Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

CENTRO UNIVERSITÁRIO PROCESSUS
Prática Extensionista

➢ **PROJETO (2024.1)**

➢ 1. Identificação do Objeto

Atividade Extensionista:

( ) PROGRAMA
(x) PROJETO
( ) CURSO
( ) OFICINA
( ) EVENTO
( ) PRESTAÇÃO DE SERVIÇOS
( ) AÇÃO DE EXTENSÃO SOCIAL

Área Temática: Direito Digital

Linha de Extensão: Conscientização do público alvo acerca da necessidade de proteção ativa de dados pessoais no ambiente digital

Local de implementação (Instituição parceira/conveniada): Defensoria Pública do Distrito Federal - Laboratório Júnior de Inovação e Tecnologia

Título Geral: Crimes Cibernéticos e a Segurança da Informação

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

Curso: Direito

Coordenador de Curso: Adalberto Nogueira Aleixo
Articulador(es)/Orientador(es): Prof. Alberto Carvalho Amaral
Aluno(a)/Equipe:

Nome Completo	Curso / Matrícula
Bernard Benson Costa Santos	Direito
Glênia de Sousa Rocha	Direito
Ires Pimenta Gontijo	Direito

João Carlos Affes de Araújo	Direito
Júlio César Rosendo Duarte	Direito
Letícia Lima Santos de Carvalho	Direito
Marcus Eduardo Miranda Martins	Direito
Maria Eduarda dos Santos Freitas	Direito
Matheus Nascimento Viana	Direito
Nícolas Souza Rodrigues	Direito

3. Desenvolvimento

Apresentação:

O presente projeto versará acerca do tema Crimes Cibernéticos, em razão da importância desse assunto para a sociedade, como um todo. Cada dia mais, o tema tem sido difundido na sociedade, sendo figura frequente em páginas jornalísticas, seja devido ao aumento exponencial nos últimos anos, em consequência do maior acesso da população às mídias eletrônicas, seja em razão da migração dos criminosos do ambiente real para o virtual.

Diante disso, o trabalho se pautará na busca de um melhor conhecimento por parte dos acadêmicos, acerca dos modus operandi dos criminosos e dos principais tipos de golpes e do cyberbullying, com vista a orientar o público-alvo sobre a necessidade de se precaver ativamente, para que não venha ser a próxima vítima.

Fundamentação Teórica:

O aumento de usuários às ferramentas virtuais tem como fatores a evolução da tecnologia e a acessibilidade de maquinários que permitem o acesso e a participação na atividade virtual.

Embora, grande parte dos usufruidores da internet queiram apenas procurar informações, entretenimento, diversão, relacionamento, há um crescente número de ocorrências de crimes no aspecto tecnológico e número de vítimas virtuais

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

A 12ª edição da pesquisa TIC Domicílios (2017), divulgada pelo Comitê Gestor da Internet no Brasil – CGI.br, revela que apesar da desigualdade no Brasil, 36,7 milhões de domicílios (54% do total) possuem acesso à internet.

Já entre a população alvo do projeto, o Comitê Gestor de Internet no Brasil, informou que na faixa etária de 15 a 20 anos, em 2022, o acesso à internet correspondia a aproximadamente 25,1 milhões de pequenos jovens.

Assim, a boa informação sobre como utilizar melhor a internet, para se proteger e evitar ser vítima de cibercrimes é necessária.

Podemos conceituar a segurança da informação como processos e práticas utilizadas com objetivo de proteção da informação contra o acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição. Assim, o usuário deve garantir o bom uso da confidencialidade, integridade, disponibilidade da informação, bem como a autenticidade dos usuários, controle de acesso, criptografia de dados. A correta implementação destas características de segurança ajuda na proteção dos dados.

De acordo com o Indicador de Tentativas de Fraude da Serasa Experian, a quantidade de tentativas de fraudes eletrônicas ocorridas em janeiro de 2023 chegou a 284.198 mil tentativas. Enquanto, uma pesquisa realizada pelo IBGE detectou que um brasileiro é vítima de roubo a cada 17 segundos. A partir dessa comparação, percebe-se que os criminosos virtuais atingem o dobro de vítimas, em um mesmo espaço temporal. De acordo com o Centro de Estudos Estratégicos e Internacionais (CSIS) e a empresa McAfee, no ano de 2018, o crime cibernético custou ao mundo cerca de U$$ 600 bilhões, o correspondente a 0,8% do PIB mundial.

Para Henrique Shneider, CEO da Netfive, a mudança no meio de prática dos crimes demonstra que os criminosos vêm acompanhando os avanços tecnológicos, inclusive aprimorando os tipos de golpes, com vistas a atingir um número maior de vítimas, devendo continuar essa tendência de aumento dos crimes virtuais.

O crescimento vertiginoso dos crimes em ambientes digitais se deu (continua se dando) justamente devido às vulnerabilidades deixadas pelos potenciais vítimas e

detectadas por aqueles ávidos em criar a cilada/armadilha para apossar-se dos bem alheios, que, muitas das vezes, são entregues por pura displicência da vítima.

Assim, as causas recorrentes de vazamento de dados decorrem da própria ação humana, seja por descuido, seja por engodo de terceiros. Logo, devemos precaver, de forma ativa, com a gestão, manipulação, fornecimento e guarda de dados sensíveis, que podem nos expor a crimes cibernéticos, especialmente no que tange a dados de acesso direto a ativos financeiros (contas bancárias, números e códigos de cartões de crédito).

Consoante PINHEIRO, os crimes com maior incidência no ambiente digital são *contaminação por vírus, uso indevido ou não autorizado de senha (qualquer tipo, do e-mail pessoal a do Internet banking), uso indevido de número de cartão de crédito, furto de dados, fraude, falsa identidade ou falsidade ideológica (alguém se passar por outra pessoa), ofensas digitais (em geral tipificadas como crimes contra a honra — difamação, calúnia e injúria, mas tem também a ameaça e a contravenção penal de perturbação da paz do indivíduo que ocorre com cyberbullying em geral). Ele também pode ser envolvido em uso não autorizado de imagem (seja a dele ou ele fazendo uso da de outra pessoa), infração de di-reitos autorais (pirataria e plágio), dano em geral, espionagem eletrônica e todo tipo de vingança digital que pode envolver até apagamento dos seus dados, alteração do seu perfil, sequestro de domínio (em especial no caso das empresas)*. (PINHEIRO, 2021, p. 137).

Por ser um tipo de crime dependente da ação ou inação humana, a melhor forma de se prevenir é justamente por meio da conscientização da população, especialmente a de classes mais baixas. Com esse intuito, pede-se licença à nobre Autora para transcrever suas nove recomendações e canais oficiais das principais mídias sociais para denúncia de incidentes, na íntegra:

➢ Recomendações

1) não abrir arquivos anexados, pois geralmente são programas executáveis que podem causar danos ao computador ou capturar informações confidenciais;

2) não clicar em links para endereços da Internet, mesmo que conste o nome da empresa ou instituição, ou, ainda, mensagens como “clique aqui”;

3) em caso de dúvidas sobre a origem e veracidade de determinada mensagem, procurar excluir o e-mail evitando executar seus anexos ou acessar os links presentes em seu conteúdo;

4) em casos de contaminação por vírus ou outro código malicioso, reformatar a máquina, reinstalar totalmente o sistema operacional e os aplicativos, evitando restaurar backups antigos;

5) evitar baixar aplicativos gratuitos só porque são de graça, buscar referências e recomendações de quem já os utiliza, visto que muitos golpistas têm utilizado aplicativos falsos para contaminar o equipamento do usuário e capturar dados do mesmo;

6) utilizar softwares de proteção (antivírus, antispam, antispyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas;

7) não emprestar sua senha de e-mail, de Internet, de rede da empresa, de cartão de crédito, de conta bancária em hipótese alguma;

8) duvidar do perfil de pessoas que se comunicam em ambientes não seguros e anônimos, como mídias sociais, evitando clicar e abrir imagens, e fazendo a verificação ou confirmação de identidade sempre que possível (se a pessoa é quem diz ser); e

9) registrar a ocorrência na delegacia mais próxima ou na especializada em crimes eletrônicos.

➢ Canais oficiais para denúncia

• Youtube : para denunciar um vídeo impróprio ou que atente contra o direito de alguém, basta acessar https://www.youtube.com/yt/policyandsafety/pt-BR/reporting.html e preencher o formulário específico disponível.

• Twitter: acessar o link https://support.twitter.com/forms/abusiveuser e preencher o formulário disponível.

• Facebook : para denunciar conteúdo abusivo ou spam deve-se usar o botão “Denunciar”, que aparece ao lado do próprio conteúdo, e acessar https://www.facebook.com/help/181495968648557/.

• WhatsApp : quando se recebe uma mensagem inicial de um contato desconhecido, há a opção “Denunciar” como spam e bloquear. Isto fará com que esse usuário seja reportado e o mesmo será adicionado à lista de contatos bloqueados.

• Instagram : para denunciar o conteúdo diretamente pelo aplicativo basta clicar no botão ou funcionalidade que aparece junto com o mesmo. Se não possuir uma conta, deve-se acessar https://help.instagram.com/contact/383679321740945.

Ante todo o exposto, para a efetiva diminuição dos crimes cibernéticos, faz-se necessária a mudança de hábito dos próprios indivíduos, que devem estar atentos e vigilantes, desenvolvendo proativamente uma melhor gestão, manipulação, disponibilização e guarda de dados pessoais utilizados no ambiente digital. Nessa linha, o presente trabalho será de grande valia para a sociedade, uma vez que se propõe à conscientização da população, alertando-a para os principais crimes cibernéticos e as formas de proteger-se contra eles, bem como disponibilizando os canais principais de atendimento em caso de lesão do bem jurídico.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Tema Geral:
Crimes cibernéticos

Tema Específico do Grupo:
Segurança digital entre o grupo de pessoas entre 15 e 20 anos de idade.

Problema verificado:

Crescente número de ocorrências de crimes no aspecto tecnológico e número de vítimas virtuais entre os adolescentes.

Objetivo geral:

Ensinar os alunos do Ensino Médio como implementar boas práticas de segurança virtuais, e a conscientização sobre os riscos dos cibercrimes e como evitá-los.

Objetivos específicos:

- Ministrar palestra na instituição parceira , com a divulgação do tema
- conscientizar os alunos e professores acerca das principais vulnerabilidade a que se expõem nas interações no ambiente digital;
- disponibilizar ao público- alvo os contatos dos principais canais de atendimento em caso de vir a ser vítima de crime cibernéticos

Justificativa:

A escolha do presente tema se deu em razão do aumento de crimes cometidos no ambiente virtual , do desconhecimento da população que existem medidas simples e práticas que são capazes de evitá-los , bem como a importância do meio jurídico , como um todo.

Metas:

- Conscientizar o público-alvo acerca dos principais crimes a que esta sujeito no ambiente digital;
- Orientar o público-alvo sobre a importância de agir de forma proativa, no ambiente virtual
- Levar ao conhecimento da sociedade as principais portas de entrada (vulnerabilidades), para esses crimes; e

- Disponibilizar canais de atendimento dos principais órgãos públicos para denúncias das vítimas;

Hipótese / Resultado esperado:

Após a execução do projeto, espera-se uma mudança comportamental do público alcançado, assim como de familiares e amigos desses participantes, passando-se, assim, a gerir melhor os dados pessoais, de forma ativa, e precavendo-se de possíveis crimes cibernéticos, a partir de um maior conhecimento das principais vulnerabilidades a que estão expostos e das formas de se evitá-las, ou seja, interagindo de forma segura no ambiente digital.

Metodologia:

Quais as ferramentas que você vai utilizar para aplicar seus objetivos específicos.

- Realização de palestras;
- Uso de folders digital;
- Slides;
- Uso de cartilha

Cronograma de execução:

Data de início: 1 de março de 2024

Data de término: 1 de julho de 2024

Evento	Período	Observação
1ª Visita Técnica	12.04.2024	Palestra sobre mediação de conflitos e sobre o funcionamento do espaço Conciliar DPDF-TJDFT-MPDFT.
2ª Visita Técnica	03.05.2024	Os alunos conheceram o Laboratório Júnior de Inovação e Tecnologia da DPDF. Os

		mentores explicaram o funcionamento e os projetos em desenvolvimento.
Apresentação presencial dos projetos de pesquisa para a turma	24.05.2024	Os grupos apresentaram os projetos e as práticas de extensão a serem implementadas junto à comunidade.
Período para implementação das práticas de extensão	25.05 a 01.07.2024	Os grupos devem seguir a previsão do projeto junto à instituição conveniada.

Referência Bibliográfica:

EGGER, Ildemar. Mediação comunitária popular: uma proposta para além da conflitologia. Tese (Doutorado em Direito). Florianópolis: UFSC, 2008. P. 221

FREGAPANI, G. S. B. Formas alternativas de solução de conflitos e a Lei dos Juizados Especiais Cíveis. Revista de Informação Legislativa. Brasília, v. 34, n. 133, p. 99-108, jan. 1197.

Lagrasta, Zafari e Martinelli.
Guilherme, Luiz Fernando do Vale de A. Manual dos MESCs: meios extrajudiciais de solução de conflitos. Disponível em: Minha Biblioteca, Editora Manole, 2016. <https://integrada.minhabiblioteca.com.br/reader/books/9788520461457/pageid/22 > Acesso em : 15.maio.2024

Lagrasta, Valeria F. Inovações Tecnológicas nos Métodos Consensuais de Solução de Conflitos. Disponível em: Minha Biblioteca, Editora Saraiva, 2022. <https://integrada.minhabiblioteca.com.br/reader/books/9786553621992/epubcfi/6/16%5 B%3Bvnd.vst.idref=miolo_3.xhtml%5D!/4> Acesso em : 15 maio.2024

Martinelli, Dante P. Negociação e Solução de Conflitos - Do Impasse ao Ganha-ganha Com o Melhor Estilo. Disponível em: Minha Biblioteca, (2nd edição). Grupo GEN, 2020. <https://integrada.minhabiblioteca.com.br/reader/books/9788597025989/epubcfi/6/24%5 B%3Bvnd.vst.idref=html11%5D!/4/28/2 > Acesso em : 15 maio . 2024
Zaffari, Eduardo, K. e Martha Luciana Scholze. Solução de conflitos jurídicos. Disponível em: Minha Biblioteca, Grupo A <https://integrada.minhabiblioteca.com.br/reader/books/9788595025233/pageid/0> Acesso em : 15 maio. 2024

PINHEIRO, Patrícia Peck. **Direito Digital**. 7ª ed. São Paulo: Saraiva Educação, 2021.Disponível em: Minha Biblioteca, Editora Saraiva, 2019

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

<https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/epubcfi/6/2[%3Bvnd.vst.idref%3Dcapa2-0.xhtml]!/4/2/2%4061:95> Acesso em : 15 maio.2024

Brasil começa 2023 com mais de 284 mil tentativas de fraude de identidade,revela serasa experian. **Site serasaexperian**,2024.Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/brasil-comeca-2023-com-mais-de-284-mil-tentativas-de-fraude-de-identidade-revela-serasa-experian/> Acesso em : 15 de maio . 2024

Cartilha Segurança Digital. **Site do TJDFT, 2021**. Disponível em: <https://www.tjdft.jus.br/publicacoes/edicoes/manuais-e-cartilhas/cartilha_segurancavirtual_22abr2021.pdf> Acesso em: 15 maio.2024