvolvimento

Fundamentação Teórica:

No cenário em constante evolução do século XXI, onde a tecnologia digital rege a maneira como vivemos, trabalhamos e interagimos, surge um novo campo de batalha para a justiça e a advocacia: os crimes cibernéticos. Os crimes cibernéticos são atividades criminosas que ocorrem no ambiente digital, envolvendo o uso de computadores, redes de computadores, dispositivos eletrônicos e a internet. No Brasil, o enfrentamento dos crimes cibernéticos envolve a promulgação de leis específicas, como a Lei Carolina Dieckmann, que aborda questões de acesso não autorizado a dispositivos e a divulgação não autorizada de imagens e vídeos íntimos. Além disso, a Polícia Federal e outras agências têm unidades especializadas para investigação e combate à cibercriminalidade.

Os Golpes digitais consistem em práticas fraudulentas realizadas por meio eletrônico ou virtual, com o intuito de obter vantagem ilícita, causar prejuízo patrimonial ou obtenção de informações sensíveis. Tais fraudes podem ocorrer por meio de várias técnicas, como Phising que é a tentativa de obter dados pessoais e financeiros por meio de mensagens falsas, geralmente via e-mail ou redes sociais, que se apresentam como entidades legítimas, Pharming e skimming que é o Redirecionamento de sites legítimos para servidores maliciosos, visando capturar dados e clonagem de cartões por meio de leitores instalados em caixas eletrônicos ou pontos de venda, esquemas de pirâmide e Fraudes bancárias ou contratações indevidas.

Os crimes exclusivamente cibernéticos são aqueles que necessariamente precisam do meio computacional para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e 154-B do Código Penal Brasileiro). Já os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo dispositivo ou sistema informático, como é o caso dos crimes de violação de direito do autor ou estelionato, que podem ser praticados tanto no ambiente virtual quanto fora do mesmo.

De acordo com o Código Penal temos alguns artigos que tratam sobre golpes e fraudes eletrônicas, visando o Art. 171 trata- se do crime de estelionato onde aplica-se aos golpes digitais quando há induzimento a erro com obtenção de vantagem ilícita, sendo eles o Art. 171, §2°-A – Fraude eletrônica, Art. 154-A – Invasão de dispositivo informático, Art. 266, que trata sobre a Interrupção de serviço telegráfico, telefônico, informativo, telemático. Em 2012 tivemos a Lei 12.737/2012 Lei Carolina Dieckmann criada com o objetivo de tipificar novas condutas ilícitas cometidas no ciberespaço, temos a Lei LGPD (lEI DE PROTEÇÃO DE DADOS) entre outros. Os golpes digitais geralmente envolvem violação do princípio da segurança da informação (art. 6º, VII) e uso indevido de dados sem base legal.

A responsabilidade das empresas é objetiva, ou seja, não depende de culpa. Se houve falha e prejuízo, a empresa deve indenizar, segundo o Código de Defesa do Consumidor. Nesse sentido, destaca-se a Súmula 479 do egrégio Superior Tribunal de Justiça: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.” Assim, é necessário que o direito penal brasileiro busque sempre meios e ações assíduas que venha penalizar os crimes cibernéticos, e que acompanhe as evoluções tecnológicas a fim de garantir segurança à população

Apresentação:

Este projeto tem como temática central os Crimes Cibernéticos, considerando sua crescente relevância no contexto social contemporâneo. Com o avanço da tecnologia e o aumento do acesso da população às mídias digitais, observa-se uma transformação no cenário da criminalidade, que passou a se expandir do ambiente físico para o virtual. Como resultado, o tema tem ganhado destaque frequente nos meios de comunicação, evidenciando a urgência de um debate mais aprofundado sobre o assunto.

Dessa forma, o objetivo deste trabalho é investigar os métodos de atuação dos cibercriminosos e os principais tipos de fraudes virtuais, proporcionando aos acadêmicos um conhecimento mais amplo e crítico sobre essas práticas. Além disso, busca-se conscientizar e orientar o público-alvo sobre a importância da adoção de medidas preventivas e comportamentos

seguros no ambiente digital, contribuindo para a redução da vulnerabilidade frente a essas ameaças virtuais.

Justificativa:

Com o avanço tecnológico, a criminalidade passou a ultrapassar os limites do espaço físico, manifestando-se com frequência alarmante no ambiente digital, o que exige atenção e reflexão crítica por parte da sociedade, especialmente dos acadêmicos e futuros profissionais.

Torna-se essencial compreender as estratégias utilizadas pelos cibercriminosos, bem como os tipos de fraudes mais comuns, a fim de capacitar os indivíduos para a identificação e prevenção dessas práticas. O projeto se justifica ainda pela necessidade de promover uma cultura de segurança digital, conscientizando o público-alvo sobre os riscos presentes no uso cotidiano da tecnologia e incentivando comportamentos responsáveis e protetivos.

Desta maneira, o estudo contribui significativamente para a formação de cidadãos mais informados e preparados frente aos desafios da era digital.

Objetivos:

Geral

O projeto busca desenvolver uma intervenção junta a comunidade alertando sobre golpes digitais e como se precaver diante da situação. Informá-los que existem leis que os respaldam diante das circunstâncias sendo uma delas a LGPD (Lei Geral de Proteção de Dados).

Específicos:

1 -Compreender e analisar e conscientizar sobre fraudes virtuais e crimes digitais;
2- Investigar as técnicas usadas pelos cibercriminosos;
3- Mapear os tipos de golpes digitais;
4- Conscientizar e orientar sobre comportamentos seguros na internet;
5 -Discutir a evolução das leis brasileiras relacionadas ao tema;
6- Fortalecer a educação digital preventiva com a interação e devolutiva para a sociedade.

Metas:

A realização da oficina humana sobre golpes digitais para a população foi para promover a conscientização dos participantes sobre os principais tipos de fraudes digitais e crimes cibernéticos ao final do projeto. Capacitar os participantes para identificar práticas seguras no uso da internet e estimular a criação de hábitos seguros no ambiente virtual.

Resultados esperados:

Conscientização da população sobre a prevenção de golpes digitais/virtuais e seus impactos.

Metodologia: Biblioteca Humana.

Cronograma de execução:

DATA DE INÍCIO: 28/03/2025

DATA DE TÉRMINO: 05/07/2025

Evento	Período	Observação
Início do projeto e escolha do tema	20/02/2025	Planejamento e organização das tarefas
Levantamento teórico	até 29/04/2025	Leitura de textos, leis e estudos sobre feminicídio

Apresentação acadêmica	29/05/2025	Exposição do projeto na sala de aula
Ação externa (Defensoria Pública)	02/06/2025	Intervenção educativa junto à instituição pública
Finalização e entrega do relatório	15/06 a 30/07/2025	Sistematização dos resultados e encerramento das atividades

Considerações finais:

Vivemos uma era em que estar conectado é parte essencial da rotina, trabalhamos, estudamos, compramos, nos comunicamos e nos divertimos pela internet. No entanto, essa presença constante no mundo digital também nos expõe a uma série de riscos. Os golpes virtuais, como os analisados neste trabalho, não são mais casos isolados: são problemas reais que afetam a vida de milhões de pessoas, causando perdas financeiras, danos emocionais e desconfiança nas plataformas digitais.

Mais do que apenas entender como esses crimes acontecem, este estudo mostrou que é urgente repensar a forma como nos protegemos e como a sociedade reage a essas ameaças. A legislação brasileira tem avançado, e ferramentas como a LGPD, o Marco Civil da Internet e a Lei Carolina Dieckmann são passos importantes. Mas elas ainda precisam ser mais conhecidas, aplicadas e, sobretudo, acompanhadas de investimentos em tecnologia e capacitação.

Referência Bibliográfica:

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Relatórios sobre cibersegurança no Brasil. Disponível em: https://www.anatel.gov.br. Acesso em: 5 abr. 2025.

• EUROPOL. Internet Organised Crime Threat Assessment (IOCTA). Relatório Anual, 2023. Disponível em: https://www.europol.europa.eu

• IBM SECURITY. Cost of a Data Breach Report. 2023. Disponível em: https://www.ibm.com/security/data-breach

• INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. Estudos sobre fraudes digitais. Disponível em: https://www.idec.org.br

• LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Lei nº 13.709, de 14 de