.

INSTITUTO FEDERAL DE MATO GROSSO DO SUL

***CAMPUS* CAMPO GRANDE**

PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

MARLON GLAUBER MARINHO

IMPLICAÇÕES PENAIS DOS CIBERCRIMES:

UM ESTUDO VISANDO APRIMORAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET

Dourados, MS

2024

MARLON GLAUBER MARINHO

Linha de pesquisa: Práticas Educativas em EPT.

Macroprojeto: Práticas Educativas no Currículo Integrado.

IMPLICAÇÕES PENAIS DOS CIBERCRIMES:
UM ESTUDO VISANDO APRIMORAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET

Projeto de Pesquisa apresentado ao Mestrado Profissional em Educação Profissional e Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul como requisito para obtenção do título de Mestre em Educação Profissional e Tecnológica.

Orientador: Danilo Ribeiro de Sá Teles

Dourados, MS

2024

Marinho, Marlon Glauber
M338i Implicações penais dos cibercrimes: um estudo visando aprimorar a formação do técnico em informática para internet. / Marlon Glauber Marinho. – Dourados-MS, 2024.
94 f. : il. ; 29 cm.

Dissertação (Mestrado em Educação Profissional e Tecnológica) – Programa de Pós-Graduação em Educação Profissional e Tecnológica, Instituto Federal de Mato Grosso do Sul-IFMS, Campus Campo Grande, 2024.
Orientador: Danilo Ribeiro de Sá Teles.

Inclui referências.
Inclui apêndices.

1. Técnico em Informática para Internet. 2. Crimes virtuais. 3. Educação Profissional Tecnológica. 3. Podcast Educacional. 4. Segurança da Informação. I. Teles, Danilo Ribeiro de Sá. II. Instituto Federal de Mato Grosso do Sul. Programa de Pós-Graduação em Educação Profissional e Tecnológica. III. Título.

CDD 23. ed. 373.011

Ficha catalográfica elaborada pela Biblioteca do Campus Campo Grande - IFMS
Bibliotecário: Igor Lins Vieira CRB1 – n. 2901

Marinho, Marlon Glauber
M338i Podcast Rastros Virtuais. / Marlon Glauber Marinho. – Dourados-MS, 2024.
8 f. : il. color. ; 29 cm.

Produto Educacional (Mestrado em Educação Profissional e Tecnológica) – Programa de Pós-Graduação em Educação Profissional e Tecnológica, Instituto Federal de Mato Grosso do Sul-IFMS, Campus Campo Grande, 2024.
Orientador: Danilo Ribeiro de Sá Teles.

Inclui ilustrações.
Podcast em 4 episódios.
Acesso ao podcast:
https://open.spotify.com/show/205iShVRJZD1yhgyn7AdHj?si=ca5e6e5c71e649ca&nd=1&dlsi=c467db1528bb4abd

1. Técnico em Informática para Internet. 2. Crimes virtuais. 3. Educação Profissional Tecnológica. 3. Podcast Educacional. 4. Segurança da Informação. I. Teles, Danilo Ribeiro de Sá. II. Instituto Federal de Mato Grosso do Sul. Programa de Pós-Graduação em Educação Profissional e Tecnológica. III. Título.

CDD 23. ed. 373.011

Ficha catalográfica elaborada pela Biblioteca do Campus Campo Grande - IFMS
Bibliotecário: Igor Lins Vieira CRB1 – n. 2901

ATA DE DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO

Mestrado Profissional em Educação Profissional e Tecnológica (ProfEPT/IFMS)

Aos 24 dias do mês de maio do ano de 2024, às 13 horas e 30 minutos, reuniu-se por webconferência a Banca Examinadora composta pelos professores Dr. Danilo Ribeiro de Sá Teles (IFMS), Dr. Ariston de Lima Cardoso (UFRB), Dr. Anderson Martins Corrêa (IFMS) e Dr. Carlos Vinícius da Silva Figueiredo (IFMS), sob a presidência do primeiro, para avaliação do trabalho do estudante Marlon Glauber Marinho, CPF 013.907.331-06, Linha de Pesquisa "Práticas Educativas em Educação Profissional e Tecnológica (EPT)", Curso de Mestrado Profissional em Educação Profissional e Tecnológica, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, apresentado sob o título "IMPLICAÇÕES LEGAIS DE CRIMES CIBERNÉTICOS: UM ESTUDO VISANDO APRIMORAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET " e orientação de Danilo Ribeiro de Sá Teles. O presidente da Banca Examinadora declarou abertos os trabalhos e agradeceu a presença de todos os membros. A seguir, concedeu a palavra ao estudante, que expôs seu Trabalho de Conclusão de Curso. Terminada a exposição, os membros da Banca Examinadora iniciaram as arguições. Terminadas as arguições, o presidente da banca fez suas considerações. A seguir, a Banca Examinadora reuniu-se em grupo virtual à parte para avaliação e emitiu, em seguida, parecer expresso conforme segue:

EXAMINADOR	AVALIAÇÃO
Dr. Danilo Ribeiro de Sá Teles - Orientador	Aprovado
Dr. Ariston de Lima Cardoso (Externo)	Aprovado
Dr. Anderson Martins Corrêa	Aprovado
Dr. Carlos Vinícius da Silva Figueiredo	Aprovado

RESULTADO FINAL:

(x) Aprovação ( ) Reprovação

OBSERVAÇÕES:

Juntamente com a dissertação citada anteriormente foi também validado pela banca avaliadora o produto educacional intitulado "Rastros Virtuais".

Nada mais havendo a ser tratado, o Presidente declarou a sessão encerrada e agradeceu a todos pela participação.

Danilo Ribeiro de Sá Teles
Presidente da Banca Examinadora

Marlon Glauber Marinho
Mestrando

Documento assinado eletronicamente por:

- **Marlon Glauber Marinho**, **TECNICO EM AUDIOVISUAL**, em 24/05/2024 15:39:28.
- **Danilo Ribeiro de Sa Teles**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 28/05/2024 19:30:03.
- **Anderson Martins Correa**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 29/05/2024 11:03:55.
- **Carlos Vinicius da Silva Figueiredo** , **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 07/06/2024 20:53:59.
- **Ariston Lima Cardoso**, **Ariston Lima Cardoso - Membro(a) de banca de mestrado - Universidade Federal do Recôncavo da Bahia - Ufrb (07777800000162)**, em 11/06/2024 12:52:03.

Este documento foi emitido pelo SUAP em 24/05/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifms.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 451372
Código de Autenticação: cef2109004

AGRADECIMENTOS

A realização desta dissertação é resultado de uma jornada de grande aprendizagem e crescimento que não teria sido possível sem o apoio e a colaboração de muitas pessoas e instituições. Gostaria de expressar minha sincera gratidão a todos que, de alguma forma, contribuíram para o sucesso deste estudo:

Em primeiro lugar, expresso minha gratidão ao meu querido orientador, Prof. Dr. Danilo Ribeiro de Sá Teles, pela orientação, paciência e apoio durante todo o processo. Suas valiosas sugestões e ensinamentos foram essenciais para o desenvolvimento deste trabalho. Foi uma honra concluir essa etapa acadêmica ao seu lado.

Aos membros da banca, Prof. Dr. Ariston Lima Cardoso, Prof. Dr. Anderson Martins Correia, Prof. Dr. Carlos Vinícius da Silva Figueiredo e Prof. Dr. Danilo Ribeiro de Sá Teles, meu profundo reconhecimento por dedicarem seu tempo e expertise à avaliação desta dissertação. Agradeço também aos membros do corpo docente do ProfEPT por compartilharem seu conhecimento e seus ensinamentos.

À minha esposa, Elis Seifert, que esteve ao meu lado durante toda a jornada, oferecendo incentivo e apoio constante. Sua compreensão e cuidado com nossa família nos momentos de ausência, foram cruciais para dedicar a minha total atenção a este trabalho. Aos meus familiares e amigos, que sempre me encorajaram e celebraram cada etapa deste caminho.

Ao Professor Jonison Almeida dos Santos e à Policial Francielle Gottardi, cujas colaborações foram inestimáveis para a elaboração do nosso produto educacional.

Ao Prof. Carlos Figueiredo, que sempre apoiou minha formação. Em seu período como Diretor-Geral do *Campus* Dourados, nunca mediu esforços para incentivar o desenvolvimento profissional de sua equipe.

Ao Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul (IFMS) e à Reitora Elaine Cassiano, expresso meu reconhecimento pelo valioso suporte oferecido. O auxílio à capacitação e à implementação do trabalho remoto foram ações cruciais que me ajudaram a concluir esta pesquisa.

A todos, muito obrigado!

RESUMO

Esta pesquisa investigou as implicações penais dos cibercrimes, realçando a formação do Técnico em Informática para Internet no contexto da Educação Profissional e Tecnológica (EPT). O estudo buscou determinar como o ensino sobre as consequências legais dos cibercrimes contribui para a formação do técnico em informática para internet. O objetivo geral foi identificar os crimes virtuais e as consequências legais que os estudantes devem compreender para aprimorar sua capacitação profissional e habilidades cidadãs no ciberespaço. Os objetivos específicos incluíram a identificação das leis brasileiras que regulamentam os ilícitos cibernéticos, a descrição e avaliação da presença do estudo das implicações penais dos cibercrimes na unidade curricular Segurança da Informação do Curso Técnico em Informática para Internet no *Campus* Dourados, bem como em literaturas recomendadas nessa unidade curricular, e a verificação da eficácia do produto educacional elaborado, um podcast educacional, como uma ferramenta suplementar para ampliar o entendimento dos alunos sobre as consequências legais dos cibercrimes. A metodologia adotada foi de abordagem qualitativa, com pesquisa bibliográfica e documental como procedimentos, e os dados foram analisados por meio da técnica de análise de conteúdo. Os resultados indicaram uma evolução significativa no arcabouço jurídico relacionado aos crimes virtuais, também foi observada uma lacuna na abordagem das implicações penais dos cibercrimes nos materiais didáticos analisados. No entanto, o podcast "Rastros Virtuais" foi bem recebido pelos estudantes, demonstrando ser uma ferramenta eficaz para complementar o ensino sobre o tema.

Palavras-chave: Técnico em Informática para Internet; Crimes Virtuais; Educação Profissional Tecnológica; Podcast Educacional; Segurança da Informação.

ABSTRACT

This research investigated the legal implications of cybercrimes, highlighting the learning process of the Internet Computing Technicians within the context of Professional and Technological Education (PTE). The study sought to determine how teaching about the legal consequences of cybercrimes contributes to the learning process of internet computing technicians. The general objective was to identify virtual crimes and the legal consequences that students must understand to enhance their professional skills and civic abilities in cyberspace. Specific objectives included identifying Brazilian laws regulating cybercrimes, describing and evaluating the presence of the study of the legal implications of cybercrimes in the Information Security curriculum of the Internet Computing Technician Course at the Dourados campus, as well as in recommended literature in this curriculum, and verifying the effectiveness of the educational product developed, an educational podcast, as a supplementary tool to enhance students' understanding of the legal consequences of cybercrimes. The methodology adopted was a qualitative approach, with bibliographic and documentary research as procedures, and data were analyzed using content analysis technique. The results indicated a significant evolution in the legal framework related to virtual crimes; however, a gap in the approach to the legal implications of cybercrimes was also observed in the analyzed teaching materials. Nevertheless, the podcast "Virtual Traces" was well received by students, demonstrating to be an effective tool to complement teaching on the subject.

Keywords: Internet Computing Technician; Cybercrimes; Professional and Technological Education; Educational Podcast; Information Security.

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADO - Ação Direta de Inconstitucionalidade por Omissão

CEP – Comitê de Ética na Pesquisa

CSRF - Cross-Site Request Forgery

ECA - Estatuto da Criança e do Adolescente

EJA - Educação de Jovens e Adultos

EPT - Educação Profissional e Tecnológica

GOOGLE FORMS – formulário online de coleta de dados de pesquisa

HTML - HyperText Markup Language (Linguagem de Marcação de Hipertexto)

HTTP - Hyper Text Transfer Protocol (Protocolo de Transferência de Hipertexto)

IFES - Instituto Federal do Espírito Santo

IFMS – Instituto Federal de Mato Grosso do Sul

JAVASCRIPT - Linguagem de programação interpretada

LGPD - Lei Geral de Proteção de Dados Pessoais

MCI - Marco Civil da Internet

PE - Produto Educacional

PPC - Projeto Pedagógico de Curso

SAFERNET - Associação civil

SDH - Secretaria de Direitos Humanos da Presidência da República

SQL - Structured Query Language (Linguagem de Consulta Estruturada)

STF - Supremo Tribunal Federal

TALE - Termo de Assentimento Livre Esclarecido

TCLE – Termo de Consentimento Livre Esclarecido

TI - Tecnologia da Informação

TJMS - Tribunal de Justiça do Estado do Mato Grosso do Sul

TJRS - Tribunal de Justiça do Estado do Rio Grande do Sul

TJDFT - Tribunal de Justiça do Distrito Federal e dos Territórios

TRF3 - Tribunal Regional Federal da 3ª Região

UCSI - Unidade Curricular Segurança da Informação

XSS - Cross-Site Scripting

SUMÁRIO

1. INTRODUÇÃO

A educação é um direito de todos e uma garantia fundamental, assegurada de maneira imutável na lei maior, a Constituição Federal. O Estado tem a obrigação de oferecê-la, devendo, para isso, atender a três objetivos primordiais: o desenvolvimento pessoal, o exercício da cidadania e a qualificação para o trabalho (BRASIL, 1988).

Com base nestes propósitos, a escola precisa atuar para fortalecer o regime democrático, pois, através dele, é possível formar um cidadão capaz de ascender intelectualmente. Neste sentido, "[...] a tendência democrática, intrinsecamente, não pode consistir apenas em que um operário manual se torne qualificado, mas em que cada "cidadão" possa se tornar "governante" e que a sociedade o coloque, ainda que "abstratamente", nas condições gerais de poder tornar-se tal" (GRAMSCI, 2010, p. 123).

Uma modalidade de educação que cumpre os preceitos constitucionais é a Educação Profissional e Tecnológica (EPT). Ela estabelece que a escola deve capacitar o estudante para estar apto a todos os aspectos de sua vida, proporcionando uma formação omnilateral. Ciavatta (2014) ensina que a "educação omnilateral ou formação em todos os aspectos da vida humana – física, intelectual, estética, moral e para o trabalho, integrando a formação geral e a educação profissional" (CIAVATTA, 2014, p. 190-191).

Seguindo estas diretrizes e atendendo uma demanda regional do mundo do trabalho, o Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul (IFMS), através do *Campus* Dourados, oferece o Curso Técnico Integrado em Informática para Internet, tendo como um dos objetivos preparar o estudante para adquirir conhecimentos suficientes para atuar no mundo da tecnologia, tornando-o um profissional mais completo e capacitado (IFMS, 2019).

A formação de um profissional não é uma tarefa simples e a escola deve prepará-lo para inúmeros desafios. O egresso deste curso precisa estar atento, visto que o ambiente virtual pode ser um espaço utilizado para cometimento de crimes. Pinheiro (2021) descreve que a internet é um meio para a prática delituosa e que grande parte dos delitos cometidos no ambiente real são igualmente praticados no virtual. A rede aparece como um facilitador, tendo em vista que os criminosos estão

munidos com a sensação de anonimato, acreditam ser um submundo e que não há leis que os alcancem.

O Estado Brasileiro detém o *jus puniendi*, que, traduzido dos brocardos jurídicos, significa o poder/dever que as autoridades públicas possuem em buscar a justa e proporcional punição à prática criminosa. Um dos ramos do direito destinado a realizar tal persecução é o Direito Penal. Entretanto, ele deve ser utilizado como última alternativa, neste passo, “O princípio da intervenção mínima, ou *ultima ratio*, é o responsável não só pela indicação dos bens de maior relevo que merecem a especial atenção do Direito Penal, mas se presta, também, a fazer com que ocorra a chamada descriminalização” (GRECO, 2017, p. 127).

A EPT se propõe a preparar o estudante para os aspectos da vida humana e o arcabouço doutrinário sustenta que o direito penal deve ser utilizado como última opção para correção de ilícitos. Dessa maneira, o estudo do saber científico presente nas bases da EPT pode ser capaz de franquear ao educando a possibilidade de aproximação com os saberes já testados e comprovados. Estes conhecimentos são construídos através do trabalho educativo, “[...] ato de produzir, direta e intencionalmente, em cada indivíduo singular, a humanidade que é produzida histórica e coletivamente direta e intencionalmente” (SAVIANI, 2003, p. 13). O estudo do direito é visto por parte da sociedade e especificamente pelos estudantes como algo complexo e de difícil entendimento. Desta forma, estes conhecimentos, advindos dos saberes científicos e sistematizados, servirão para elucidá-lo sobre os riscos dos crimes praticados em seu ambiente profissional, bem como fortalecer sua atuação cidadã.

Existem inúmeras definições doutrinárias para conceituar os cibercrimes. Segundo Teixeira (2020), o “crime de informática é aquele que, quando praticado, utiliza-se de meios informáticos como instrumento de alcance ao resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos” (TEIXEIRA, 2020, p. 652). Além disso, é possível distinguir entre crimes próprios virtuais e crimes impróprios virtuais. Os crimes próprios virtuais exigem uma tipificação específica dos sujeitos ativos ou passivos, enquanto os crimes impróprios virtuais envolvem a utilização da internet como meio para cometer um crime, sem necessidade de uma qualificação específica dos sujeitos (GRECO, 2017).

Portanto, os crimes virtuais podem ser praticados de duas maneiras: quando a internet é utilizada como meio para se chegar ao crime, ou quando o tipo penal exige uma qualificação específica que só pode ser praticada através da internet.

Para efetuar o levantamento dos crimes cibernéticos no Brasil, a Safernet (2022), uma associação civil sem fins lucrativos, mantém a Central Nacional de Denúncias de Crimes Cibernéticos em parceria com Ministérios Públicos e a Secretaria de Direitos Humanos da Presidência da República (SDH). O Estado de Mato Grosso Sul, está alinhado com esta instituição e disponibiliza através do site "cidadanialgbt" algumas opções para cadastrar as denúncias dos crimes virtuais, entre elas está o link/telefone da SaferNet (MATO GROSSO DO SUL, 2022).

Os dados e indicadores aqui apresentados são os mais recentes disponibilizados por esta associação. Então, os principais crimes praticados no ambiente virtual em todo o território nacional no ano de 2022 são apresentados na Tabela 1.

Tabela 1 - Principais crimes cibernéticos praticados no Brasil em 2022.

Crime	**Quantidade**
Abuso e exploração sexual infantil na internet (pornografia infantil)	111.929
Misoginia	28.679
Xenofobia	10.686
Apologia a crimes contra a vida	10.384
Racismo	9.259
LGBTFobia	8.136
Maus tratos contra animais	4.250
Intolerância religiosa	4.220
Neonazismo	2.661
Tráfico de pessoas	1.194
Total	191.398

Fonte: elaborado pelo autor com dados da Safernet (2022).

Ao analisar os registros de crimes, fica evidente que os números são preocupantes. Um exemplo disso são os dados relacionados à pornografia infantil, os quais indicam que somente no ano de 2022 foram registrados 111.929 casos em todo o território nacional (SAFERNET, 2022).

O crime de pornografia infantil, previsto no Estatuto da Criança e do Adolescente (Lei n.º 8.069/1990), é indiscutivelmente um dos delitos que mais repulsa e indignação causa na sociedade. Os dispositivos legais que regulam esse crime estão estabelecidos nos artigos 240 e 241 do ECA (GOMES, 2016), os quais contêm uma série de proibições destinadas a proteger as crianças e adolescentes. As penas para esse crime começam com um ano de reclusão e podem chegar a mais de dez anos, levando em conta os agravantes.

Os números dos crimes de ódio também são preocupantes, totalizando aproximadamente 74 mil denúncias, apenas em 2022 (SAFERNET, 2022). Nesse rol estão inseridos a prática de LGBTfobia, misoginia, neonazismo, racismo, xenofobia e a intolerância religiosa.

Os atos de homofobia e de transfobia foram reconhecidos como crimes em junho de 2019 na Ação Direta de Inconstitucionalidade por Omissão (ADO) n.º 26/DF no Supremo Tribunal Federal (STF). A LGBTfobia foi equiparada ao crime de racismo com previsão na Lei n.º 7.716, DE 5 de janeiro de 1989. O Congresso Nacional foi considerado inerte e esta equiparação estará vigente até que uma legislação própria regulamente este tema (STF, 2019).

São inúmeros os crimes que podem ser consumados no ambiente virtual e é pertinente que o futuro Técnico em Informática para Internet reconheça as consequências legais dos ilícitos mais recorrentes em sua profissão. Neste enfoque, foi realizada uma investigação no Projeto Pedagógico de Curso (PPC) - Técnico em Informática para Internet, *campus* Dourados (2019). Nesta análise, verificou-se que o curso não previu em seu PPC uma unidade curricular que ofereça ao aluno uma formação capaz de ensiná-lo a respeito dos cibercrimes e as suas consequências.

O pesquisador se sentiu motivado a explorar este tema devido à sua formação em direito e à falta de estudos sobre o assunto. É relevante traduzir esses conhecimentos em uma linguagem acessível e compartilhá-los com os envolvidos. O objetivo foi criar não apenas uma dissertação, mas também um produto ou recurso educacional que pudesse contribuir de forma significativa para a

compreensão e enfrentamento dos crimes virtuais pela sociedade, ampliando assim o impacto e a utilidade do trabalho.

Por isso, chegou-se à seguinte indagação: em que medida o ensino das consequências legais dos crimes cibernéticos pode enriquecer a formação do profissional técnico em informática para internet? Então, o objetivo desta pesquisa foi identificar os crimes virtuais e as consequências legais que os estudantes devem compreender para aprimorar sua capacitação profissional e habilidades cidadãs no ciberespaço.

Para tanto, buscou-se atender aos seguintes objetivos específicos: identificar no âmbito da legislação penal brasileira as leis que regulamentam os ilícitos cibernéticos; descrever e avaliar a presença do estudo das implicações penais dos cibercrimes na unidade curricular Segurança da Informação, assim como em literaturas recomendadas em sua unidade curricular; verificar se o conteúdo do podcast "Rastros Virtuais" foi efetivo como uma ferramenta adicional para complementar o entendimento dos alunos do Curso Técnico em Informática para Internet sobre as consequências legais dos cibercrimes.

Neste estudo, o foco da pesquisa está no ensino médio integrado, mais especificamente no sexto semestre do Curso Técnico em Informática para Internet, com ênfase na unidade curricular de Segurança da Informação, ministrada no Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul (IFMS), *Campus* Dourados.

A investigação deste trabalho teve por fundamento uma pesquisa de abordagem qualitativa, de natureza aplicada, com os objetivos exploratórios/descritivos, adotando como procedimentos: a pesquisa bibliográfica e documental.

O programa de mestrado trabalha com duas linhas de pesquisa, a saber, Organização e Memórias de Espaços Pedagógicos na Educação Profissional e Tecnológica (EPT) e Práticas Educativas em Educação Profissional e Tecnológica (EPT). Esta pesquisa está inserida nesta última, visto que atua “[...] com foco nas estratégias transversais e interdisciplinares, que possibilitem formação integral e significativa do estudante, sustentados no trabalho como princípio educativo e na pesquisa como princípio pedagógico, em espaços formais e não formais” (IFES, 2018, p. 3).

A pesquisa se insere no Macroprojeto Práticas Educativas no Currículo Integrado, onde a elaboração de um Produto Educacional (PE) é um dos critérios de avaliação da dissertação. Nesse contexto, o PE desenvolvido como decorrência desta dissertação foi um Podcast, intitulado Rastros Virtuais. O seu objetivo foi proporcionar que o estudante aprendesse sobre as implicações legais acerca do cometimento dos crimes cibernéticos descritos na legislação brasileira.

Considerando as definições de espaços formais e não formais conforme Jacobucci (2008), destaca-se que o podcast pode ser considerado um recurso educacional que transcende os limites do espaço formal da escola, podendo ser acessado em diversos ambientes, como em casa, no transporte público, ou em qualquer lugar onde haja conexão com a internet, integrando conceitos de espaços formais e não formais de aprendizagem, ampliando o acesso ao conhecimento sobre as leis relacionadas aos crimes cibernéticos para além da sala de aula.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo abordou a fundamentação teórica utilizada para elaborar a pesquisa, iniciando com reflexões sobre a Educação Profissional e Tecnológica no Brasil (EPT). Ponderou como o saber científico e o conhecimento sistematizado contribuem para a formação profissional e cidadã do estudante. Efetuou uma análise bibliográfica das obras indicadas no PPC do Curso Técnico Integrado em Informática para Internet do IFMS *Campus* Dourados. Realizou um breve histórico do direito digital na legislação pátria e explorou os principais crimes cibernéticos praticados no meio virtual. Por fim, apresentou a ferramenta podcast 'Rastros Virtuais' como um produto educacional desenvolvido como resultado desta pesquisa.

A Educação Profissional e Tecnológica (EPT)

A Educação Profissional e Tecnológica (EPT) é uma categoria educacional prevista na Lei n.º 9.394/1996, regramento que estabelece as diretrizes e bases da educação nacional. Esse dispositivo orienta os rumos da educação nacional, estabelecendo que a Educação Profissional Técnica de Nível Médio, além de oferecer o ensino médio, pode preparar o aluno para trabalhar em profissões técnicas, atuando de forma articulada ou subsequente (Brasil, 1996).

Um dos objetivos a serem alcançados pela EPT é proporcionar ao seu educando uma formação integral. Através dela, se torna possível a construção omnilateral dos sujeitos, integrando as dimensões essenciais da vida: o trabalho, a ciência e a cultura. Entender o trabalho como princípio educativo é assimilar a indissociabilidade entre trabalho, ciência e cultura. O princípio educativo é oposto ao conceito de "aprender fazendo" e diferencia-se da formação para o exercício do trabalho. O objetivo da formação integral é proporcionar que as pessoas compreendam as dinâmicas sócio-produtivas das sociedades modernas, é proporcionar que o profissional seja habilitado para exercer sua profissão de forma crítica e autônoma (RAMOS, 2007).

Ciavatta (2012) realiza uma reflexão sobre a formação integrada ao iniciar apontamentos sobre os conceitos abordados historicamente, discutindo sobre trabalho, ciência e cultura na base do currículo, até chegar aos pressupostos para

uma formação integrada e humanizada. Segundo a autora, é preciso ter um projeto de sociedade, buscando acabar com o dualismo de classes; ter leis que possam criar uma articulação entre o ensino médio de formação geral e a educação profissional; garantir a integração da instituição com os discentes e seus familiares; fomentar a prática da democracia na formação integrada; solidificar a instituição de ensino como um lugar de memória e lutar por garantia de investimentos na educação.

Frigotto (2004) reforça que o ensino médio se relaciona com o mundo do trabalho, a cultura e a ciência, sendo um direito social do cidadão em formação. A criticidade é formada a partir desses fundamentos, objetivando emancipar os educandos, oferecendo ferramentas intelectuais para agir sobre a realidade onde vivem.

O Saber Científico

O saber científico é um dos pilares da EPT e se justifica, considerando que, “a ciência busca organizar e sistematizar o conhecimento do homem e o cientista é um ser preocupado com a veracidade e a comprovação de seu conhecimento” (RIZZATTO, 2017, p. 45). O conhecimento científico diferencia-se do senso comum. Visto que, este é popular, trivial, desorganizado. Enquanto o científico se pauta pela sistematização, coerência e constatação (RIZZATTO, 2017). Complementarmente, “a ciência é compreendida como os conhecimentos produzidos pela humanidade que possibilita o contraditório avanço produtivo” (RAMOS, 2007 - 2008, p. 4).

Um exemplo recente da demonstração do senso comum, ocorreu após o pleito eleitoral de 2022, no qual centenas de pessoas foram para as rodovias brasileiras realizar bloqueios ilegais, entre outras pautas, pediam uma intervenção militar e também publicaram suas ações em suas redes sociais convocando “os cidadãos de bem” para “lutarem pela democracia” (FALCÃO, 2022). Movidas por uma onda gigantesca de desinformações baseadas no senso comum, acreditavam estarem exercendo um direito constitucional, a liberdade de expressão, com previsão legal na Constituição Federal, art. 5, IX: “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença” (BRASIL, 1988).

Entretanto, não há direito absoluto e a liberdade de expressão não pode ser usada para incorrer em práticas criminosas. No exemplo citado, entre outros delitos, poderiam incorrer no crime de abolição violenta do Estado Democrático de Direito, com previsão na Lei n.º 14.197/2021, Art. 359-L: “Tentar, com emprego de violência ou grave ameaça, abolir o Estado Democrático de Direito, impedindo ou restringindo o exercício dos poderes constitucionais”. Ademais, acrescenta-se, nesta análise hipotética, o crime praticado através do meio virtual, com previsão no Código Penal, o Art. 287: “Fazer, publicamente, apologia de fato criminoso ou de autor de crime”.

Por isto que o conhecimento científico é tão essencial no processo de ensino e aprendizagem dentro da EPT, ele possibilita uma evolução intelectual ao cidadão, proporcionando que ele parta do senso comum para um conhecimento concreto, científico. O valor educacional atrelado ao saber científico é imprescindível, por isso a pesquisa preocupou-se em estudar o saber científico que fundamenta o direito digital. A ciência jurídica está alocada no ramo das ciências humanas, ela cuida de investigar e examinar o ordenamento jurídico, tendo como objetivo direcionar a sua atenção para o homem e a sua existência (RIZZATTO, 2017).

Para o futuro profissional técnico em Informática para Internet, este estudo se mostrou necessário, dado que, conforme ensina Ramos (2014), um dos sentidos do trabalho como princípio educativo é capacitar os educandos para exercer de forma autônoma e crítica as profissões. Ou seja, este saber amplia a sua área de conhecimento, além de franquear o acesso a um saber científico e sistematizado inédito em formação, sendo um ensino agregador e essencial para o desempenho laboral, contribuindo para uma atuação crítica e autônoma.

Para o egresso, que opte por não atuar nesta área, esta formação contribuirá para aperfeiçoar a sua cidadania, posto que, “[...] a formação da consciência cidadã nos estudantes possibilita que eles exerçam a cidadania ativa, sabendo exigir o cumprimento de seus assegurados direitos e, também, em contrapartida, que tenham pleno juízo do necessário cumprimento dos seus assentes deveres” (PELLOSO, 2021, p.15). Outrossim, “Não conhecer as leis e seus direitos exprime que o cidadão não tem acesso ao próprio país de forma completa” (ANTEZANA e SKAF, 2017, p. 154).

Ademais, é fundamental que o professor participe do compartilhamento desses saberes, afinal, ao atuar na EPT, ele deve conseguir direcionar a aprendizagem dos alunos, identificando-se como uma liderança cultural. Além disso,

o professor precisa contribuir para a superação da educação bancária, propondo em sua prática docente reflexões críticas, com ênfase em uma mudança cultural e social, não sendo um mero transmissor de conteúdos, deve mediar o ensino e aprendizagem, com vistas a contribuir para a promoção da cidadania do educando, sendo um pensador que problematize e ensine seus alunos a serem líderes intelectuais (ARAUJO, 2010).

O Saber sistematizado

Saviani (2011) ao refletir sobre os objetivos da escola, elucida que este local "é uma instituição cujo papel consiste na socialização do saber sistematizado" (Saviani, 2011, p. 14). Segue ponderando que "não se trata, pois, de qualquer tipo de saber. Portanto, a escola diz respeito ao conhecimento elaborado e não ao conhecimento espontâneo; ao saber sistematizado e não ao saber fragmentado; à cultura erudita e não à cultura popular" (Saviani, 2011, p. 14). O referido autor preocupa-se com o saber científico, com a organização do saber, com o conhecimento fundamentado, testado e comprovado, a escola tem este objetivo, ser um local de partilha desses conhecimentos.

Neste contexto, foi fundamental estudar as ciências jurídicas como um saber sistematizado, apresentando uma contextualização da construção desse conhecimento no Brasil. O estudo do direito se inicia, academicamente, no ano de 1827, com a instituição do curso de ciências jurídicas e sociais, regulamentado pelo Imperador Dom Pedro Primeiro, sendo o primeiro curso instituído no país, após a declaração de independência (Brasil, 1827). O estudo das ciências jurídicas no Brasil era destinado às elites, isto pode ser verificado entre os objetivos da primeira faculdade de direito, a saber, "[...]constituir um corpo de elite social e política para a administração do país, compor um ideário que organizasse o Estado Nacional Republicano […]" (DINIZ, 2022, p.179).

Além disso, a dualidade presente no ensino sempre segregou as classes sociais de forma distinta. Para a classe trabalhadora são destinadas "profissões manuais para as quais se requeria uma formação prática limitada à execução de tarefas mais ou menos delimitadas, dispensando-se o domínio dos respectivos fundamentos teóricos" (SAVIANI, 2007, p.159). Desta forma, para as classes menos abastas sempre houve uma clara discriminação relacionada ao ensino formal. De

outro modo, o ensino para burguesia era destinado para “profissões intelectuais para as quais se requeria domínio teórico amplo a fim de preparar as elites e representantes da classe dirigente para atuar nos diferentes setores da sociedade” (SAVIANI, 2007, p. 159).

Assim, torna-se compreensível que o estudo das ciências jurídicas sempre foi reservado às elites, deixando essa oportunidade inacessível para a classe trabalhadora. Neste ponto, “o dominado não se liberta se ele não vier a dominar aquilo que os dominantes dominam. Então, dominar aquilo que os dominantes dominam é condição de libertação” (SAVIANI, 2000, p. 45).

Possibilitar o compartilhamento de uma parcela, pequena que seja, de um saber historicamente sistematizado e elitizado, é ir ao encontro dos anseios dos alunos, por mais que eles não tenham ciência desta importância. Visto que, ao aduzir sobre os conteúdos escolares, Saviani (2011) ensina que os conhecimentos sistematizados são saberes essenciais produzidos através da história para que o estudante se torne um aluno concreto. O estudante empírico ao deparar-se com este conhecimento pode não demonstrar o desejo de aprendizagem desses conteúdos, mas é fundamental aos anseios do aluno concreto e a escola tem a atribuição de possibilitar ao educando este conhecimento, despertando o interesse do aluno empírico.

Consequentemente, é preciso selecionar os conteúdos que permitiram a evolução do gênero humano até o presente momento histórico. Esses conhecimentos são resultados das contestações da luta de classes (DUARTE, 2016).

Sendo assim, a formação franqueada pela EPT deve pensar na formação do sujeito preparando-o para o mundo, uma formação omnilateral, e o estudo da ciência jurídica, neste contexto, visa capacitar o estudante para o enfrentamento dos desafios em sua profissão e para uma prática cidadã plena. Atendendo, assim, a um dos desígnios da Educação Profissional e Tecnológica, o ensino do saber científico.

Ademais, ao oferecer uma formação adicional sobre um saber sistematizado específico, como o estudo das implicações legais dos crimes cibernéticos, ofertada através do podcast Rastros Virtuais: As Consequências dos Crimes Digitais, será proporcionado ao aluno sincrético, partir de um entendimento difuso/confuso e ao final alcançar um novo entendimento, tornando-se um aluno concreto, capaz de compreender a relevância destes saberes para a sua atuação profissional.

2.1 O Curso Técnico Integrado em Informática para Internet

No Instituto Federal de Mato Grosso do Sul, o curso Técnico em Informática é ofertado em todos os dez campi do Estado. Todavia, o *Campus* Dourados e o *Campus* Naviraí, se diferenciam dos demais, pois na modalidade ensino médio integrado são os únicos voltados para a especificidade Internet, ofertando o Curso Técnico em Informática para Internet. Cabe observar que, apesar do *campus* Jardim também ofertá-lo, este direciona-se para a Educação de Jovens e Adultos (EJA).

Analisando especificamente o *Campus* Dourados, este curso se justifica, dado que o contexto socioeconômico da microrregião da cidade, necessita de profissionais que atuem no setor de tecnologia da informação, particularmente nos ramos de Desenvolvimento de Software e Sistemas de Informação. Os setores industriais, comerciais e de serviços buscam a cada dia profissionais qualificados para ampliar a agilidade e eficácia em seus processos (IFMS, 2019).

Todo curso integrado do IFMS passa pela aprovação de um Projeto Pedagógico de Curso (PPC). Neste sentido, ele foi desenvolvido para "contribuir com a formação de profissionais em Tecnologia da Informação (TI), tendo em vista colaborar com o incremento dos mais variados setores da economia deste Estado" (IFMS, 2019, p.17). O PPC estabelece como objetivo geral do curso:

> Formar integralmente o educando, egresso do ensino fundamental, para o exercício pleno da cidadania e para a atuação no mundo do trabalho, por meio da aquisição de conhecimentos científicos, de saberes culturais e tecnológicos, habilitando-o para o exercício da profissão como técnico em Informática para Internet. (IFMS, 2019, p.19)

Observa-se que o objetivo geral do curso está alinhado com as diretrizes da Educação Profissional e Tecnológica, buscando uma formação integral, enfatizando a atuação cidadã e proporcionando capacitação para a prática profissional.

Desta forma, ao concluir o curso, o Técnico em Informática para Internet estará apto a desenvolver suas habilidades em qualquer instituição, pública ou privada, que necessite de serviços computacionais para internet, amparo técnico, projetos gráficos, além de programar sistemas. Poderá implantar e manter sistemas de informação para internet; diagnosticar problemas e propor soluções fundamentadas em sistemas para internet; aplicar de maneira correta os recursos computacionais (IFMS, 2019).

As habilidades específicas desenvolvidas ao longo da formação incluem: “prestação de serviço de suporte na área de tecnologia da informação; desenho de produtos gráficos para a Web; instalar, configurar e administrar softwares aplicativos e ferramentas de apoio”(IFMS, 2019, p. 22).

O curso é organizado no âmbito curricular, atendendo a formação geral e a formação específica do estudante, compreendendo: “fundamentos científicos, sociais, organizacionais, econômicos, políticos, culturais, ambientais, estéticos e éticos que alicerçam a formação integral, omnilateral” (IFMS, 2019, p. 25). As unidades curriculares voltadas à formação específica deste profissional estão dispostas no PPC 2019 e organizam-se conforme apresentado no Quadro 1.

Quadro 1: Disciplinas específicas do curso Técnico em Informática para Internet.

1º PERÍODO	Ferramentas de desenho; linguagem computacional 1; desenvolvimento front-end 1.
2º PERÍODO	Fundamentos de design web e arquitetura da informação; desenvolvimento front-end 2; linguagem computacional 2; projeto e design web.
3º PERÍODO	Desenvolvimento front-end 3; linguagem computacional 2; fundamentos de projeto de interface gráfica.
4º PERÍODO	Programação server side; análise e projeto de sistemas web 1; banco de dados 1; rede de computadores.
5º PERÍODO	Marketing web; análise e projeto de sistemas web 2; banco de dados 2; frameworks
6º PERÍODO	Segurança da informação; frameworks 2; internet das coisas; banco de dados 3

Fonte: elaborado pelo autor com dados extraídos do Projeto Pedagógico de Curso - 2019.

Ao examinar as unidades curriculares destinadas à formação técnica, nota-se que não há uma disciplina específica que aborde as consequências legais dos crimes cibernéticos. Todavia, a unidade curricular Segurança da Informação, disposta no sexto período deste curso, apresenta alguns tópicos que podem correlacionar os dispositivos de segurança e as condutas criminosas.

2.1.1 Análise da Unidade Curricular: Segurança da Informação

A seguir, foi realizada uma análise bibliográfica sobre as obras indicadas na unidade curricular Segurança da Informação. Esta apreciação foi necessária, sobretudo porque, foi averiguado que esta disciplina é a única que apresenta alguma similaridade com o objeto de estudo desta pesquisa.

Além disso, essa análise é importante para atender a um dos objetivos específicos desta pesquisa, que é descrever detalhadamente as disciplinas presentes na Unidade Curricular do Curso Técnico em Informática para Internet do *Campus* Dourados, especificamente a unidade curricular Segurança da Informação.

Do mesmo modo, esta apreciação se faz necessária, pois, segundo Sacristán (2013), o currículo detém a finalidade de auxiliar na construção da carreira do educando, ele "é uma espécie de ordenação ou partitura que articula os episódios isolados das ações, sem a qual esses ficariam desordenados, isolados entre si ou simplesmente justapostos, provocando uma aprendizagem fragmentada (SACRISTÁN, 2013, p.17)".

O estudo das consequências legais dos crimes virtuais é essencial para o prosseguimento da carreira deste profissional. Este ensino pode ser realizado de maneira articulada e complementar à disciplina Segurança da Informação, evitando assim uma aprendizagem fragmentada, possibilitando uma integração curricular.

O currículo e as unidades curriculares dos cursos técnicos integrados do IFMS são dispostas no Projeto Pedagógico do Curso (PPC) e ao verificar os objetivos a serem alcançados pela ementa da disciplina Segurança da Informação, tem-se:

> Finalidade, importância e objetivo da segurança da informação. Riscos, ameaças e pontos vulneráveis em ambientes computacionais. Incidentes e medidas de Segurança. Políticas de segurança em ambientes computacionais. Conceitos de assinatura e certificação digital. Medidas de segurança no desenvolvimento de sistemas (IFMS,2019).

Pode-se observar que a unidade curricular em questão parece não estar direcionada para abordar as implicações legais dos crimes cibernéticos. Entretanto, para confirmar essa suposição, foi necessário aprofundar a análise da bibliografia básica indicada no PPC.

2.1.2 Discutindo os Livros

Neste segmento, serão exploradas as obras indicadas no Projeto Pedagógico do Curso (PPC), que servem como fundamento para o entendimento da unidade curricular de segurança da informação. A análise inicia-se com a obra ‘Informação, Codificação e Segurança de Redes’ de Alencar (2015), segue com ‘Segurança em Aplicações Web’ de Ferreira (2017) e conclui com ‘Segurança para Desenvolvedores Web, usando JavaScript, HTML e CSS’ de Mueller (2016). Todos esses títulos estão disponíveis no acervo físico da biblioteca do IFMS *Campus* Dourados e foram utilizados como referência para a estruturação do conteúdo discutido.

Livro: Informação, Codificação e Segurança de Redes (Alencar, 2015)

Escrito por Marcelo Sampaio de Alencar em 2015, aborda temas essenciais para estudantes e profissionais de Sistemas de Informação. Com nove capítulos e um apêndice distribuídos em 255 páginas, este livro foca em temas como: medida da informação e entropia; fontes de informação; códigos usuais; fundamentos para o cálculo da capacidade de canais de comunicações; espalhamento espectral; conceitos fundamentais dos códigos corretores de erros; códigos convolucionais; princípio e a abordagem matemática da criptografia; criptografia em redes; alternativas para prevenir ataques e os protocolos de segurança (ALENCAR, 2015).

Após uma apreciação cuidadosa desta obra, destacamos o capítulo nove - Segurança de Redes. Ele aborda conceitos relacionados à criptografia aplicada a redes de computadores, destacando os fundamentos da segurança da informação. As potenciais vulnerabilidades de redes no qual explica os pontos vulneráveis e pondera as ações a serem tomadas para fortalecer a proteção da rede. Relata a habilidade de um espião e como ele pode monitorar a rede, pegar as informações para posteriormente modificá-la, mascarando a sua identidade, redirecionando ou até apagando os dados (ALENCAR, 2015).

De maneira resumida, o capítulo nove trata dos fundamentos da segurança da informação, especificando as potenciais vulnerabilidades das redes. Destacando as estratégias que um hacker pode utilizar, quais os tipos de ameaças e as alternativas para proteção dos ataques a redes de computadores (ALENCAR, 2015).

Desta forma, o livro atende aos objetivos a serem alcançados pela ementa do curso, escrito com uma linguagem técnica e formal, um estudante de outra área poderá ter muitas dificuldades para compreendê-lo, por isto, é um livro direcionado ao seu público-alvo. Todavia, constata-se que apesar do autor apresentar citações para explicar a aplicação dos dispositivos de segurança e mecanismos de defesas a serem adotados pelo profissional, ele não aborda os cibercrimes de maneira aprofundada, não discutindo as implicações e responsabilidades sobre a prática desses crimes.

Livro: Segurança em Aplicações Web (Ferreira, 2017)

Escrito por Rodrigo da Silva Ferreira Caneppele em 2017, é voltado para desenvolvedores web e aborda mecanismos de segurança para prevenir ataques relacionados às vulnerabilidades presentes em aplicações web. Com 11 capítulos distribuídos em 156 páginas.

O público-alvo desta obra são os desenvolvedores Web, com conhecimentos básicos em Banco de Dados, protocolo HTTP e nas linguagens SQL, HTML e JavaScript, tendo por propósito ensinar mecanismos de segurança para prevenir ataques relacionados às vulnerabilidades presentes na própria aplicação. Expõe detalhadamente como os ataques acontecem, como verificar se a aplicações estão desprotegidas e como proceder para corrigi-las.

O autor aborda, separadamente em cada capítulo, um tipo de ataque. Na fase introdutória dos capítulos ele traz uma reflexão relacionando os riscos dos ataques com as inseguranças das pessoas, apresentando exemplos do cotidiano, além de trazer casos reais de ataques que ocorreram ao redor do mundo. Em seguida, expõe as vulnerabilidades, como os ataques funcionam, mecanismos de proteção/defesa e conclui relembrando o que foi estudado. Aborda os ataques como: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Session Hijacking, etc (FERREIRA, 2017).

Em síntese, este livro também cumpre os objetivos a serem alcançados pela ementa do curso, apresenta-se com uma linguagem acessível e uma didática instrutiva. Apesar da obra ser destinada ao seu público, é possível que qualquer leitor compreenda a sua essência. Logo, para o futuro Técnico em Informática para Internet o aprendizado de seu conteúdo é crucial, por abordar inúmeros tipos de ataques hacker e os mecanismos de proteção e defesa contra essas invasões.

Porém, apesar de explicá-los detalhadamente, também não instrui sobre as consequências legais da prática desses crimes.

Livro: Segurança para Desenvolvedores Web, usando JavaScript, HTML e CSS (MUELLER, 2016)

Escrito por John Paul Mueller e traduzido para o português em 2016, é uma obra abrangente que oferece instruções e ferramentas para solucionar problemas de segurança em aplicações web. Com 17 capítulos distribuídos em 412 páginas,

Este livro apresenta instruções e ferramentas necessárias para solucionar problemas de segurança de aplicações web, a despeito de onde elas sejam executadas, celulares, desktops, etc. Indicado para os profissionais como web designer, desenvolvedor de frontend, designer de UI, diretor de arte, engenheiro de software, analista de sistemas e todos os profissionais que já criaram aplicações web em algum momento. A obra estima que o leitor tenha um conhecimento prévio sobre ameaças à segurança e foca em como vencer as ameaças mais recentes, além de demonstrar muitos exemplos de programação, requerendo do leitor conhecimentos sedimentados sobre CSS3, HTML5 e JavaScript (MUELLER, 2016).

O livro apresenta instruções de como criar um plano de segurança para empresa, especificando as ameaças às aplicações web e como proceder para detectá-las. Orienta como planejar senhas, utilizando frases-senhas, biometria, cartões-chave e estratégia de token. Traz estratégias atuais de testes de segurança nas aplicações e como atualizar os mecanismos de segurança, ensinando a realizar o monitoramento dessas ameaças (MUELLER, 2016).

O capítulo 9 - Pensando como um hacker, apresenta as fontes mais comuns de brechas de segurança. Instruí como evitar os ataques mais comuns, como a injeção de SQL, Cross-Site Scripting, etc. O capítulo 16 - Monitorando as ameaças de segurança atuais, foca em orientações, ensina como prever situações e como criar um plano para updates baseado em ameaças, por fim, sugere a leitura de artigos de especialistas para que o profissional se mantenha atualizado (MUELLER, 2016).

Em suma, o livro é muito completo, abordando temas e invasões como Ransomware 1, vírus, ataques DDos, ataques man-in-the-middle e as brechas de segurança. A linguagem é técnica, destinada ao seu público, porém atual, com um

pouco de esforço é possível compreendê-la. Porém, assim como os demais livros, não traz nenhuma página sobre as repercussões legais da prática desses ilícitos.

2.1.3 Considerações bibliográficas

Preliminarmente, para uma melhor visualização dos livros analisados, apresenta-se um comparativo, quadro 2, indicando os títulos dos livros e os capítulos descritos em seus sumários. Esta visualização é importante para notar quais temas são abordados nestas literaturas.

Quadro 2: Comparativo dos títulos e capítulos dos livros analisados

LIVRO	**LIVRO**	**LIVRO**
INFORMAÇÃO, CODIFICAÇÃO E SEGURANÇA DE REDES	SEGURANÇA EM APLICAÇÕES WEB	SEGURANÇA PARA DESENVOLVIMENTO WEB, USANDO JAVASCRIPT, HTML E CSS
CAPÍTULOS	**CAPÍTULOS**	**CAPÍTULOS**
1.Teoria da Informação	1. O velho e conhecido SQL Injection	1. Definindo o ambiente da aplicação
2. Fontes de Informação	2. Cross-Site Scripting is my hero!	2. Acolhendo as necessidades e expectativas dos usuários
3. Codificação de Fonte	3. Cross-Site Request Forgery	3. Obtendo assistência de terceiros
4. Informações e Capacidade de Canais	4. Mass Assignment Attack	4. Desenvolvendo interfaces bem-sucedidas
5. Informações e Capacidade de Canais	5. Session Hijacking	5. Implementando um código confiável
6. Códigos Corretores de Erros	6. Exposição de dados sensíveis	6. Incorporando bibliotecas
7. Códigos Convolucionais	7. Redirects não validados	7. Usando APIs com cuidado
8. Criptografia	8. Outras vulnerabilidades	8. Considerando o uso de microsserviços
9. Segurança de Redes	9. Content Security Policy	9. Pensando como um hacker
Apêndice A Teoria de Probabilidades	10. Subresource Integrity	10. Criando uma zona de segurança para APIs
----------	11. Conclusão	11. Verificando se há brechas

		de segurança em bibliotecas e APIs
----------	----------	12. Usando empresas terceirizadas de testes
----------	----------	13. Definindo claramente os ciclos de upgrade
----------	----------	14. Considerando as opções de update
----------	----------	15. Considerando a necessidade de relatórios
----------	----------	16. Monitorando as ameaças de segurança
----------	----------	17. Proporcionando treinamento necessário

Fonte: o autor, dados extraídos dos livros.

O exame das três literaturas indicadas, "Informação, Codificação e Segurança de Redes", "Segurança em Aplicações Web" e "Segurança para Desenvolvedores Web", permitiu constatar que em mais de suas 800 páginas, nenhuma delas focou em abordar a ilegalidade dos ilícitos cibernéticos. Esses livros, no entanto, evidenciam a discussão sobre os mecanismos de segurança da informação.

Os livros apresentam alguns tópicos como "pensando como hacker", "invadindo aplicações", "brechas de segurança", etc. Na visão apresentada nestas obras, para lidar com a prevenção dos crimes, o profissional precisa aprender como um hacker executa suas ações. Este método de ensino é muito replicado, entretanto, é fundamental elucidar os educandos das implicações legais. Caso alguém opte por cruzar a fronteira da legalidade, é essencial que esteja ciente dos riscos legais de suas ações.

Em consonância com essa ideia, será apresentado no próximo tópico, "O Direito Digital", um histórico da evolução do direito virtual no Brasil, bem como os crimes mais recorrentes e suas implicações legais.

2.3 O Direito Digital

O arcabouço jurídico sobre os crimes virtuais foi se construindo e se solidificando com o passar dos anos. A doutrina jurídica considera que a regulamentação do direito digital se deu legalmente no Brasil com a promulgação da Lei n.º 12.737/2012. Este regramento estabelece a tipificação para alguns delitos informáticos e altera alguns artigos do Código Penal. Esta inovação foi considerada uma resposta do Estado às ações dos infratores que, até então, se aproveitavam de lacunas legais.

Um exemplo de um crime que não detinha uma tipificação penal específica era o delito de cópia indevida de dados ou informações, que, até a aprovação desta lei, não era enquadrado corretamente, ocasionando assim grandes embates jurídicos. Contudo, o processo de atualização do Código Penal foi avançado, quando um acontecimento envolvendo Carolina Dieckmann, atriz da Rede Globo, repercutiu em escala nacional. A artista sofreu uma violação de privacidade com o acesso não autorizado e divulgação de 36 imagens íntimas que estavam armazenadas em seu computador pessoal. Esse incidente impulsionou avanços significativos na legislação de proteção de dados. O dispositivo legal foi aprovado, ficando conhecido como Lei Carolina Dieckmann (GOMES, 2016).

Em maio de 2021, o Código Penal foi alterado novamente através da lei n.º 14.155/21. Esta atualização entrou em vigor “para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet” (BRASIL, 2021).

No ano de 2014, foi sancionada a Lei n.º 12.965/14, regramento que estabeleceu os princípios, as garantias, os direitos e os deveres para quem utiliza a internet no Brasil, o chamado Marco Civil da Internet (MCI). Brandão (2019) assenta que esta lei tem um caráter civil, visto que não focou em uma linha criminalizadora do uso da internet, sendo considerada uma referência global e elogiada por inúmeros países por seu conteúdo e, principalmente, pelo amplo processo de discussão com a sociedade civil que originou sua elaboração.

As evoluções legislativas, alterações/elaborações de leis, por vezes são morosas, acredita-se, em virtude dos trâmites legislativos que precisam ser seguidos. Por isso, a legislação vem, na maioria das vezes, após as atualizações esperadas pela sociedade.

Em agosto de 2018, foi sancionada a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que altera o MCI. Esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, aspirando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Em 2023, no dia 12 de abril, a Presidência da República promulgou o Decreto 11.491/2023. A presente Convenção é considerada necessária para prevenir ações que ameacem a confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados, além de combater o abuso desses sistemas, redes e dados. Ela propõe a criminalização de tais condutas, estabelece competências para lidar com esses crimes de forma eficaz, facilita a descoberta, investigação e julgamento dessas infrações, tanto em níveis nacionais quanto internacionais, e estabelece mecanismos para uma cooperação internacional rápida e confiável. (BRASIL, 2023, preâmbulo).

Após a promulgação, é responsabilidade do Brasil desenvolver novas medidas para a tipificação dos crimes virtuais. Esta iniciativa se alinha com as progressões legislativas pelas quais o país tem passado. Espera-se que futuras atualizações estejam conforme o tratado internacional, potencialmente contribuindo para a harmonização das normas em escala global. Tendo em vista a evolução legislativa dos crimes digitais, a discussão passará a abordar os ataques cibernéticos mais recorrentes.

2.3.1 Os Ataques cibernéticos mais recorrentes

Segundo o site da Microsoft (2023), os ataques virtuais visam causar danos ou obter acesso a documentos e sistemas relevantes, tanto pessoais quanto comerciais. Os ataques cibernéticos mais comuns incluem Malware, Ataque de DDoS (ataque de negação de serviço), Phishing, Ataques de injeção de SQL, Cross-site scripting (XSS), Botnets e Ransomware. A seguir, esses ataques serão contextualizados de forma resumida.

O termo "*Malware*" abrange uma ampla gama de programas destinados a realizar atividades prejudiciais em sistemas computacionais. Dentre os exemplos de

códigos maliciosos estão vírus, worms, bots, cavalos de tróia, rootkits, entre outros (PINHEIRO, 2021).

De acordo com Teixeira (2020), os trojans são conhecidos como cavalos de Tróia ou backdoors, sendo programas enviados a um sistema alvo que possibilitam que o computador infectado se conecte ao computador do invasor sem a necessidade de autorização prévia.

O ataque DDoS é operacionalizado da seguinte forma: em um cenário desse tipo, um conjunto de computadores designados como mestres recebe uma instrução. Esses mestres têm controle sobre uma rede de computadores "zumbis", que são principalmente computadores domésticos infectados por vírus. Todos esses computadores acessam um site ao mesmo tempo, conforme ordenado (TEIXEIRA, 2020).

O Phishing é descrito como uma "mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros" (PINHEIRO, 2021, p. 370). Um relatório recente da Kaspersky revelou que um em cada cinco usuários da internet no Brasil foi alvo de pelo menos uma tentativa de ataque de phishing em 2020 (RODRIGUES, 2021).

O ataque do tipo SQL injection, segundo Ferreira (2017), está entre os dez mais realizados no meio informático. Sua execução não é considerada uma tarefa complicada; ao contrário, resume-se a digitar comandos SQL nos campos de entrada de formulários da aplicação, não exigindo conhecimentos técnicos avançados por parte do invasor. Essas ações podem ser utilizadas, entre outras coisas, para apagar todos os registros de aplicação, manipular um banco de dados ou obter informações dos usuários, como dados de cartões de crédito.

Segundo Ferreira (2017), o ataque XSS assemelha-se ao ataque SQL Injection, porquanto exploram a mesma vulnerabilidade: o tratamento incorreto das informações digitadas pelos usuários. O objetivo dessa ação é enviar comandos em JavaScript com o objetivo de enganar o usuário, levando-o a fornecer suas informações pessoais, realizar ações sem perceber ou ser redirecionado para aplicações fraudulentas.

O termo "*botnets*" advém da união das palavras "robot" (robô) e "network" (rede). Isso ocorre quando vários computadores, geralmente em uma rede privada,

são infectados por vírus e outros tipos de software malicioso, como mensagens pop-up ou spam (MICROSOFT, 2023).

O ataque ransomware é um tipo de software malicioso que ameaça uma vítima bloqueando o acesso a dados críticos ou sistemas até que um resgate seja pago (MICROSOFT, 2023).

Existem outros tipos de ataques que podem ser realizados no meio informático, mas esses exemplos demonstram como os invasores podem articular vários desses ataques/ferramentas para praticar crimes cibernéticos. Após a discussão sobre os ataques cibernéticos mais recorrentes, será iniciado o estudo dos crimes digitais que ocorrem em decorrência do uso dessas ferramentas.

2.3.2 Crimes Virtuais

Os crimes virtuais próprios estão dispostos tanto no Código Penal quanto em leis esparsas. Esses crimes exigem uma tipificação específica dos sujeitos ativos ou passivos. Por outro lado, o crime impróprio virtual é aquele em que a internet é utilizada como meio para cometer o crime, não exigindo uma qualificação específica dos sujeitos (GRECO, 2017).

Portanto, os cibercrimes podem ser cometidos de duas maneiras: primeiro, quando a internet é utilizada como meio (sendo considerado ilícito mesmo fora dela) para se chegar ao crime; segundo, quando o tipo penal exige uma qualificação específica (somente podendo ser praticado através da internet). A seguir, será apresentado um compêndio desses delitos próprios dispostos no ordenamento jurídico pátrio.

A Invasão de Dispositivo Informático, já mencionada anteriormente, requer uma análise detalhada. O tipo penal está previsto no artigo Art. 154-A do Código Penal, com o objetivo de "obter, adulterar ou destruir dados, ou informações sem autorização expressa, ou tácita do usuário do dispositivo, ou de instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2021). Recentemente, com a última alteração legislativa, este crime teve sua pena agravada, passando para "Reclusão, de um a quatro anos, e multa" (BRASIL, 2021).

Além disso, responde por este crime "quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir tais condutas" (BRASIL, 2021). Cabe acrescentar que o tipo penal previu alguns

agravantes, como por exemplo, se da invasão resultar prejuízo econômico, se resultar na obtenção de conteúdo de comunicações eletrônicas privadas, se a invasão objetivar segredos comerciais ou industriais, ou se os crimes foram praticados contra Presidente da República, governadores e prefeitos.

Existem centenas de exemplos de condenações a hackers que tentam praticar este crime. Por exemplo, a assessoria de comunicação social do Tribunal Regional Federal da 3ª Região publicou uma nota em dezembro de 2021, onde a Justiça Federal "(...) condenou, por falsificação de documento público e invasão de dispositivo informático, dois homens acusados de tentar invadir, entre os meses de janeiro e fevereiro deste ano, sistemas eletrônicos utilizados pela Justiça Federal da 3ª Região" (TRF3, 2023). A pena de um dos réus passou de nove anos de prisão, iniciando o cumprimento de pena em regime fechado.

A Interrupção ou perturbação de Serviço Informático/Telemático é prevista no art. 266 do Código Penal, incorrendo neste delito quem "Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa" (BRASIL, 2012). Além disso, equipara as mesmas penas do artigo, "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (BRASIL, 2012). Penalizando em dobro quem praticar a conduta por conjuntura de calamidade pública. Essa tipificação "Trata-se de verdadeira punição por ataques DoS (Denial of Service) praticados em face de sites públicos, algo que se tornou muito comum no Brasil, principalmente como forma de protesto por grupos de hacktivistas" (GOMES, 2016, p.155).

O Estelionato Digital ou Fraude Eletrônica é um desdobramento do crime previsto no art.171 do Código Penal, que se caracteriza por causar prejuízo alheio, obtendo vantagens ilícitas, enganando a vítima. Com o avanço tecnológico, evoluiu também as práticas ilícitas nesses ambientes, forçando o legislador a criar um novo tipo penal. Desta forma, este crime é praticado no momento em que o "criminoso consegue enganar alguém, por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como, senhas de acesso, bancos ou número de cartão de crédito ou débito" (TJDFT, 2021).

A tipificação prevista no Art.171, parágrafo segundo, que "a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro

induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo" (BRASIL, 2021). Estipula uma pena partindo de quatro anos de reclusão e podendo chegar a oito, além da multa. Ademais, pode ser agravada se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e/ou se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

O Furto Mediante Fraude Eletrônica também é uma inovação recente. Com a previsão no Art. 155, parágrafo quarto-b do Código Penal, é descrito como aquele praticado "por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo" (BRASIL, 2021). O sujeito ativo do crime estará sujeito a uma pena de reclusão, de quatro a oito anos, e multa. Assim como no estelionato digital, a pena é agravada se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e/ou se o crime é praticado contra idoso ou vulnerável.

Conforme mencionado por Pinheiro (2021), este delito está se tornando cada vez mais comum, especialmente no que concerne à prática de furto mediante fraude, na qual ocorre o envio de e-mails falsos *(phishing*) para os usuários. Isso resulta na captura de dados de suas contas bancárias por meio da instalação de arquivos maliciosos em seus dispositivos.

A inserção de dados falsos em sistemas de informações é uma prática criminalizada pelo Art. 313-A do Código Penal. Este dispositivo legal abrange a ação de inserir ou facilitar, por parte de funcionários autorizados, a inclusão de informações falsas, assim como a modificação ou eliminação indevida de dados corretos nos sistemas informatizados ou bancos de dados sob responsabilidade da Administração Pública. Aqueles que cometem essa conduta geralmente têm a intenção de obter vantagem indevida ou causar danos. A penalidade estabelecida para essa infração é a reclusão, com duração variando de dois a doze anos, além da imposição de multa (BRASIL, 2000). Este ato ilícito é caracterizado pelos seguintes elementos: a ação de inserir ou facilitar, por parte do funcionário público, a inclusão de dados falsos; e a modificação ou exclusão indevida de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública (GRECO, 2017). Acrescenta que o agente deve estar "atuando, sempre, com a

finalidade especial de obter vantagem indevida para si ou para outrem ou para causar dano" (GRECO, 2017, p. 769).

A modificação ou alteração não autorizada de sistemas de informações está prevista no Art. 313-B do Código Penal. A conduta se consuma quando "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de três meses a dois anos, e multa" (BRASIL, 2000). Além disso, agrava-se a pena se a modificação resultar dano para a Administração Pública ou para o administrado. Greco (2017) esclarece que, para que se configure o delito em questão, é necessário que o ato seja cometido por um indivíduo no exercício de uma função pública. Outra observação enriquecedora deste autor refere-se aos alvos da conduta:"Os objetos materiais das condutas praticadas são o sistema de informações ou programa de informática. Por sistema de informações podemos entender o sistema que manipula informações por meio do uso de banco de dados; programa de informática é o software" (GRECO, 2017, p. 775).

A clonagem/falsificação de cartão de crédito e débito está disposta no Art. 298 do Código Penal, prevendo uma pena de reclusão, de um a cinco anos, e multa. O tipo equipara-se a documento particular, o cartão de crédito ou débito e penaliza quem "Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro" (BRASIL, 2021). Logo, "o legislador brasileiro optou por tipificar tal conduta, que anteriormente era tratada como crime informático impróprio, sustentado pelo artigo 155 do Código Penal (Furto). Neste caso, a clonagem do cartão fica equiparada à falsificação de documento particular" (GOMES, 2016, p.155).

Existe alguma divergência doutrinária a respeito do enquadramento dos crimes próprios. Alguns juristas defendem a inserção de mais crimes nesse rol; todavia, esta é uma discussão jurídica e acadêmica que, na prática, não influi na penalização dos atos praticados.

Com vistas a complementar este estudo, neste momento, serão apresentados alguns crimes que podem ser cometidos utilizando o ambiente virtual como meio para se chegar à prática criminosa, os crimes impróprios.

Estupro por meio virtual de vulnerável. O crime de estupro está disposto no art. 217-A do Código Penal: “Ter conjunção carnal ou praticar outro ato libidinoso

com menor de 14 (catorze) anos: Pena - reclusão, de 8 (oito) a 15 (quinze) anos" (BRASIL, 2009).

Embora o termo "estupro por meio virtual de vulnerável" não esteja especificamente previsto na norma jurídica, esse enquadramento penal decorre da interpretação dos magistrados, tanto em primeira instância quanto nos Tribunais Regionais. Segundo informações do site do TJMS (2023), o Estado de Mato Grosso do Sul registrou sua primeira condenação por estupro virtual. Na sentença proferida, o juiz condenou um homem a uma pena de 13 anos e 24 dias de reclusão, em regime inicial fechado.

Conforme relatado, o magistrado, ao proferir a sentença, observou que, por meio da internet, o réu chantageava a vítima, uma menor de 14 anos, exigindo fotos de suas partes íntimas e ordenando que praticasse atos libidinosos para satisfazê-lo, destacando-se a introdução de objeto na vagina (TJMS, 2023). Adicionalmente, uma decisão semelhante foi confirmada pela 8ª Câmara Criminal do TJRS, na qual um estudante de medicina foi condenado a 12 anos, 9 meses e 20 dias de reclusão por estupro virtual contra uma criança de 10 anos (TJMS, 2023).

A expressão "*Ciberbullying*" refere-se a uma forma específica de bullying praticada através de meios digitais. A Lei n.º 13.185 de 2015, instituiu o Programa de Combate à Intimidação Sistemática (*Bullying*), definindo-o em seu artigo 2º como uma prática que envolve "violência física ou psicológica em atos de intimidação, humilhação ou discriminação" (BRASIL, 2015). Essa intimidação pode ocorrer de diversas formas, como verbal, moral, sexual, social, psicológica, física, material e até mesmo virtual, incluindo ações como depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social (BRASIL, 2015).

No contexto penal, a prática do ciberbullying pode desencadear uma série de crimes. A seguir, será apresentado um quadro com alguns dos crimes que podem ocorrer em decorrência do ciberbullying.

Quadro 3 : Crimes que podem ser cometidos através do ciberbullying

Crime	**Conduta**	**Pena**
Difamação (art.139, CP)	Imputar algo ofensivo à	Pena - detenção, de três

	reputação de outrem.	meses a um ano, e multa.
Calúnia (art.138, CP)	Dizer de forma mentirosa que alguém cometeu crime. Propagar/Divulgar sabendo ser falsa a imputação.	Pena - detenção, de seis meses a dois anos, e multa.
Incitação ao crime (art.286,CP)	Incitar, publicamente, a prática de crime	Pena - detenção, de três a seis meses, ou multa.
Ameaça (art.147,CP)	Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.	Pena - detenção, de um a seis meses, ou multa.
Injúria (art.140, CP)	Ofender a dignidade ou o decoro.	Pena - detenção, de um a seis meses, ou multa.
Constrangimento Ilegal (art. 146, CP)	Constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda:	Pena - detenção, de três meses a um ano, ou multa.
Falsa identidade (art.307, CP)	Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:	Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.
Racismo (art. 20, lei n.º 7.716/89)	Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.	Pena: reclusão de um a três anos e multa.

Apologia do Nazismo (parágrafo 1º do art. 20, lei n.º 7.716/89)	Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.	Pena: reclusão de dois a cinco anos e multa.

Fonte: o autor.

A discussão realizada neste tópico possibilitou inferir que uma pessoa que faz uso diário das tecnologias da informação, tanto no trabalho quanto no cotidiano, deve estar atenta, não deixando de se preocupar com os riscos e as vulnerabilidades que essas ferramentas apresentam.

Foi possível apresentar as evoluções legislativas que regulamentam a internet e, de maneira mais específica, os crimes virtuais. Este percurso teve início na primeira lei aprovada no Brasil em 2012, a chamada "Lei Carolina Dieckmann", e foi até a última atualização nesse âmbito, com a promulgação do Decreto que ratificou a Convenção Internacional sobre o Crime Cibernético.

Os exemplos de ataques virtuais mencionados no texto dão uma noção clara de como o usuário está exposto na sua relação com o ciberespaço. São invasões que executam ações maliciosas nos aplicativos, roubam informações financeiras e instalam programas que capturam tudo que se passa em seu computador ou celular. Portanto, a preocupação e os cuidados devem ser constantes.

Além disso, foi possível acompanhar na legislação brasileira os crimes próprios e alguns crimes impróprios. O profissional da tecnologia que usa suas habilidades para cometer ilícitos ou o curioso que escolhe se envolver no mundo obscuro da criminalidade virtual poderá ser penalizado.

2.4 Produto Educacional

Esta seção apresenta o podcast como a ferramenta escolhida para o desenvolvimento do Produto Educacional. Visto que a sua elaboração é requisito do programa: “O Trabalho de Conclusão de Curso a ser defendido deverá contemplar

o produto educacional, bem como o relatório de pesquisa em forma de dissertação, de acordo com o regulamento local de cada IA" (IFES, 2018, p. 7).

Optou-se pela sua utilização, pois está em linha as possibilidades apresentadas Capes, visto que os Produtos Educacionais podem constituir-se em vídeos, áudios, páginas de internet, aplicativos, manuais, guias, jogos, entre outros, objetivando a sua utilização por parte dos docentes e demais profissionais envolvidos no ensino (CAPES, 2019).

2.4.1 Podcast como recurso pedagógico

O podcast é uma ferramenta que vem se mostrando cada vez mais popular. No Brasil, houve uma explosão de podcasters, principalmente após o início do período pandêmico, março de 2019. Na recente campanha eleitoral de 2022, por exemplo, viu-se uma gigantesca atenção emanada até mesmo dos presidenciáveis a estes programas.

Nuzum (2020) explica que a definição deste formato é a distribuição de arquivos de áudio em um feed *Really Simple Syndication* (RSS), contendo informações e metadados. É importante que a distribuição seja vista não como uma tecnologia, mas sim como um produto que crie experiências de áudio e que siga os receptores de sua programação ao longo de suas vidas, seja qual for a plataforma onde os conteúdos estejam disponibilizados.

Os podcasts podem dividir-se em quatro categorias. 1) Expositivo/Informativo: podendo ser um resumo, um artigo, um poema, descrição do funcionamento de ferramentas, etc. 2) Feedback/Comentários: são comentários aos trabalhos efetuados pelos alunos, explicitados pelos docentes. A ferramenta deve buscar uma construção de conhecimentos, além de propor alternativas. 3) Instruções/Orientações: Instruir para realizar trabalhos práticos, orientar estudos, etc. 4) Materiais autênticos: destinados ao público, não específicos para os estudantes (CARVALHO; AGUIAR, 2009).

Momesso et al. (2016) sugerem passos para elaboração de um podcast, iniciando com a pauta que serve como guia inicial para o próximo episódio, onde são apresentados tópicos de importância que serão debatidos pelo grupo de produção. Os temas serão investigados com fontes apropriadas, seguido pela

análise crítica desses assuntos e, por fim, a escolha do que terá prioridade e a forma mais adequada de apresentá-los.

O script constitui o conteúdo a ser articulado pelo locutor, no qual se encontram elementos característicos da linguagem radiofônica. Está centrada na palavra, na música, nos efeitos sonoros e no uso do silêncio, incorpora também técnicas destinadas a assegurar uma comunicação clara, tais como a exclusão de termos de difícil pronúncia e a prevenção de cacofonias, entre outras estratégias (MOMESSO et al. 2016).

A locução é fundamental, envolvendo a modulação da voz, a entonação, o ritmo e a postura. Há exercícios direcionados para aprimorar cada uma dessas características, uma vez que uma voz sem expressividade ou excessivamente lenta pode comprometer inteiramente o desempenho do trabalho (MOMESSO et al. 2016).

De acordo com Cebeci e Tekdal (2006), há uma sugestão de que os podcasts devem ter uma duração máxima de 15 minutos. Após este período, observa-se que o consumo desse tipo de mídia de maneira prolongada, poderá resultar em uma diminuição significativa da concentração auditiva.

Após a gravação do áudio, inicia-se a etapa de edição, que compreende a seleção, corte, adição de efeitos sonoros, remoção de ruídos indesejáveis e inserção de trilha sonora, seja em primeiro plano ou em segundo plano (background). Todas essas ações são realizadas no software de edição de som (MOMESSO et al. 2016).

O podcast como Produto Educacional no Programa de pós-graduação em Educação Profissional e Tecnológica pode apresentar-se como uma alternativa viável. Em pesquisas realizadas, chegou-se, por exemplo, na dissertação de Oliveira (2022), na qual foi elaborado um Produto Educacional denominado AE-Cast: O Podcast da Assistência Estudantil, tendo como objetivo franquear informações relacionadas à Política de Assistência Estudantil no Ifes, *Campus* Vitória. Buscou-se, através desta ferramenta, colaborar com mais um instrumento de informação para os estudantes.

Outro exemplo foi o Produto Educacional elaborado por Raulino (2021), “Podcast sobre estágio supervisionado: uma proposta de orientação para estudantes da Educação Profissional Técnica de Nível Médio Integrado”. Em sua análise, a autora destacou que o Podcast é uma ferramenta pouco explorada pelos

discentes, entretanto, com potencial para colaborar com o estudo de diversos assuntos. Afirmou que a série de podcast atendeu ao objetivo da pesquisa (RAULINO, 2021).

Diante do exposto, torna-se evidente o crescente papel dos podcasts, eles emergem como uma ferramenta educacional e comunicacional poderosa, capaz de inovar e até mesmo transformar o ensino e a aprendizagem.

3. PERCURSO METODOLÓGICO

A investigação neste trabalho fundamentou-se em uma pesquisa de abordagem qualitativa, de natureza aplicada, com os objetivos exploratórios/descritivos, adotando como procedimentos a pesquisa bibliográfica e documental. Os dados produzidos foram analisados mediante a técnica de análise de conteúdo. A partir dos resultados da pesquisa realizada, elaborou-se um Produto Educacional materializado na forma de um podcast, denominado “Rastros Virtuais”.

Segundo Moreira (2011), a pesquisa qualitativa aspira interpretar os sentidos atribuídos pelos atores às suas atitudes em uma realidade socialmente construída, observando participativamente, ou seja, o investigador se entrega na pesquisa de interesse.

A pesquisa de natureza aplicada abarca análises, desejando solucionar problemas levantados no meio social que os pesquisadores vivenciam (GIL, 2023). Neste sentido, o problema de pesquisa que o investigador buscou debruçar-se, localiza-se em um curso técnico oferecido em seu local de trabalho, ajudando a corroborar a natureza aplicada da pesquisa.

Segundo Gil (2023), as pesquisas exploratórias têm a finalidade de causar uma maior proximidade com o problema, objetivando explicá-lo ou auxiliar na construção de hipóteses. O planejamento não é rígido, mas sim adaptável, visto que é importante refletir sobre inúmeros aspectos do fenômeno em análise. A afinidade com o problema é constatada, considerando que o pesquisador buscou explorar em sua pesquisa o tema de crimes cibernéticos, correlacionando com a formação acadêmica, desta forma, possibilitou que os participantes da pesquisa tivessem uma aproximação/aprofundamento com a temática proposta.

A pesquisa é descritiva, porquanto visa detalhar as características de uma população ou acontecimento (Gil, 2023), a saber, as percepções de um grupo

específico: os estudantes do curso técnico em informática para internet, com nível de escolaridade no ensino médio integrado, localizados no IFMS *Campus* Dourados.

Sobre os procedimentos da pesquisa, foi adotada a pesquisa bibliográfica “A pesquisa bibliográfica é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui ampla variedade de material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos” (GIL, 2023, p. 44). Procedendo a revisão de literatura e análise documental “[...]vale-se de toda sorte de documentos, elaborados com finalidades diversas, tais como assentamento, autorização, comunicação, etc. Mas há fontes que ora são consideradas bibliográficas, ora documentais (GIL, 2023, p. 44)”.

Neste passo, foram examinadas publicações científicas que oferecem percepções relevantes para a temática proposta. A revisão é um processo que permeia toda a pesquisa e foi realizada por meio da análise de publicações, artigos, monografias e livros. Para essa procura utilizou-se os seguintes vocábulos: “crimes cibernéticos”, “cibercrimes”, “podcast”, “ensino médio integrado”, focando em trazer um levantamento das produções acadêmicas com objetivo de chegar a uma percepção sobre as discussões realizadas até aqui. Esta busca foi efetuada no Catálogo de Teses e Dissertações e na Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e no Portal de Periódicos da CAPES.

Os dados catalogados após a aplicação dos questionários foram analisados seguindo a análise de conteúdo, sendo definida como:

> Um conjunto de técnicas de análise das comunicações visando obter por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) dessas mensagens (BARDIN, 2011, p. 44).

Bardin (2011) propõe um método que se desdobra em algumas etapas principais. A primeira etapa, denominada pré-análise, concentra-se na organização inicial das ideias. A segunda etapa envolve a exploração detalhada do material coletado. Em seguida, na terceira etapa, os resultados são tratados e interpretados. A codificação é a quarta etapa, na qual as unidades de registro e de contexto são identificadas e categorizadas. Por fim, a inferência, última etapa, envolve a análise dos pólos e processos de inferência, considerando as variáveis relevantes para a pesquisa.

3.1 Local e Sujeitos da pesquisa

A pesquisa foi realizada no *Campus* Dourados do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul. Neste campus são oferecidos dois cursos integrados para o ensino médio: Técnico em Administração e o Técnico em Informática para Internet, além de disponibilizar o Técnico subsequente em Marketing e atuar na Educação de Jovens e Adultos com o Curso Integrado em Administração, oferece também a qualificação profissional, graduação, pós-graduação, educação a distância e o ensino de idiomas (IFMS, 2023).

A justificativa para a escolha do *locus* da pesquisa fundamentou-se em duas frentes. Primeiro, como já foi dito, o *Campus* Dourados, juntamente com o Campus Naviraí, são os únicos entre os campi do IFMS que oferecem o curso Técnico em Informática para Internet voltado para o ensino médio, isto apresenta-se como um diferencial, pois o problema de pesquisa teve um enfoque na atuação do futuro profissional. Outra justificativa está no fato do pesquisador trabalhar no *campus* desde maio de 2016, o que lhe proporciona uma maior familiaridade com o *locus* e com os participantes da pesquisa.

Os sujeitos da pesquisa foram estudantes de ambos os sexos, devidamente matriculados na turma do sexto semestre do curso Técnico Integrado em Informática para Internet, na modalidade EMI, no IFMS *Campus* Dourados - MS, no ano de 2023. Foram excluídos da investigação os estudantes cujos pais e/ou responsáveis se recusaram a assinar e preencher o termo de consentimento livre e esclarecido e do termo de assentimento livre e esclarecido por parte dos adolescentes e os discentes não inseridos nos critérios de inclusão da pesquisa.

Esta pesquisa garantiu e garantirá a confidencialidade e o sigilo das informações. A divulgação dos dados será de forma genérica, não sendo possível mediante os resultados da pesquisa identificar os participantes.

4. RESULTADOS E DISCUSSÕES

Neste capítulo, serão abordados os desdobramentos da pesquisa, a partir da aplicação dos questionários aos estudantes, explorando-se o processo de coleta de dados e a interação com os participantes. Posteriormente, serão apresentados os resultados obtidos a partir desses questionários. A análise desses resultados permitirá uma reflexão mais aprofundada, contribuindo para a compreensão do impacto dos crimes cibernéticos no contexto educacional.

4.1 Aplicação dos questionários prévios aos estudantes

Em um primeiro momento, na sala de aula, com a concessão de um período de aula de 45 minutos e a respectiva anuência do professor da disciplina de Segurança da Informação, o pesquisador realizou uma introdução à temática do trabalho, com ênfase em sensibilizar os estudantes. Também foi projetado um vídeo contendo algumas notícias veiculadas em grandes mídias sobre prisões de indivíduos envolvidos em crimes cibernéticos, com o objetivo de captar a atenção dos estudantes.

Posteriormente, com o intuito de sondar os conhecimentos prévios dos alunos, elaborou-se um questionário com nove questões. Seguindo Gil (2023), a formulação do questionário elucidou os objetivos específicos da investigação e apesar de não haver uma norma pré-estabelecida, seguiu algumas diretrizes propostas. A elaboração prezou por questões relacionadas ao problema de pesquisa, evitando perguntas íntimas, além de buscar uma linguagem de fácil entendimento.

As três primeiras questões se relacionam à identificação e ao consentimento dos estudantes. Os participantes foram questionados sobre sua familiaridade com os cibercrimes, conforme a questão 4: "Você já ouviu falar em Cibercrimes (Crimes Cibernéticos, Crimes Digitais)?". Em seguida, a questão 5 explorou as percepções dos alunos sobre o conceito de cibercrimes. Posteriormente, a questão 6 investigou se consideravam relevante discutir as consequências legais dos crimes virtuais em ambiente educacional, seguida pela justificativa de suas respostas.

A pesquisa também indagou se o Curso Técnico Integrado em Informática para Internet já havia abordado o ensino das consequências legais dos crimes

cibernéticos em algum semestre, conforme a questão 7. Os participantes foram convidados a explicar suas respostas. Além disso, eles foram solicitados a listar os crimes cibernéticos que conheciam ou já ouviram falar, conforme a questão 8. Por fim, a questão 9 buscou evidenciar se os alunos acreditavam que uma formação adicional sobre os principais crimes cibernéticos e suas consequências poderia contribuir para uma atuação mais ética em suas futuras profissões na área de informática para internet.

Após a verificação dos termos necessários para iniciar a análise dos dados, constatou-se que havia um total de 27 integrantes aptos. Todos eles foram devidamente informados de que a participação era totalmente voluntária e que poderiam optar por deixar a pesquisa a qualquer momento. É relevante mencionar que todos os partícipes estavam matriculados no último semestre do curso técnico em informática para internet e demonstraram aparente satisfação em participar da pesquisa. Após a coleta de dados, partiu-se para a análise tendo como método a análise de conteúdo.

A partir de agora, serão apresentadas as análises realizadas após a aplicação do método proposto. O exame dessas respostas proporcionou resultados valiosos sobre a percepção dos acadêmicos em relação aos cibercrimes.

4.2 Apresentação dos Resultados do Questionário prévio

- Você já ouviu falar em Cibercrimes (Crimes Cibernéticos, Crimes Digitais)?

Esta questão foi formulada com o propósito de averiguar se os alunos participantes da pesquisa já possuem conhecimento sobre os cibercrimes. Como era de se esperar, 100% dos respondentes afirmaram que já ouviram falar em crimes cibernéticos. A análise das literaturas indicadas, juntamente com os conteúdos abordados no Projeto Pedagógico do Curso (PPC), permitiu inferir que os respondentes certamente teriam conhecimento dos crimes cibernéticos.

- Para você, o que são cibercrimes?

Com o objetivo de compreender melhor a percepção dos estudantes foi realizada a análise do enunciado da questão número 5, que indagou sobre a definição de cibercrimes. A partir das respostas obtidas, foi possível categorizar as diferentes concepções dos participantes em três grandes grupos: “local dos crimes”,

“natureza dos crimes” e “métodos utilizados”. Neste quadro de categorização, serão apresentados exemplos de respostas representativas de cada categoria, juntamente com a frequência de ocorrência e os respectivos enunciados dos participantes. Esse processo permitiu delinear as percepções dos estudantes sobre cibercrimes. Esse processo pode ser visualizado no quadro 4.

Quadro 4 - A visão sobre o conceito dos cibercrimes

Categoria	Exemplo da categoria	Frequência	Ocorrência
Local dos crimes	“Crimes no meio virtual, digital. Que pode acontecer roubos de dados.”**(E-25).**	5 (18,51%)	(E1), (E13), (E24), (E25), (E27),
Natureza dos crimes	“Manipulação, desvio de informações pessoas e quaisquer tipo de crime realizado no meio digital” **(E-21)**.	7 (25.9%)	(E1), (E2), (E5), (E11), (E16),(E19), (E21).
Métodos utilizados	"Crimes que acontecem em um ambiente virtual, através de links ou sites duvidosos."**(E-3).**	15 (55.6%)	(E3), (E4), (E6), (E8), (E9), (E10), (E12), (E14), (E15), (E17), (E18), (E20), (E22), (E23), (E26).

Fonte: o autor.

A categoria “Local dos crimes”, com a incidência de 18,5%, surge em resposta ao reconhecimento por parte dos estudantes de que os cibercrimes podem se manifestar no mundo virtual, na internet ou em dispositivos conectados. Quando questionado sobre o significado de cibercrimes, um estudante respondeu: "são atividades que infringem as leis, porém ocorrem de alguma forma no ambiente digital" (E-27). A resposta do estudante enfatiza que para ele os cibercrimes são delitos perpetrados no "ambiente virtual". Conforme assentado por Teixeira (2020), o crime de informática é caracterizado pelo uso de meios informáticos como ferramenta para alcançar o resultado desejado.

A segunda categoria “Natureza dos Crimes”, totalizando 25,9% das respostas, emerge da percepção que os estudantes tiveram de cibercrimes como atividades ilícitas, caracterizando como roubo de dados, fraudes, violações de privacidade e ciberbullying. Aqui, eles descreveram algum verbo nuclear do tipo

penal, ou seja, a ação principal que caracteriza o crime descrito na legislação. Quando questionado sobre o significado de cibercrimes, um estudante respondeu: “Manipulação, desvio de informações pessoas e quaisquer tipo de crime realizado no meio digital” (E21). De acordo com a legislação brasileira , a prática de modificar ou alterar sistemas de informações sem autorização está contemplada no Art. 313-B do Código Penal. Esta ação é caracterizada pela alteração não autorizada de sistemas de informações ou programas de informática por parte de funcionários.

A terceira categoria, intitulada "Métodos Utilizados", aborda os diversos métodos empregados na execução dos crimes, tais como *phishing*, ataques DDos, spoofing, entre outros. A alta frequência de respostas nesta categoria, correspondendo a 55,6%, é justificada pela inclusão desses ataques e medidas preventivas nos conteúdos programáticos do curso, o que proporciona aos acadêmicos uma maior familiaridade com o tema. Um estudante mencionou que os ataques frequentemente ocorrem "através de links ou sites duvidosos, onde conteúdos pessoais de pessoas são vazados ou utilizados para extorquir a vítima do ataque" (E3). Destaca-se a referência aos "links ou sites duvidosos". Outro participante ressaltou a prática de "hackear coisas de outras pessoas, clonar cartões, usar uma falsa identidade para enganar outras pessoas" (E17), evidenciando a expressão "hackear".

A análise das respostas revelou que os estudantes têm uma boa compreensão sobre o que são cibercrimes. Ao responderem a questão, evidenciou-se que as definições apresentadas destacam que esses são crimes cometidos no ambiente virtual, envolvendo diversas atividades ilícitas, como roubo de dados, violações de privacidade, fraudes, entre outros. Ademais, algumas respostas indicam uma percepção mais ampla, incluindo atividades como ciberbullying e exposição indevida de informações pessoais.

Conforme destacado por Sacristán (2013), o currículo desempenha um papel crucial na orientação da carreira do estudante. Dessa forma, pode-se inferir que a escola tem preparado os futuros profissionais para a identificação dos crimes virtuais.

- Você considera importante discutir as consequências legais do cometimento de crimes virtuais em sala de aula? Sim ( ) Não ( ) Justifique sua resposta.

Com o objetivo de ouvir a opinião dos estudantes sobre a importância de discutir ou não em sala de aula as consequências legais da prática dos crimes virtuais, bem como suas justificativas, foram criadas duas categorias: "conscientização e prevenção" e "educação e informação". Este quadro oferece uma visão abrangente das percepções dos participantes sobre a relevância dessa discussão no ambiente educacional. Serão apresentados exemplos representativos de cada categoria, juntamente com a frequência de ocorrência e os respectivos enunciados dos participantes. A categorização pode ser visualizada, a seguir, no quadro 5.

Quadro 5 - Opinião sobre o estudo das consequências dos Cibercrimes.

Categoria	Exemplos das categorias	Frequência	Ocorrência
Conscientização e Prevenção	"sim, porque muitas pessoas acham que cibercrimes não são crimes de verdade" **(E1)** "Sim. Para alertar sobre o que pode acontecer caso você faça algum desses crimes" **(E2)** "Sim,para que as pessoas tenha conscientização" **(E17)**	16 (59.3%)	(E1), (E2), (E3) (E4), (E5), (E6), (E7),(E8),(E9) (E10),(E11), (E12),(E13), (E14),(E15) (E17)
Educação e Informação	"Sim claro, pois principalmente nossa geração está nas telas e vulnerável o tempo todo para quaisquer tipos de ameaças virtuais" **(E16).** "Sim, acho interessante tratar desse tema pouco discutido em sala e conscientizar os estudantes sobre os riscos e consequências" **(E18).**	11 (40.7%)	(E16), (E18),(E19) (E20), (E21),(E22) (E23),(E24), (E25) (E26),(E27)

Fonte: o autor.

A categoria "Conscientização e prevenção" surge do retorno dos estudantes, representando 59,3% das respostas. Os estudantes enfatizam que a discussão das consequências legais pode conscientizar os alunos e ajudá-los a evitar a prática desses crimes, além de protegê-los de possíveis ataques virtuais. Eles ressaltam a importância de abordar as consequências legais para conscientizar e prevenir os alunos contra os crimes virtuais, como evidenciado na seguinte resposta: "Sim, pois é um bom jeito de ensinar sobre e também para alertar aos alunos sobre os crimes que acontecem e como evitá-los" (E3). A menção a "como evitá-los" remete à ideia

de prevenção. Da mesma forma, na resposta "Sim, é de suma importância para conscientizar, alertar e informar os possíveis/futuros infratores ou vítimas" (E9), percebe-se uma preocupação com a conscientização dos estudantes.

A categoria “Educação e Informação” com uma frequência de 40,7%, indica que a discussão dessas consequências, na percepção dos respondentes, contribui para a educação dos alunos sobre ética digital e responsabilidade legal. Além de reconhecerem o aumento dos crimes virtuais com o avanço tecnológico. Seguindo as respostas, um estudante escreveu: “sim, pois precisamos nos informar nesse mundo contemporâneo” (E26), uma resposta genérica, mas que verifica-se a preocupação com a informação. Outro estudante apontou: “Sim, acho interessante tratar desse tema pouco discutido em sala e conscientizar os estudantes sobre os riscos e consequências” (E18). Esta resposta reflete a necessidade de abordar o tema em sala de aula, destacando que é um assunto pouco discutido, reconhecendo a necessidade de fornecer conhecimento e orientação para que a comunidade acadêmica esteja mais preparada para lidar com os desafios do ambiente digital.

- Na sua opinião, o Curso Técnico Integrado em Informática para Internet, ofereceu em algum semestre o ensino das consequências legais da prática desses crimes? Explique

Nesta questão, o objetivo foi explorar a perspectiva dos discentes sobre a relevância de abordar as consequências legais dos crimes virtuais em sala de aula, assim como suas justificativas para tal. A partir das respostas foram criadas três categorias: “Ensino não ofertado”, “Citação da Disciplina” e “Segurança e Prevenção”. O quadro 6 foi elaborado para auxiliar na visualização dos dados catalogados.

Quadro 6 - Investigação sobre o ensino das consequências legais da prática de crimes cibernéticos

Categoria	Exemplos das categorias	Frequência	Ocorrência
	“Não” **(E7).** “não, de consequência não mas explicando os tipos de ataque, foi comentado em sala de aula mas nada mais afundo sobre” **(E10)**. “Não, até agora aprendemos mais sobre o que são esses crimes e como se precaver”	4 (14,81%)	(E7), (E10), (E18), (E22).

Ensino não ofertado	**(E18)**. “Não, na matéria de Segurança da informação aprendemos sobre vários tipos de ataques e golpes que existem na internet e a importância da segurança de nossos dados, mas não das consequências penais” **(E22)**.		
Citação da Disciplina	“Sim, nas aulas de segurança da informação” **(E4)** “Sim, na disciplina de Segurança da Informação”**(E6)**. “Sim, na disciplina de segurança da informação, oferecida no sexto semestre do curso”**(E11)**. “Sim, na matéria de segurança da informação esse tema é abordado” **(E12)**. “Sim,na aula do Jonison no sexto semestre em segurança da informação” **(E17)**. “Sim, no 6º semestre, através da disciplina de Segurança da Informação” **(E19)**. “sim, a matéria ofertada "Segurança da Informação" no sexto semestre ministrado pelo docente Jonison” **(E26).**	9 (33,33%)	(E1), (E4), (E6), (E11), (E12)(E17), (E19), (E26), (E27).
Segurança e Prevenção	“Sim, a matéria segurança da informação nos faz ter mais noção sobre esses crimes que acontecem, e como evita-los, estudando sobre como eles funcionam” **(E3)**. “sim, na matéria de segurança da informação nós estamos trabalhando os diferentes tipos de ataques virtuais”**(E5)**. “Sim, no 6 semestre na matéria do jonison, ele ensina a se precaver contra os milhares ataques” **(E8)**. “Claro, no sexto semestre nos temos a disciplina de segurança da informação, onde aprendemos a nos proteger e os diferentes tipos de crimes virtuais” **(E9)**. “Sim, na disciplina de segurança da informação, onde vemos como podemos alguns exemplos e como nos proteger”**(E14)**. “Ofereceu sim, no nosso ultimo semestre do Curso Técnico Integrado em Informática para Internet temos a matéria de Segurança da Informação que faz com que conhecemos os crimes virtuais, como funcionam, o que são, como se proteger deles e como fazer acontecer” **(E15)**.	11 (40,74%)	(E3), (E5), (E8), (E9), (E14), (E15), (E16),(E20), (E21), (E23), (E25).

Fonte: o autor.

A categoria "Ensino não ofertado" registrou uma incidência de 14,8%. Ao analisar as respostas, observou-se uma percepção da falta de abordagem

específica sobre as implicações dos cibercrimes. Os estudantes expressaram que o ensino não foi oferecido em sua formação. Um estudante foi enfático com um simples "Não" (E7). Da mesma forma, outro estudante descreveu: "Não, de consequência não, mas explicando os tipos de ataque, foi comentado em sala de aula mas nada mais aprofundado sobre" (E10). Essas respostas indicam que esse tópico não foi incluído no currículo do curso ou não foi abordado de forma adequada durante suas aulas. Eles mencionaram que aprenderam sobre os tipos de ataques, golpes e a segurança da informação, conforme reforçado por um participante: "Não, na matéria de Segurança da Informação, aprendemos sobre vários tipos de ataques e golpes que existem na internet e a importância da segurança de nossos dados, mas não sobre as consequências penais" (E22). As respostas indicaram que o foco principal do ensino foi na prevenção de crimes virtuais e na segurança da informação.

As categorias "Citação da Disciplina", com 33,33%, e "Segurança e Prevenção", com 40,74%, representam um total de 74,04% das respostas. Optou-se por analisar essas categorias em conjunto, dada a similaridade conceitual entre as respostas apresentadas. Na primeira categoria, os participantes simplesmente mencionaram ter estudado e citaram a disciplina de segurança da informação, como exemplificado por esta resposta: "Sim, na disciplina de segurança da informação, oferecida no sexto semestre do curso" (E11). Na segunda categoria, os participantes explicaram os mecanismos de segurança e informação, como evidenciado pelas seguintes respostas dos estudantes: "Sim, a matéria segurança da informação nos faz ter mais noção sobre esses crimes que acontecem, e como evitá-los, estudando sobre como eles funcionam" (E3). "Sim, na matéria de segurança da informação, nós estamos trabalhando os diferentes tipos de ataques virtuais" (E5). Diante disso, torna-se pertinente realizar um detalhamento dessas respostas.

O primeiro aspecto a ser destacado é a possibilidade de ter ocorrido uma confusão conceitual entre segurança da informação e as consequências legais dos crimes virtuais. Pode-se argumentar que os estudantes talvez interpretaram erroneamente a pergunta, confundindo a abordagem sobre crimes virtuais com a prevenção desses crimes. Quando questionados sobre se o curso ofereceu alguma formação nesse sentido, é plausível que tenham automaticamente associado a disciplina de Segurança da Informação com a discussão das implicações legais dos crimes cibernéticos, mesmo que o conteúdo específico não tenha sido abordado,

conforme análises realizadas nesta pesquisa. Possivelmente, devido ao fato de a aplicação ter ocorrido em uma aula dessa disciplina, eles puderam fazer essa conexão de alguma maneira.

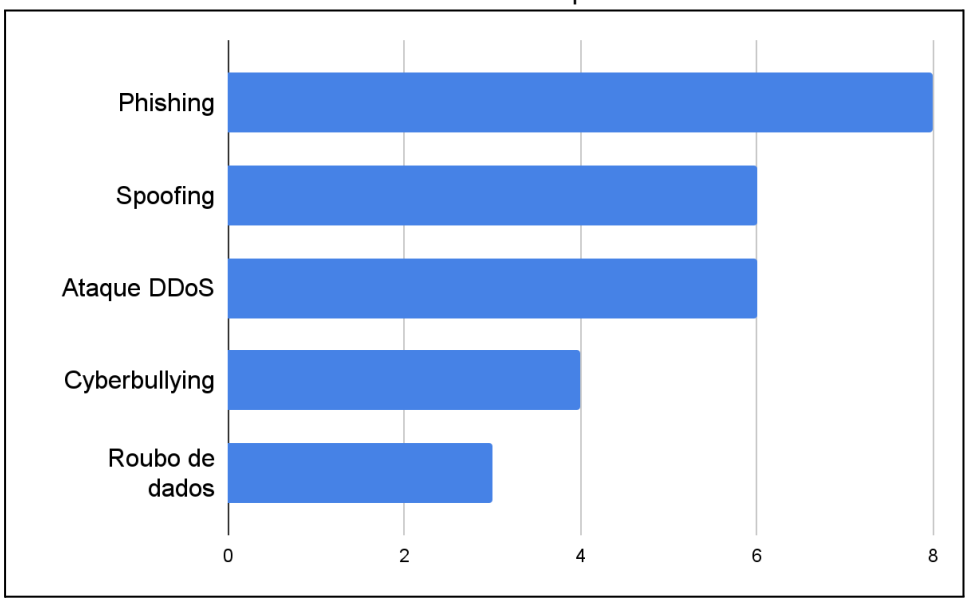
O segundo ponto é a limitação da abordagem da disciplina. Embora a disciplina Segurança da Informação possa ter tratado de alguns aspectos relacionados aos crimes virtuais, como prevenção e segurança digital, não oferece uma análise detalhada das consequências legais. Nesse caso, os estudantes podem ter suposto que a discussão sobre segurança da informação abrange automaticamente todas as implicações legais, o que não é verdadeiro.

O último ponto observado pelo pesquisador é a influência do ambiente acadêmico. Durante a aplicação do questionário prévio aos estudantes, o professor permaneceu em sala de aula, e essa permanência pode ter influenciado as respostas dos alunos. Eles podem ter hesitado em afirmar que o ensino das consequências legais dos crimes virtuais não foi oferecido, talvez com receio de parecerem desatentos ou críticos em relação ao currículo do curso.

- Elenque abaixo os Crimes Cibernéticos que você conhece ouviu já ouviu falar.

Para favorecer uma análise mais clara e visual das tendências observadas, optou-se por apresentar um gráfico que destaca os crimes mais citados pelos entrevistados.

Gráfico 1 - Os crimes cibernéticos mais citados pelos estudantes.



Fonte: o autor.

Diante das respostas dos estudantes, identificaram-se algumas tendências. Segundo a maioria, o "Phishing" destaca-se como o crime mais conhecido, com oito citações, evidenciando sua prevalência como método de fraude. Em seguida, tanto o "Spoofing" quanto os "Ataques DDoS" ocupam a segunda posição com seis citações cada, sugerindo uma ameaça significativa à segurança online. Adicionalmente, o "roubo de dados" também foi mencionado por dois respondentes.

Adicionalmente, pode-se deduzir que os estudantes, ao aprofundarem-se em conhecimentos específicos, tendem a desenvolver uma maior consciência sobre os crimes cibernéticos que mais frequentemente impactam seu campo de estudo. Os ataques cibernéticos citados são diretamente relevantes para a área de Informática para Internet, o que pode explicar a familiaridade dos alunos com esses conceitos devido ao conteúdo ensinado em sua disciplina.

- Como aluno (a) do Curso Técnico Integrado em Informática para Internet, você acredita que uma formação adicional que explique os principais crimes e as suas consequências, pode ajudá-lo(a) a ter uma atuação mais ética em sua profissão? Explique.

Nesta questão, a maioria dos estudantes reconhece que tal formação pode ajudá-los a evitar serem vítimas de golpes e a instruir outras pessoas e possíveis vítimas. Uma parcela vê a relevância desse conhecimento para sua futura atuação profissional, especialmente quem deseja seguir na área da tecnologia da informação. Alguns alunos destacam que essa formação pode ampliar sua consciência ética, ajudando-os a compreender melhor os limites legais de sua profissão. A seguir, tem-se um quadro com a categorização da questão, onde foram criadas 3 categorias: “conscientização e prevenção”, “relevância para atuação profissional” e “ampliação da consciência ética”. O quadro 7 elucida os dados elaborados.

Quadro 7 - Opinião do estudante acerca da formação adicional sobre as consequências dos cibercrimes.

Categoria	Exemplos das categorias	Frequência	Ocorrência

Conscientização e prevenção	“Pode ajudar pois nos faz evitar cair em golpes e educar outras pessoas sobre o assunto”**(E1)**.	18 (66,66%)	(E1), (E3), (E4), (E7), (E8), (E10), (E11), (E12), (E13), (E15), (E18), (E19), (E21), (E22), (E23), (E24), (E25), (E27).
Relevância para a atuação profissional	“Sim, é importante para uma profissão relacionada à internet, o conhecimento desses crimes e suas consequências, não só para acrescentar algo no currículo, mas também para evitar o profissional ou a empresa onde trabalha ser alvo de um desses crimes” **(E12).**	6 (22,22%)	(E2), (E6), (E9), (E20).
Ampliação da consciência ética	“Sim, para ter ética precisamos ter esses conhecimentos e para ter um cuidado maior para não cair em golpes” **(E17).**	3 (11,11%)	(E5), (E16), (E17)

Fonte: o autor.

Na categoria “conscientização e prevenção”, 66,7% dos estudantes responderam que uma formação adicional sobre os principais crimes cibernéticos e suas consequências pode ajudá-los a evitar a cair em golpes, além de serem fontes de conhecimento para informar outras pessoas, conforme pontuado: “pode ajudar pois nos faz evitar de cair em golpes e em educar outras pessoas sobre o assunto”(E1). Também foi destacado que esse conhecimento ajudaria a se precaver desses crimes, e a ajudar as vítimas desses ataques, conforme citação de um estudante: “Sim, pois pode me ajudar a entender melhor como me precaver sobre esses crimes e também para ajudar aos outros quando eles forem atingidos por ataques cibernéticos”(E3).

Na categoria “relevância para a atuação profissional”, mencionada por 22,2% dos estudantes, foi ressaltada a importância dessa formação adicional para suas trajetórias profissionais. Um estudante afirmou: "Sim, principalmente caso eu vá trabalhar na área de segurança da informação"(E6). O Estudante 9, por sua vez, enfatiza a relevância da atuação no ciberespaço para qualquer cidadão, além de destacar o enriquecimento para sua profissão, afirmando:"[...] e principalmente para as pessoas que trabalham e estudam nesse meio, como, por exemplo, o Curso Técnico Integrado em Informática para Internet" (E9).

A última categoria, “ampliação da consciência ética", 11,1% dos estudantes mencionaram que essa formação adicional os tornaria mais conscientes sobre o tipo

de informação que repassam para os outros. Os ajudaria a entender os limites legais de sua profissão e a agir de forma ética, além evitar cair em golpes ou cometer infrações. Um estudante mencionou que “sim, pois trás uma consciência do tipo de informação repassada para os demais”(E5). Outro participante pontou “Sim, para ter ética precisamos ter esses conhecimentos”[…] (E17). Conforme Ramos (2014), é fundamental fortalecer a integração ética entre ensino e pesquisa para fomentar a autonomia intelectual em todas esferas sociais.

Após discutirem os ataques cibernéticos mais comuns, os estudantes reconheceram a importância de uma formação adicional sobre crimes cibernéticos. Destacaram a necessidade de evitar cair em golpes, de ensinar outras pessoas sobre o assunto, e a valia desse conhecimento para suas carreiras profissionais. Também reconheceram a importância da ética na disseminação de informações e no exercício da profissão, ressaltando a integração ética entre ensino e pesquisa para promover a autonomia intelectual.

5. PODCAST : RASTROS VIRTUAIS

Com o objetivo específico de verificar a eficácia do contato com o "Podcast Rastros Virtuais" na supressão da lacuna identificada na formação do Técnico em Informática para Internet, o programa foi concebido para explorar as consequências legais dos crimes cibernéticos. Buscou-se criar um produto educacional acessível e replicável, visando garantir uma boa receptividade por parte dos participantes e uma aprendizagem satisfatória.

O produto educacional visa oferecer uma formação básica, mas indispensável, sobre as implicações legais dos crimes cometidos no ambiente de trabalho futuro dos estudantes. Sua aplicação e validação foram realizadas no IFMS *Campus* Dourados. A escolha desta ferramenta como PE oferece diversas possibilidades de uso, permitindo que o ouvinte acesse os programas em momentos oportunos, como durante o trajeto para a escola ou enquanto executa tarefas cotidianas em casa.

Além disso, a discussão sobre o desenvolvimento e a estruturação do Podcast não apenas é fundamental para a pesquisa em questão, mas também pode servir de inspiração para futuros pesquisadores interessados em criar uma ferramenta educacional semelhante. Ademais, serão explorados os processos envolvidos na concepção do conteúdo, na escolha do formato, na gravação e edição, bem como na distribuição do programa. Dessa forma, será fornecido um roteiro para aqueles que desejam iniciar um projeto educacional por meio de *podcasting*.

Agora serão detalhadas as etapas do processo de elaboração desse PE. Na primeira etapa, o pesquisador concentrou-se na seleção de equipamentos e software essenciais para a gravação do podcast. Durante esse processo foi crucial definir a estrutura física necessária e escolher o programa de edição e captação de áudio adequado. O objetivo foi garantir que o resultado final atendesse aos padrões de qualidade estabelecidos, uma vez que a qualidade do áudio desempenha um papel fundamental na manutenção do interesse do ouvinte. Assim, foi dedicado esforço para encontrar ferramentas que assegurassem uma boa qualidade de gravação. A seguir, apresenta-se uma lista detalhada dos equipamentos físicos/software empregados para as gravações:

- 02 - Microfones Microfone Behringer Ultravoice Xm8500 Dinâmico Cardióide;
- 02 - Suporte De Mesa Para Microfone Mini Pedestal Portátil Mtg 025;
- 02 - Cabo Xlr Macho X Xlr Balanceado Profissional - 4 Mt;
- 01 - Interface De Áudio Behringer U-phoria Umc22;
- 01 - Notebook : Samsung Book NP550XDA-KH3BR;
- 02 - Akg Fechados Fone de Ouvido
- 01 - REAPER (software de áudio)

O pesquisador já possuía todos os equipamentos mencionados para a gravação dos programas, eliminando a necessidade de despesas adicionais para a produção do PE. Essas ferramentas são altamente recomendadas e o investimento nelas é justificado pela qualidade do resultado final e pela durabilidade dos produtos. Contudo, é possível encontrar alternativas mais acessíveis em termos de equipamentos, sem comprometer significativamente a qualidade. Há numerosos profissionais no campo do audiovisual que realizam avaliações diárias desses produtos na internet.

Na segunda etapa ocorreu a definição de diversos aspectos cruciais para a produção do podcast, incluindo o nome do programa, a quantidade de episódios, o apresentador, os temas a serem abordados, os convidados para cada episódio, a duração máxima, a plataforma de hospedagem dos episódios, o site utilizado para criação dos *layouts* do produto educacional, e o portal escolhido para baixar a música tema dos episódios. Esta etapa desempenha um papel fundamental na estruturação do podcast, garantindo a organização e coesão de cada episódio, com o intuito de alcançar os objetivos estabelecidos. A seguir, no quadro 8, apresenta-se esses tópicos mencionados.

Quadro 8: Roteirização do podcast Rastros Virtuais.

Nome do podcast	Rastros Virtuais
Apresentador	Marlon Glauber Marinho
Títulos e links dos Episódios	**Episódio 1** - Os Ataques cibernéticos mais recorrentes https://open.spotify.com/episode/2SiLCuS6lvRrzXq2pAKtmI?si=e59ca0d13c4345fd **Episódio 2** - Os Ataques cibernéticos mais recorrentes II https://open.spotify.com/episode/4vLkVVsR2JkJCAzOVHT2ln?si=b84a5b5609714375

	Episódios 3 - As implicações penais dos ataques virtuais https://open.spotify.com/episode/62ody8NGixGfyR6aZjtcn1?si=98d0ff68a0aa43ff **Episódios 4** - Os Crimes Virtuais e suas Implicações Legais https://open.spotify.com/episode/3A3kU7zBmIKCWRNgKlofaO?si=31e3fe2d68a64016
Convidados	Professor Jonison Almeida dos Santos Policial Francielle Gottardi Ferreira
Duração	Definido a duração máxima de 15 minutos
A hospedagem dos podcasts	Spotify (*spotify for Podcasters*)
Layout	Design criados no site canva.com
Música de abertura/ fechamento dos episódios	Site: Youtube Studio Música: *Top Of The Morning* Artista: *TrackTribe* Licença: Livre (Nenhuma atribuição é necessária).

Fonte: o autor.

Os convidados concordaram em participar dos episódios de forma voluntária. Optou-se por convidar uma pessoa do sexo masculino e uma pessoa do sexo feminino para respeitar a diversidade de gênero.

A plataforma de áudio utilizada, o *Spotify*, oferece ferramentas exclusivas para produtores de conteúdo de maneira gratuita. Da mesma forma, o site escolhido, Canva, foi empregado na criação das capas dos programas sem custos adicionais.

Na terceira etapa, após o planejamento e a pré-produção que envolveram a definição do tema e objetivo de cada episódio, foram elaborados roteiros específicos para cada programa e enviados previamente aos convidados. No dia da gravação, realizou-se um briefing para a troca de ideias antes do início das gravações, com o propósito de alinhar o roteiro e criar um ambiente descontraído com os participantes. A seguir, de forma sucinta, será abordado o conteúdo dos quatro episódios gravados nesta série de podcasts, iniciando com as imagens utilizadas em cada episódio e seguindo para um resumo dos assuntos abordados.

Episódio 1 - Os Ataques Cibernéticos Mais Recorrentes. O episódio se inicia com o apresentador, Marlon Marinho, detalhando as complexidades e implicações dos crimes cibernéticos, apontando que o podcast é resultado desta

pesquisa de mestrado intitulada “Implicações Penais dos Cibercrimes: Um Estudo Visando Aprimorar a Formação do Técnico em Informática para Internet”. O episódio conta com a participação especial do professor Jonison Almeida dos Santos, um especialista em segurança da informação, servidor do IFMS desde 2015, que também leciona a disciplina de Segurança da Informação para os alunos do sexto semestre do curso Técnico Integrado em Informática para Internet, sendo este um dos focos desta pesquisa.

Em seguida, foram abordados exemplos históricos de ataques cibernéticos, como o vírus "*I Love You*" e os vazamentos de e-mails do Comitê Nacional Democrata em 2016, destacando a engenharia social como um componente crucial nesses ataques.

A conversa se aprofunda na descrição dos ataques DDoS (Distributed Denial of Service), exemplificando ataques massivos contra o GitHub em 2018 e a Amazon Web Services em 2020. O professor Jonisson explica como esses ataques funcionam e como são executados por meio de uma rede coordenada de computadores infectados, conhecida como botnet.

O episódio fornece conhecimento sobre a importância da segurança da informação e destaca a necessidade de os profissionais de informática estarem cientes dos diferentes tipos de ataques cibernéticos e de como se proteger contra eles. Caminhando para o encerramento, o apresentador agradece aos ouvintes e anuncia a continuação da discussão no próximo episódio. Em resumo, ele oferece uma visão abrangente dos desafios enfrentados na segurança cibernética e destaca a importância da educação e conscientização sobre o tema, especialmente para os futuros profissionais de informática para internet.

Episódio 2 - Os Ataques cibernéticos mais recorrentes II. Este programa é uma continuação do primeiro episódio. O professor Jonison prossegue a discussão sobre os ataques cibernéticos mais recorrentes, abordando especificamente o ataque *Hanzo Cryptolocker*, que ocorreu em 2013 e se destacou como um dos primeiros grandes ataques cibernéticos a atingir a internet globalmente, criptografando os arquivos dos usuários, exigindo um resgate para liberá-los. O ataque teve um impacto significativo em todo o mundo, afetando cerca de meio milhão de pessoas e resultando em perdas financeiras estimadas em 30 milhões de dólares pelo FBI em 2017.

Ademais, o episódio aborda a técnica de *phishing*, exemplificada por dois casos: a Operação Aurora em 2009-2010, que teve origem na China e visava grandes corporações, e o ataque ao Twitter em 2020, atribuído a um jovem de 17 anos na Flórida. O *phishing* é uma técnica antiga que envolve enganar os usuários para obter informações pessoais valiosas, muitas vezes por meio de e-mails ou mensagens falsas que se passam por entidades confiáveis.

Durante a discussão, também são exploradas as vulnerabilidades das redes públicas de Wi-Fi e a importância de medidas de segurança cibernética, como a criptografia de dados e o uso de redes privadas virtuais (VPNs), especialmente ao acessar redes públicas. A conversa destaca a necessidade de conscientização sobre segurança cibernética e a constante evolução das ameaças digitais, além de fornecer dicas práticas para proteger informações pessoais e evitar ataques cibernéticos.

Episódios 3 - As implicações penais dos ataques virtuais. O episódio discute a relevância do estudo das implicações penais dos ataques virtuais em uma era em que a tecnologia permeia todas as esferas da vida. Os ataques cibernéticos tornaram-se uma ameaça significativa, exigindo uma análise cuidadosa das consequências legais dessas ações. A conversa é conduzida pelo apresentador e sua convidada, a escrivã da polícia do Mato Grosso do Sul, Francielle Gottardi Ferreira, uma profissional qualificada que compartilha sua experiência tanto como cientista da computação quanto como policial civil.

Francielle expõe sua trajetória profissional, desde sua formação em Ciência da Computação até sua entrada na carreira policial. Ela destaca a complexidade dos crimes cibernéticos, como a invasão de dispositivos informáticos e o furto qualificado mediante fraude eletrônica. A invasão de dispositivos, exemplificada pelo caso da atriz Carolina Dieckmann, é discutida em relação à dificuldade em identificar e tipificar os crimes, muitas vezes envolvendo fraudes eletrônicas e furtos qualificados.A fraude eletrônica, frequentemente perpetrada por meio de engenharia social, é mencionada como um crime em ascensão, com um número significativo de ocorrências registradas no estado.

Por fim, a convidada destaca o papel da polícia na investigação e combate aos crimes cibernéticos, enfatizando que a internet não é uma terra sem lei e que os responsáveis por esses crimes serão identificados e responsabilizados. O episódio

encerra com uma mensagem de conscientização sobre a importância de estar atento às ameaças online e da atuação constante das autoridades para manter a segurança digital.

Episódios 4 - Os Crimes Virtuais e suas Implicações Legais. O quarto e último episódio da série "Rastros Virtuais" discute uma variedade de crimes virtuais tipificados na legislação brasileira. O apresentador conduz uma revisão dos temas abordados nos episódios anteriores, como invasão de dispositivos informáticos, interrupção ou perturbação de serviços informáticos, estelionato digital e furto mediante fraude eletrônica.

O crime de invasão de dispositivo informático é explicado como a manipulação, adulteração ou destruição de dados sem a autorização do proprietário do dispositivo. Casos recentes, como a invasão do sistema da Justiça Federal, são citados como exemplos das graves penalidades que podem resultar dessa prática.

A interrupção ou perturbação de serviços informáticos é destacada como uma conduta criminosa que pode resultar em detenção de um a três anos, além de multa. O estelionato digital, fraude eletrônica e furto mediante fraude eletrônica são abordados com detalhes, ressaltando as severas penas previstas na lei para esses crimes. Os ouvintes são alertados sobre os perigos das armadilhas digitais, como *phishing* e outras técnicas de engenharia social.

Outrossim, são discutidos crimes relacionados ao cyberbullying, violação de direitos autorais, racismo e apologia ao nazismo. O apresentador destaca a importância de respeitar o próximo e evitar práticas que possam resultar em graves consequências legais.

O episódio encerra com uma reflexão sobre a necessidade de vigilância constante e conscientização sobre os riscos e vulnerabilidades das tecnologias digitais. A mensagem final ressalta que a legislação brasileira está atenta aos crimes virtuais e que os infratores não ficarão impunes.

5.1 Resultados obtidos na aplicação do produto

Após a conclusão da série de podcast “Rastros Virtuais”, os episódios foram inseridos na plataforma de áudio Spotify. O instrumento escolhido para realizar a aplicação dos questionários junto aos estudantes foi a escala de Likert. Segundo Gil

(2008), a elaboração desta escala deve levantar questões que denotam opinião relacionada ao tema estudado. Os participantes escolhem entre (1) concordo totalmente, (2) concordo parcialmente, (3) não concordo, nem discordo, (4) discordo parcialmente e (5) discordo totalmente. As avaliações mais altas referem-se à concordância, enquanto as avaliações mais baixas ocorrem a discordância.

A utilização desta escala teve como objetivo analisar a eficácia do podcast como uma ferramenta de ensino para futuros Técnicos em Informática para Internet, além de fornecer conhecimentos essenciais sobre as consequências legais dos crimes praticados no ambiente virtual.

A elaboração do questionário pós-aplicação do produto educacional contou com dez perguntas que abordam diversos aspectos relacionados à estrutura, conteúdo, linguagem e relevância do curso para os objetivos propostos. Ademais, incluiu-se uma questão aberta com o intuito de colher sugestões, elogios e reclamações. Este instrumento de avaliação foi encaminhado para todos os participantes da pesquisa por meio do e-mail acadêmico. O período disponibilizado para que os estudantes avaliassem o produto educacional foi de 27 no mês de dezembro do ano de 2023.

O formulário foi encaminhado a 27 estudantes que aceitaram participar da pesquisa, obtendo retorno de dez deles, o que corresponde a 37,1%. Esta taxa de resposta pode ser atribuída, em grande parte, ao mês de dezembro, visto que é um período festivo. Além disso, tem-se que considerar que os participantes estavam no último semestre do curso e concentrados em vestibulares ou na escolha das faculdades que iriam cursar. Diante desses fatores, o pesquisador realizou um esforço adicional de sensibilização por meio do chat de e-mail, incentivando os participantes a responderem ao questionário. Considerando o contexto, o número de respostas obtidas foi satisfatório.

A seguir, serão apresentados os gráficos com as avaliações realizadas pelos estudantes, organizados e aglutinados seguindo o mesmo padrão de avaliações realizadas pelos estudantes, disponível no Apêndice C.

Neste primeiro agrupamento, as respostas foram coletadas de cinco questões, com o mesmo percentual de respostas. Elas estão descritas no quadro 9.

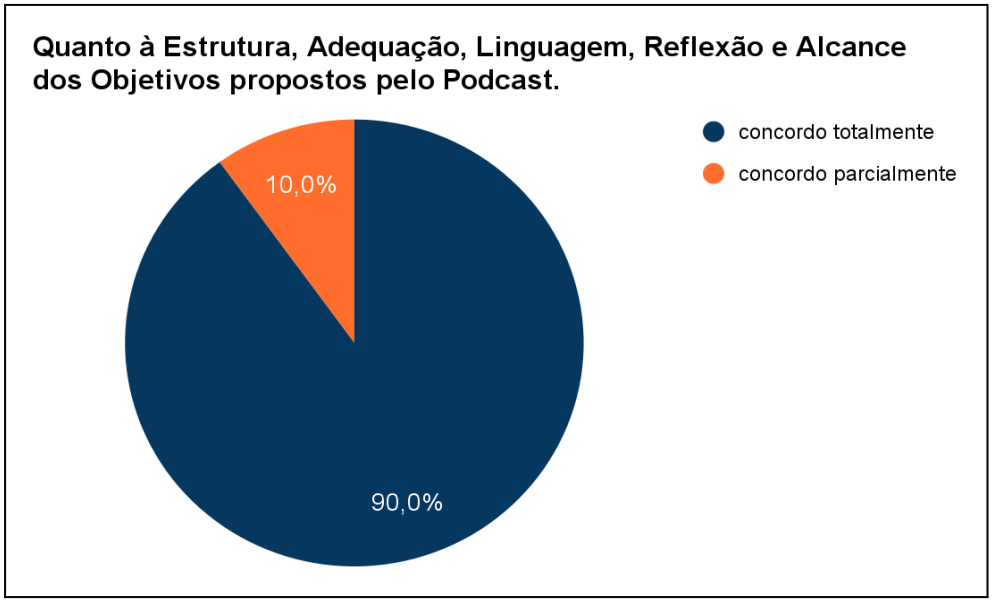
Quadro 9: Questionário sobre o primeiro agrupamento (90%)

Questão	Descrição da Questão
1	A forma como o podcast está estruturado é apropriada para alcançar os objetivos propostos.
3	Os episódios dos podcasts são adequados para alcançar os objetivos propostos
4	A linguagem utilizada no conteúdo do podcast é apropriada para sua compreensão
6	O conteúdo do podcast permite momentos de reflexão adequados aos assuntos tratados
7	O conteúdo do podcast é adequado ao alcance dos objetivos propostos

Fonte: o autor.

Com base nas respostas, é coerente constatar que a estrutura do podcast, a adequação dos episódios, a linguagem utilizada, o conteúdo para gerar reflexões e a adequação do conteúdo para alcançar os objetivos propostos foram avaliados positivamente pelos participantes. Nessas questões, 90% dos participantes concordam totalmente, enquanto 10% concordam parcialmente. Essas análises sugerem uma recepção positiva e uma eficácia geral do podcast em alcançar seus objetivos. A seguir, apresenta-se o gráfico 2 a fim de ilustrar o percentual das respostas obtidas.

Gráfico 2 - Avaliação dos Objetivos do Podcast.



Fonte: elaborado pelo autor.

No segundo agrupamento, as respostas foram agrupadas em três questões com o mesmo percentual de respostas, descritas no quadro 10.

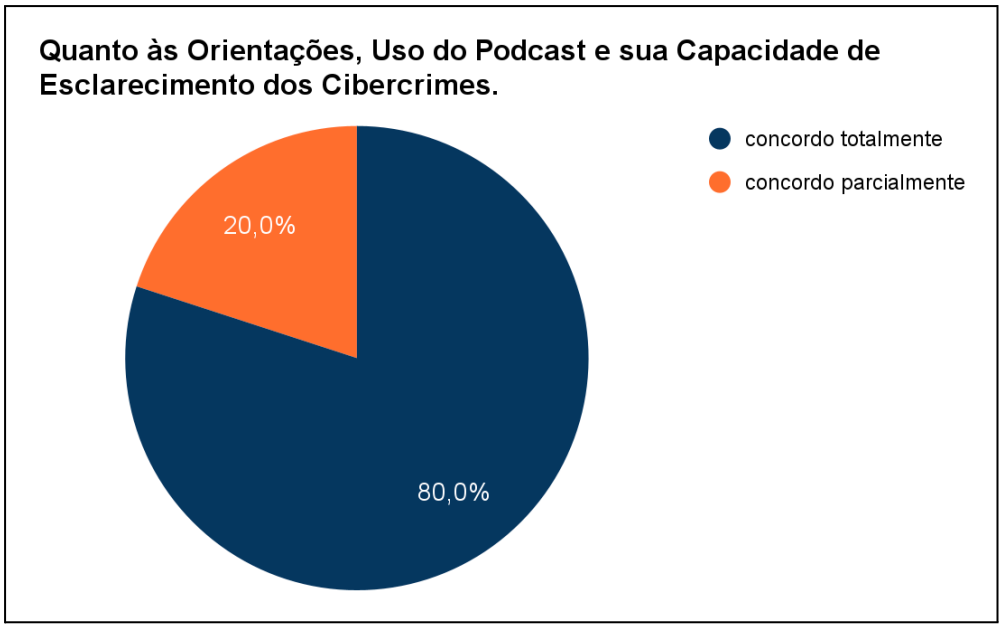
Quadro 10: Questionário sobre o segundo agrupamento (80%)

Questão	Descrição da Questão
2	As orientações repassadas no podcast são de fácil compreensão
8	Considero que a realização do podcast pode ser utilizada para complementar os ensinamentos obtidos em disciplinas que abordam o tema na instituição de ensino
9	Considero o podcast um recurso importante que os professores poderão indicar aos seus alunos para o esclarecimento sobre as consequências do cometimentos de crimes na Internet

Fonte: o autor.

Com base nas respostas coletadas, observa-se que a clareza das orientações no podcast, a utilização do podcast para complementar ensinamentos e a possibilidade de indicação da ferramenta do docente para o aluno, receberam uma avaliação geral positiva, com 80% dos participantes concordando totalmente e os restantes 20% concordando parcialmente. Esses resultados sugerem uma percepção positiva do podcast como um recurso educacional e esclarecedor. A seguir, no gráfico 3, apresenta-se o percentual das respostas obtidas.

Gráfico 3 - Utilização do podcast.



Fonte: elaborado pelo autor.

No terceiro e último agrupamento, as respostas relacionam-se a duas questões, conforme o quadro 11.

Quadro 11: Questionário sobre o terceiro agrupamento (100%)

Questão	Descrição da Questão
5	O recurso escolhido, o Podcast, é adequado para estudar as consequências dos cibercrimes
10	Considero o podcast um recurso importante a ser utilizado pela instituição de ensino;

Fonte: o autor.

Nesta seção, ao responderem as duas questões, houve uma aceitação unânime, sugerindo que todos os participantes reconhecem o valor dessa ferramenta no contexto educacional e a sua adequação para estudar as consequências dos cibercrimes, indicando uma avaliação extremamente positiva desta ferramenta.

Por fim, foi aberto um campo para que os ouvintes pudessem descrever suas percepções sobre o produto educacional:

- “Caso tenha marcado a opção discordo em algum item avaliado, por gentileza, contribua com sugestões de melhorias para aprimorarmos o curso. Caso queira, esse espaço também pode ser utilizado para elogios e reclamações”. Apresentamos no quadro 8 as respostas obtidas.

Quadro 8: Comentários dos estudantes

Estudante	Descrição do comentário
(E1)	“Top”.
(E2)	“Muito bom o podcast”.
(E3)	“Perfeito!!!”.
(E4)	“Um podcast de altíssima qualidade, em todos os níveis, desde técnicos até didáticos”.
(E5)	“O podcast ficou muito bom, explicativo e realmente auxilia sobre os crimes, ficou ótimo”.

(E6)	“É uma ótima forma de aprendermos sobre a temática trabalhada”.
(E7)	“eu ameii o podcast,arrasou demaisss,sem reclamações apenas elogio mesmo,sucesso!!!”.
(E8)	“Os podcasts são importantes para o ensino, estão ótimos”.
(E9)	“Ótimo trabalho, sucesso!👏”.
(E10)	“Nada a opinar, show!”.

Fonte: o autor.

Os comentários revelam uma recepção positiva, com elogios que enfatizam a qualidade técnica, a clareza da apresentação, a utilidade do conteúdo e a importância dos podcasts como recurso educacional. A ausência de críticas significativas sugere uma satisfação geral com o produto educacional. Diante desses resultados, o pesquisador constata que esta ferramenta, o podcast, possui potencial para se adaptar às necessidades e expectativas dos ouvintes/estudantes, possibilitando uma experiência educacional eficaz e satisfatória.

6. CONSIDERAÇÕES FINAIS

As considerações primárias deste trabalho iniciam-se sobre a reflexão dos pilares da Educação Profissional e Tecnológica (EPT) no contexto da formação dos estudantes. A busca pela formação integral dos alunos visa integrar as dimensões do trabalho, ciência e cultura e essa abordagem é baseada na compreensão do trabalho como princípio educativo e na busca por uma formação crítica e autônoma dos profissionais, conforme ensinado por Ciavatta (2012) e Frigotto (2005). Partindo desse aprendizado valioso, passamos então a construir os eixos da nossa pesquisa.

Para entendermos a evolução das disciplinas abordadas pela instituição foi necessário observar a dualidade presente no ensino, onde as classes sociais eram tratadas de maneira distinta, sendo a classe trabalhadora destinada a profissões manuais e as elites burguesas reservadas a profissões intelectuais, evidenciando uma discriminação no ensino formal (SAVIANI, 2007).

Essa análise nos levou a compreender que o acesso ao estudo das ciências jurídicas sempre foi privilegiado para as elites, enquanto a classe trabalhadora era privada desse conhecimento essencial. Tal exclusão impede a emancipação plena dessa classe, que poderia ser alcançada por meio do estudo e do acesso ao saber jurídico. A formação oferecida pela EPT deve capacitar o estudante de maneira abrangente, preparando-o para desafios profissionais e para exercer uma cidadania plena e o estudo da ciência jurídica contribuiu para o cumprimento desse propósito educacional.

Posto isso, partimos, então, para a investigação das implicações penais dos cibercrimes, com foco na formação do Técnico em Informática para Internet no contexto do IFMS *Campus* Dourados, é possível afirmar que este estudo trouxe à tona questões cruciais sobre a preparação dos estudantes para os desafios de sua futura atuação profissional. Ao buscar responder à pergunta fundamental sobre como o ensino das consequências legais dos crimes cibernéticos pode enriquecer a formação profissional dos futuros técnicos em informática para internet, identificamos uma série de aspectos que merecem ser ressaltados.

Ao longo desta pesquisa, identificamos os crimes virtuais que os estudantes devem compreender para aprimorar sua formação profissional e, além disso, também fortalecer a cidadania junto ao ciberespaço. Para isso, delimitamos três objetivos específicos que incluíram a análise das leis brasileiras relacionadas aos

ilícitos cibernéticos, a descrição da presença ou não do estudo das implicações penais dos cibercrimes na unidade curricular Segurança da Informação, e verificamos se a utilização do podcast ‘Rastros Virtuais’ foi uma ferramenta apropriada para complementar o entendimento dos alunos do Curso Técnico em Informática para Internet sobre as consequências legais dos cibercrimes.

Quanto ao primeiro objetivo específico, que é “ identificar, no âmbito da legislação penal brasileira, as leis que regulamentam os ilícitos cibernéticos”, constatou-se que o arcabouço jurídico relacionado aos crimes virtuais reflete uma evolução significativa ao longo dos anos. Iniciando com a Lei “Carolina Dieckmann” que foi um marco importante na regulamentação do direito digital no Brasil. Continuando, com alterações adicionais ao Código Penal tornando mais graves os crimes cometidos de forma eletrônica ou pela internet. Além disso, a implementação do Marco Civil da Internet desempenhou um papel fundamental na definição de princípios, garantias e direitos, para os usuários da internet no Brasil.

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou outro ponto de referência, visando proteger os direitos fundamentais de liberdade e privacidade dos indivíduos. Por fim, o país ratificou a Convenção sobre cibercrime, reforçando o compromisso em combater ameaças à segurança digital.

Analisamos também as tipificações e classificações dos crimes virtuais. A título exemplificativo, vimos o crime de invasão de dispositivo informático, estelionato digital e furto mediante fraude eletrônica e ciberbullying. Esses crimes demonstraram a complexidade e a necessidade de adaptação do ordenamento jurídico frente aos avanços tecnológicos e suas implicações criminais.

O segundo objetivo específico foi “descrever e avaliar a presença do estudo das implicações penais dos cibercrimes na unidade curricular Segurança da Informação, assim como em literaturas recomendadas em sua unidade curricular”. A análise revelou que, embora os livros abordassem de maneira abrangente os aspectos técnicos da segurança da informação, como medidas de proteção contra ataques cibernéticos, não há uma discussão sobre as consequências legais da prática desses crimes. O livro "Informação, Codificação e Segurança de Redes" trata dos fundamentos da segurança da informação, especificando as potenciais vulnerabilidades das redes, mas não discute as implicações jurídicas dos cibercrimes.

Do mesmo modo, os livros "Segurança em Aplicações Web" e "Segurança para Desenvolvedores Web" abordam mecanismos de segurança para prevenir ataques cibernéticos, mas não oferecem uma análise detalhada das implicações legais dessas práticas. Em suma, embora os livros analisados forneçam uma base sólida em termos de segurança da informação, podemos afirmar que há uma lacuna no que diz respeito à abordagem das implicações penais dos cibercrimes, até porque esse não é o foco das literaturas.

O terceiro objetivo específico, a saber, “verificar se o conteúdo do podcast "Rastros Virtuais" é apropriado e efetivo como uma ferramenta adicional para complementar o entendimento dos alunos do Curso Técnico em Informática para Internet sobre as consequências legais dos cibercrimes”. A análise dos questionários indicou uma avaliação positiva do podcast em diversos aspectos. A maioria dos participantes concordou que a estrutura, orientações, adequação dos episódios, linguagem utilizada e conteúdo do podcast eram apropriados e eficazes para alcançar os objetivos propostos.

De acordo com a avaliação dos estudantes, o Produto Educacional foi considerado adequado para estudar as consequências dos cibercrimes, permitindo momentos de reflexão e sendo capaz de alcançar os objetivos propostos. A maioria também concordou que o podcast poderia ser utilizado para complementar os ensinamentos obtidos em disciplinas que abordam o tema na instituição de ensino, e que era um recurso importante que os professores poderiam indicar aos alunos para o esclarecimento sobre as consequências dos crimes na Internet. Concluímos, então, que o podcast é uma ferramenta eficaz para complementar o entendimento dos estudantes.

Considerando os achados desta pesquisa, há diversas áreas que merecem atenção para futuras investigações. Uma possível linha de estudo seria analisar detalhadamente o impacto das leis de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD), uma legislação relativamente nova e com um vasto campo a ser explorado. Investigar de que forma essas regulamentações influenciam o comportamento dos indivíduos e das organizações na proteção de informações pessoais e na prevenção de ataques virtuais poderia fornecer perspectivas valiosas para aprimorar políticas públicas e estratégias de segurança cibernética.

Outra área de interesse é a análise do impacto psicossocial dos cibercrimes na sociedade. Compreender como as vítimas desses crimes lidam com as consequências emocionais, financeiras e sociais pode fornecer direcionamentos importantes para o desenvolvimento de políticas de apoio e intervenções preventivas. Existem diversas oportunidades para pesquisas futuras na área do direito cibernético e da tecnologia digital, desde a análise do efeito das leis de proteção de dados até o desenvolvimento de novas tecnologias bem como a compreensão do impacto psicossocial dos cibercrimes na sociedade. Essas recomendações representam apenas algumas das possibilidades e espero que inspirem futuros estudos que contribuam para a melhoria da segurança digital e suas consequências e o bem-estar dos estudantes e usuários do ciberespaço.

REFERÊNCIAS

ALVES JÚNIOR, Ivan José. **Ética e integridade na pesquisa: um curso on-line para jovens pesquisadores**. 2021. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul - IFMS, [S. l.], 2021. Disponível em: https://educapes.capes.gov.br/handle/capes/597526. Acesso em: 9 dez. 2022.

ANTEZANA, M. B. O. ; SKAF, R. C. **O direito constitucional e a educação: uma proposta interdisciplinar para a formação da cidadania dos jovens**. Revista Metalinguagens, v.4., n.2, p. 149 - 165, 2017. Disponível em : <http://revista2.spo.ifsp.edu.br/index.php/metalinguagens/issue/view/27> Acesso em: 08/05/2023

ARAUJO, Ronaldo Marcos de Lima. **Formação de professores para Educação Profissional e Tecnológica e a necessária atitude docente Integradora**. In: DALBEN, ângela imaculada Loureiro de Freitas (org.) Convergências e tensões no campo da formação e do trabalho docente. Belo Horizonte: Autêntica, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm\>. Acesso em: 22 mar. 2023.

BRASIL. Lei n.º 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. [S. l.], 13 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 5 dez. 2022.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 abr. 2023.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 18 abr. 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade por Omissão 26/DF** - Distrito Federal. Relator: Ministro Celso de Mello. Disponível em : https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/tesesADO26.pdf. Acesso em: 22 março 2023.

BRASIL. Lei n.º 11 DE AGOSTO DE 1827, de 11 de agosto de 1827. **Crêa dous Cursos de sciencias Juridicas e Sociaes, um na cidade de S. Paulo e outro na de Olinda**. [S. l.], 1827. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lim/lim.-11-08-1827.htm. Acesso em: 13 dez. 2022.

BRASIL. Lei n.º 9.394, de 20 de dezembro de 1996. **Estabelece as diretrizes e bases da educação nacional**. [S. l.], 20 dez. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 15 fev. 2023.

BRASIL. Lei n.º 14.197, de 1 de outubro de 2021. **Acrescenta o Título XII na Parte Especial do Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito**. 1 out. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm#:~:text=Democr%C3%A1tico%20de%20Direito-,Art.,da%20pena%20correspondente%20%C3%A0%20viol%C3%AAncia. Acesso em: 23 mar. 2023.

BRASIL. Decreto n.º 11.491, de 12 de abril de 2023. **Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001**. [S. l.], 12 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 25 abr. 2023.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. [S. l.], 30 nov. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 fev. 2023.

BRANDÃO, Luíza Couto Chaves. **O Marco Civil da Internet e a Proteção de Dados: diálogos com a LGPD**. Cadernos Adenauer, Rio de Janeiro, n. 3, p. 35-48, out. 2019.

CAPES. **Produção técnica**. Brasília:Ministério da Educação, 2019.

CARVALHO, A. A. A.; AGUIAR, C.; MACIEL, R. Taxonomia de Podcasts: da criação à utilização em contexto educativo. In: CARVALHO, A. A. A., org. Actas do Encontro sobre Podcasts, Braga, Portugal, 2009. Braga: Universidade do Minho. Centro de Investigação em Educação (CIEd), 2009. ISBN 978-972-8746-69-8. p. 96-109. Disponível em: <https://hdl.handle.net/1822/10032\>. Acesso em: 20 fev. 2024.

CEBECI, A., & TEKDAL, M. (s.d.). **Podcasting como Objeto de Aprendizagem de Áudio**. [S.l.: s.n.]. Disponível em: https://www.researchgate.net/publication/260943340_Using_Podcasts_as_Audio_Learning_Objects. Acesso em: 20 fev. 2024.

CIAVATTA, Maria. O Ensino Integrado, a Politecnia e a Educação Omnilateral. Por que lutamos? **Trabalho & Educação**, Belo Horizonte, v. 3, n. 1, p. 187-205, jan./abr. 2014. Disponível em: https://periodicos.ufmg.br/index.php/trabedu/article/view/9303/6679. Acesso em: 20 dez. 2022.

CIAVATTA, Maria. **A formação integrada a escola e o trabalho como lugares de memória e de identidade**. Trabalho Necessário, Niterói, v. 10, n. 16, 2012.

Disponível em: https://periodicos.uff.br/trabalhonecessario/article/view/6122. Acesso em: 20 dez. 2022.

DINIZ, Mariana Ferreira. **A revista da primeira Faculdade de Direito do Brasil na transição Império-República: 1893 a 1913, escrita e poder**. Rio de Janeiro, n. 29, p. 178-197, jan.-Abr. 2022 - Revista Maracanan. Disponível em: https://www.e-publicacoes.uerj.br/index.php/maracanan. Acesso em: 12/05/2023

DUARTE, Newton. **Os conteúdos escolares e a ressurreição dos mortos: contribuição à teoria histórico-crítica do currículo**. Campinas, SP: Autores Associados, 2016.

FALCÃO, Márcio. **Hacker Delgatti é condenado a 20 anos de prisão por invadir celulares de autoridades da Lava Jato e vazar mensagens**. G1, Brasília, 21 ago. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/08/21/hacker-delgatti-e-condenado-a-20-anos-na-operacao-que-investiga-o-vazamento-de-conversas-da-lava-jato.ghtml. Acesso em: 25 set. 2023.

FERREIRA, Rodrigo. **Segurança em Aplicações Web**. São Paulo: Editora Casa do Código, 2017.

FRIGOTTO, Gaudêncio; CIAVATTA, Maria; RAMOS, Marise (org.). **Ensino médio integrado: concepção e contradições**. 3º. ed. São Paulo: Cortez, 2012.

FRIGOTTO, Gaudêncio; CIAVATTA, Maria (orgs.). **Ensino médio: ciência, cultura e trabalho**. Brasília: MEC/SEMTEC, 2004.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo : Atlas, 2008.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 7. ed. Barueri, SP: Atlas, 2023.

GOMES, Frederico Félix. **Direito eletrônico e internet**. Londrina : Editora e Distribuidora Educacional S.A., 2016.

GRECO, Rogério.**Curso de Direito Penal: parte geral**, volume I. 19. ed. Niterói, RJ: Impetus, 2017.

INSTITUTO FEDERAL DO ESPÍRITO SANTO. **Regulamento geral do Programa de Mestrado Profissional em Educação Profissional e Tecnológica em Rede Nacional**. Ministério da Educação: IFES, 2018. Disponível em: https://profept.ifes.edu.br/images/stories/ProfEPT/Turma_2018/Regulamento/Res_CS_22_2018_-_Regulamento.pdf. Acesso em: 28 mar. 2023.

INSTITUTO FEDERAL DO MATO GROSSO DO SUL. **Projeto Pedagógico de Curso Técnico em Informática para Internet**. Dourados, 2019. Disponível em: https://www.ifms.edu.br/centrais-de-conteudo/documentos-institucionais/projetos-pe

dagogicos/projetos-pedagogicos-dos-cursos-tecnicos/projeto-pedagogico-do-curso-tecnico-integrado-em-informatica_-campus-dourados.pdf. Acesso em: 01 dez. 2022.

JACOBUCCI, Daniela Franco Carvalho. **CONTRIBUIÇÕES DOS ESPAÇOS NÃO-FORMAIS DE EDUCAÇÃO PARA A FORMAÇÃO DA CULTURA CIENTÍFICA**. Em Extensão Uberlândia, p. 55-66, 2008. EDUFU - Editora da Universidade Federal de Uberlândia.

MATO GROSSO DO SUL. Subsecretaria de Políticas Públicas LGBT. **Crimes Virtuais**. [Dourados]: Subsecretaria de Políticas Públicas LGBT. Disponível em: https://www.cidadanialgbt.ms.gov.br/?page_id=23. Acesso em: 21 março 2023.

MOMESSO, Maria Regina; YOSHIMOTO, Eduardo; CARVALHO, Ana Amélia; DIEGUES, Vitor; MEIRELLES, Mauro (Organizadores). **Educar com podcasts e audiobooks**. Porto Alegre: CirKula, 2016. 180 p. [e-Book].

MONASTA, A. **Antonio Gramsci** / Atillio Monasta; tradução: Paolo Nosella. – Recife:Fundação Joaquim Nabuco, Editora Massangana, 2010.

MOREIRA, Marco Antonio. **Metodologias de pesquisa em ensino.** São Paulo: Editora Livraria da Física, 2011.

NELSON, Saldanha. **Teoria do direito e crítica histórica**. Revista de informação legislativa, v. 22, ed. n. 88, p. 67-74, 10 1985. Disponível em: https://www2.senado.leg.br/bdsf/item/id/181648. Acesso em: 24 jan. 2023.

NUZUM, Eric. **Make noise a creators guide to podcasting and great audio storytelling**. [e-book]. Workman publishing, New York, 2020.

OLIVEIRA, Alessandro Zardini de. **Política de assistência estudantil do Ifes : ações inclusivas para o acesso, permanência e êxito dos(as) estudantes do Proeja**. 2022. 204 p. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo, [S. l.], 2022. Disponível em: https://repositorio.ifes.edu.br/handle/123456789/1702. Acesso em: 13 jan. 2023.

PELLOSO, João Augusto Grecco. **Educação Para Cidadania: do contexto de produção ao contexto da prática**. 2021. 137 p. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, Campo Grande, MS, 2021.

MICROSOFT. **O que é um ataque cibernético**?. Microsoft, 2023. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-cyberattack. Acesso em: 10 set. 2023.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book (573 p.).

RAMOS, Marise. **Concepção do Ensino Médio Integrado**. s.l., 2007. Disponível em:

https://tecnicadmiwj.files.wordpress.com/2008/09/texto-concepcao-do-ensino-medioi ntegrado-marise-ramos1.pdf. Acesso em: 03 dez. 2022.

RAMOS, Marise Nogueira. **História e Política da Educação Profissional**. [S. l.: s. n.], 2014. Disponível em: https://memoria.ifrn.edu.br/handle/1044/2219. Acesso em: 30 mar. 2023.

RAULINO, Cíntia Grazielle de Souza. **Podcast sobre estágio supervisionado**: uma proposta de orientação para estudantes da Educação Profissional Técnica de nível médio Integrado. 2021. 101 p. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, Campo Grande, MS, 2021.

RODRIGUES, Renato. **Brasileiros são principais alvos de ataques de phishing no mundo**. kaspersky, 2021. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/ . Acesso em: 10 set. 2023.

SAFERNET, org. **Central Nacional de Denúncias - 2022**. Disponível em: <https://docs.google.com/spreadsheets/d/1QVeMKdRAgyHLvOCkKWwPWjij9_JRm EgxkRN13mHtUd4/edit#gid=0>. Acesso em: 24 abril 2023.

SAVIANI, Dermeval. **Pedagogia histórico-crítica: primeiras aproximações**. 11.ed.rev. Campinas, SP: Autores Associados, 2011.

SAVIANI, Dermeval. **Trabalho e educação: fundamentos ontológicos e históricos**. Revista Brasileira de Educação, Campinas, v. 12, n. 34, p. 15-30, maio 2007. Disponível em: https://www.scielo.br/j/rbedu/a/wBnPGNkvstzMTLYkmXdrkWP/. Acesso em: 13 abr. 2023.

SAVIANI, Dermeval. **Pedagogia histórico-crítica: primeiras aproximações**. 8ª ed. Campinas, SP: Autores Associados, 2003.

SAVIANI, Dermeval. **Teorias Pedagógicas Contra-Hegemônicas no Brasil**. Ideação, [S. l.], v. 10, n. 2, p. 11–28, 2000. DOI: 10.48075/ri.v10i2.4465. Disponível em: https://e-revista.unioeste.br/index.php/ideacao/article/view/4465. Acesso em: 31 maio. 2023.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). Edição semanal - **Estelionato**. TJDFT, 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edic ao-semanal/estelionato-1#:~:text=A%20fraude%20eletr%C3%B4nica%20ocorre%20 quando,cart%C3%A3o%20de%20cr%C3%A9dito%20ou%20d%C3%A9bito. Acesso em: 10 set. 2023.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO DO SUL (TJMS). **Homem é condenado a 13 anos de reclusão por estupro virtual de vulnerável**. TJMS, 2023. Disponível em: https://www.tjms.jus.br/noticia/63121. Acesso em: 26 Set. 2023.

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO (TRF3). **Justiça Federal condena hackers por falsificação de documento público em sistema processual**. TRF3, 2021. Disponível em: https://web.trf3.jus.br/noticias/Noticiar/ExibirNoticia/414225-justica-federal-condena-hackers-por-falsificacao-de. Acesso em: 10 set. 2023.

APÊNDICE A - PRODUTO EDUCACIONAL

SUMÁRIO

Bem-vindo ao podcast Rastros Virtuais, o programa que mergulha no mundo obscuro dos crimes cibernéticos e explora as intricadas teias digitais que conectam os principais ataques cibernéticos às suas consequências penais. Esta série de podcast é resultado da minha pesquisa de mestrado, intitulada: Implicações Penais dos Cibercrimes: Um Estudo Visando Aprimorar a Formação do Técnico em Informática para Internet, desenvolvida no Programa de Pós-Graduação em Educação Profissional e Tecnológica, sob orientação do Professor Dr. Danilo Teles.
Então, prepare-se para mergulhar no mundo dos "Rastros Virtuais" e venha conosco enquanto exploramos as complexidades e as implicações dos crimes digitais.

Autor: Marlon Marinho


PODCAST
RASTROS VIRTUAIS
PROFESSOR JONISON
PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
EP. 1
Os Ataques Cibernéticos Mais Recorrente - I
Os Ataques cibernéticos mais recorrentes
PREVIEW Dec 2023 · Rastros Virtuais
Save on Spotify


PODCAST
RASTROS VIRTUAIS
PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
PROFESSOR JONISON
EP. 2
Os Ataques Cibernéticos Mais Recorrente - II
Os Ataques cibernéticos mais recorrentes II
PREVIEW Dec 2023 · Rastros Virtuais
Save on Spotify


PODCAST
RASTROS VIRTUAIS
POLICIAL FRANCIELLE
PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
EP. 3
As implicações penais dos Ataques Virtuais
As implicações penais dos ataques virtuais
PREVIEW Dec 4 - Rastros Virtuais
Save on Spotify


PODCAST
RASTROS VIRTUAIS
MARLON MARINHO
PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
EP. 4
Os crimes virtuais e suas Implicações Legais
Os Crimes Virtuais e suas Implicações Legai
PREVIEW Dec 2023 · Rastros Virtuais
Save on Spotify

PODCAST RASTROS VIRTUAIS

AUTOR:
Marlon Glauber Marinho
https://orcid.org/0000-0001-7760-6914
http://lattes.cnpq.br/7519180451357839
Instituto Federal de Ciência e Tecnologia de Mato Grosso do Sul
E-mail: marlon.marinho@ifms.edu.br

ORIENTADOR:
Danilo Ribeiro de Sá Teles
https://orcid.org/0000-0001-9725-2762
http://lattes.cnpq.br/2528182839566669
Instituto Federal de Ciência e Tecnologia de Mato Grosso do Sul
E-mail: danilo.teles@ifms.edu.br

INSTITUTO FEDERAL
Mato Grosso do Sul

PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

2024

APÊNDICE B – QUESTIONÁRIO PRÉ-APLICAÇÃO DO PRODUTO EDUCACIONAL PARA OS ESTUDANTES

Prezado(a) estudante,

Por meio dos aspectos levantados neste questionário, pretendemos elaborar um produto educacional que promova uma explicação relacionada às consequências legais dos crimes cometidos no ambiente virtual, visto que, em sua futura profissão, um dos espaços em que atuará com frequência é o virtual. Sua participação é fundamental para a pesquisa, contribuindo assim para criação do podcast que pretendemos desenvolver como produto educacional do Mestrado Profissional em Educação Profissional e Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

Agradecemos a sua valiosa participação!

1. E-mail:

   _____

2. Está matriculado (a) no Curso Técnico Integrado em Informática para Internet - IFMS *Campus* Dourados?
   ( ) Sim ( ) Não

3. Concorda em participar desta pesquisa?
   ( ) Sim ( ) Não

QUESTIONÁRIO SOBRE CIBERCRIMES

4. Você já ouviu falar em Cibercrimes (Crimes Cibernéticos, Crimes Digitais) ?
   ( ) Sim ( ) Não

5. Para você, o que são cibercrimes?
   _____
   _____
   _____

6. Você considera importante discutir as consequências legais do cometimento de crimes virtuais em sala de aula? Sim ( ) Não ( )Justifique sua resposta.

   _____
   _____
   _____

7. Na sua opinião, o Curso Técnico Integrado em Informática para Internet, ofereceu em algum semestre o ensino das consequências legais da prática desses crimes? Explique

   _____
   _____
   _____

8. Elenque abaixo os Crimes Cibernéticos que você conhece ou já ouviu falar.

   _____
   _____
   _____

9. Como aluno (a) do Curso Técnico Integrado em Informática para Internet, você acredita que uma formação adicional que explique os principais crimes e as suas consequências, pode ajudá-lo(a) a ter uma atuação mais ética em sua profissão? Explique.

   _____
   _____
   _____
   _____

Agradecemos a sua participação!

As questões foram elaboradas/readaptadas com base em Pelloso (2021). PELLOSO, João Augusto Grecco. **Educação Para Cidadania: do contexto de produção ao contexto da prática.** 2021. 137 p. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, Campo Grande, MS, 2021.

APÊNDICE C – QUESTIONÁRIO PÓS-APLICAÇÃO DO PRODUTO EDUCACIONAL – ESTUDANTES

Prezado(a),

No intuito de avaliar o Podcast como um produto educacional que possa contribuir para que você, futuro Técnico em Informática para Internet receba uma formação essencial sobre as consequências legais dos crimes praticados no ambiente virtual, convidamos você a participar desta pesquisa respondendo o questionário a seguir. Sua participação é muito importante para a pesquisa.

Agradecemos a sua valiosa participação!

1. A forma como o podcast está estruturado é adequada ao alcance dos objetivos propostos

( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

2. As orientações repassadas no podcast são de fácil compreensão

( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

3. Os episódios dos podcasts são adequados para alcançar os objetivos propostos

( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

4. A linguagem utilizada no conteúdo do podcast é adequada para sua compreensão

( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

5. O recurso escolhido, o Podcast, é adequado para estudar as consequências dos cibercrimes
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

6. O conteúdo do podcast permite momentos de reflexão que sejam adequados aos assuntos tratados
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

7. O conteúdo do podcast é adequado ao alcance dos objetivos propostos
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

8. Considero que a realização do podcast, pode ser utilizada para complementar os ensinamentos obtidos em disciplinas que abordam o tema na instituição de ensino
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo

( ) discordo parcialmente
( ) discordo totalmente

09. Considero o podcast um recurso importante que os professores poderão indicar aos seus alunos para o esclarecimento sobre as consequências do cometimentos de crimes na Internet
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

10. Considero o podcast um recurso importante a ser utilizado pela instituição de ensino
( ) concordo totalmente
( ) concordo parcialmente
( ) não concordo, nem discordo
( ) discordo parcialmente
( ) discordo totalmente

Caso tenha marcado a opção discordo em algum item avaliado, por gentileza, contribua com sugestões de melhorias para aprimorarmos o curso. Caso queira, esse espaço também pode ser utilizado para elogios e reclamações.

_____
_____
_____
_____

Agradecemos a sua participação!

As questões foram elaboradas (readaptadas) com base em Alves Júnior (2021). ALVES JÚNIOR, Ivan José. **Ética e integridade na pesquisa: um curso on-line para jovens pesquisadores.** 2021. Dissertação (Mestrado em EPT) - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul - IFMS, [S. l.], 2021. Disponível em: https://educapes.capes.gov.br/handle/capes/597526. Acesso em: 9 dez. 2022.

APÊNDICE D - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RESPONSÁVEIS)

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE) – Questionário e/ou entrevista para responsáveis de estudantes do IFMS *Campus* Dourados

Convidamos o(a) estudante do IFMS que você é responsável legal para participar da pesquisa do Mestrado Profissional em Educação Profissional e Tecnológica – ProfEPT intitulada: **“ IMPLICAÇÕES LEGAIS DOS CRIMES CIBERNÉTICOS: UM SABER SISTEMATIZADO A FIM DE APERFEIÇOAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET”**, sob a responsabilidade do pesquisador Marlon Glauber Marinho e sob orientação do pesquisador Danilo Ribeiro de Sá Teles, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

O objetivo desta investigação é contribuir para que o Técnico em Informática para Internet receba uma formação básica, porém essencial, sobre as consequências legais das práticas dos crimes praticados no ambiente virtual, corroborando com o aprimoramento ético no desempenho de sua profissão. A pesquisa será realizada no IFMS *Campus* Dourados.

Ao final da pesquisa será apresentado um recurso pedagógico no formato de Podcast com o intuito de proporcionar que o estudante aprenda sobre as consequências legais acerca do cometimento dos crimes cibernéticos descritos na legislação brasileira. Buscando possibilidades de transformação das percepções identificadas no discurso dos participantes, que abordam o conhecimento prévio dos cibercrimes a partir da abordagem técnica para promover a aprendizagem.

Para que possamos elaborar o podcast precisamos conhecer as principais dúvidas dos estudantes, futuros profissionais, acerca das consequências penais dos crimes cibernéticos.

Para isso será realizada a aplicação de um questionário. Desta forma, o presente termo autoriza o envio do questionário no e-mail indicado para este fim, que passará por subsequente análise e identificação das informações.

Caso haja alguma dúvida no entendimento das respostas do questionário por parte dos pesquisadores existe a possibilidade de agendarmos uma entrevista para compreensão das respostas.

A participação na pesquisa é voluntária, ou seja, o(a) estudante não é obrigado(a) e possui plena autonomia para decidir se participa ou não, bem como retirar sua participação a qualquer momento, se assim desejar. Não terá prejuízo algum caso decida não consentir a participação ou desistir da mesma. Contudo, ela é muito importante para a execução da pesquisa.

Esta pesquisa apresenta riscos mínimos aos participantes, como por exemplo uma eventual quebra de confidencialidade pelo uso de dados, o que será minimizado pelo comprometimento dos pesquisadores em manter o anonimato das informações. Outro risco envolve a possibilidade de haver alguma forma de desconforto enquanto os participantes respondem às perguntas, o que também será minimizado pela conscientização do participante de que a sua identidade será mantida em sigilo e somente os pesquisadores terão acesso aos dados. Fica também garantida a indenização em casos de danos comprovadamente decorrentes da participação na pesquisa.

_____ _____
Rubrica responsável - participante Rubrica pesquisador

Dentre os benefícios da pesquisa, considera-se que a compreensão das consequências penais dos crimes cibernéticos possa ampliar a qualificação do futuro profissional e concomitantemente ampliar a preocupação de uma atuação mais ética em sua profissão.

Os dados obtidos serão armazenados pelo pesquisador principal durante cinco anos e depois serão incinerados ou deletados por definitivo após esse período. O TCLE e o TALE serão rubricados em todas as páginas e assinados em duas vias pelo pesquisador e pelo participante, sendo que ambos receberão uma via de cada documento.

Os resultados deste estudo serão utilizados para a construção do podcast e também poderá ser divulgado em eventos científicos, dissertação de mestrado e resumos, sem qualquer identificação dos participantes. Você poderá solicitar esclarecimentos sobre o trabalho a qualquer momento.

Em caso de dúvidas sobre a pesquisa você poderá entrar em contato com o pesquisador Marlon Glauber Marinho pelo telefone (67) 9.9648-5977 ou e-mail: marlon.marinho@ifms.edu.br, podendo solicitar esclarecimento por telefone, e-mail ou presencialmente.

_____
Assinatura do Participante ou responsável legal

E-mail para o envio do questionário: _____

Deseja receber o resultado da presente pesquisa por e-mail? ( ) Não ( ) Sim.
E-mail:_____

_____
Marlon Glauber Marinho
Pesquisador responsável

Data: _____/ _____/_____

APÊNDICE E - Termo de Consentimento Livre e Esclarecido

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE) – Questionário ou entrevista, para Estudantes maiores de 18 anos do IFMS *Campus* Dourados

Convidamos o(a) Sr(a) para participar, voluntariamente, da pesquisa do Mestrado em Educação Profissional e Tecnológica – ProfEPT, intitulada: “ **IMPLICAÇÕES LEGAIS DOS CRIMES CIBERNÉTICOS: UM CONHECIMENTO SISTEMATIZADO A FIM DE APERFEIÇOAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET**”, sob a responsabilidade do pesquisador Marlon Glauber Marinho e sob orientação do pesquisador Danilo Ribeiro de Sá Teles, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

O objetivo desta investigação é contribuir para que o Técnico em Informática para Internet receba uma formação básica, porém essencial, sobre as consequências legais das práticas dos crimes praticados no ambiente virtual, corroborando com o aprimoramento ético no desempenho de sua profissão. A pesquisa será realizada no IFMS *Campus* Dourados.

Ao final da pesquisa será apresentado um recurso pedagógico no formato de Podcast com o intuito de proporcionar que o estudante aprenda sobre as consequências legais acerca do cometimento dos crimes cibernéticos descritos na legislação brasileira. Buscando possibilidades de transformação das percepções identificadas no discurso dos participantes, que abordam o conhecimento prévio dos cibercrimes a partir da abordagem técnica para promover a aprendizagem.

Para que possamos elaborar o podcast precisamos conhecer as principais dúvidas dos estudantes, futuros profissionais, acerca das consequências penais dos crimes cibernéticos.

Para isso será realizada a aplicação de um questionário. Desta forma, o presente termo autoriza o envio do questionário no e-mail indicado para este fim, que passará por subsequente análise e identificação das informações.

A participação na pesquisa é voluntária, ou seja, o(a) Sr(a) não é obrigado(a) e possui plena autonomia para decidir se participa ou não, bem como retirar sua participação a qualquer momento, se assim desejar. Não terá prejuízo algum caso decida não consentir a participação ou desistir da mesma. Contudo, ela é muito importante para a execução da pesquisa.

Esta pesquisa apresenta riscos mínimos aos participantes: um dos riscos envolve eventual quebra de confidencialidade pelo uso de dados, uma vez que a coleta será online e não haverá identificação dos respondentes. Entretanto, os pesquisadores se comprometem a buscar manter o anonimato das informações. Outro risco envolve a possibilidade de haver alguma forma de desconforto enquanto os participantes respondem às perguntas. Nesse caso, orienta-se que os mesmos interrompam a coleta de dados. Fica, também, garantida a indenização em casos de danos comprovadamente decorrentes da participação na pesquisa.

_____ _____

Rubrica responsável - participante Rubrica pesquisador

Dentre os benefícios da pesquisa, considera-se que a compreensão das consequências penais dos crimes cibernéticos possa ampliar a qualificação do futuro profissional e concomitantemente ampliar a preocupação de uma atuação mais ética em sua profissão.

Os dados obtidos serão armazenados pelo pesquisador principal durante cinco anos e depois serão incinerados ou deletados por definitivo após esse período. O TCLE e o TALE serão rubricados em todas as páginas e assinados em duas vias pela pesquisador e pelo participante, sendo que ambos receberão uma via de cada documento.

Os resultados deste estudo serão utilizados para a construção do podcast e também poderá ser divulgado em eventos científicos, dissertação de mestrado e resumos, sem qualquer identificação dos participantes. Você poderá solicitar esclarecimentos sobre o trabalho a qualquer momento.

Em caso de dúvidas sobre a pesquisa você poderá entrar em contato com o pesquisador Marlon Glauber Marinho pelo telefone (67) 9.9648-5977 ou e-mail: marlon.marinho@ifms.edu.br, podendo solicitar esclarecimento por telefone, e-mail ou presencialmente.

Este Termo online é para certificar que eu li o termo de consentimento livre e esclarecido acima e concordo em participar deste estudo. Estou ciente que poderei me retirar do estudo a qualquer momento sem nenhum prejuízo.

( ) Aceito participar do estudo

( ) Não aceito participar do estudo

Dourados, MS _____/ _____/_____

_____ _____

Marlon Glauber Marinho
Pesquisador responsável

Assinatura do Participante

APÊNDICE F – Termo de Assentimento Livre e Esclarecido (TALE)

Você está recebendo este questionário porque seu representante legal indicou esse e-mail no Termo de Consentimento Livre e Esclarecido (TCLE). Você está sendo convidado a participar, voluntariamente, da pesquisa do Mestrado em Educação Profissional e Tecnológica – ProfEPT, intitulada: **"IMPLICAÇÕES LEGAIS DOS CRIMES CIBERNÉTICOS: UM CONHECIMENTO SISTEMATIZADO A FIM DE APERFEIÇOAR A FORMAÇÃO DO TÉCNICO EM INFORMÁTICA PARA INTERNET"**, sob a responsabilidade do pesquisador Marlon Glauber Marinho e sob orientação do pesquisador Danilo Ribeiro de Sá Teles, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul. Este estudo pretende contribuir para que o Técnico em Informática para Internet receba uma formação básica, porém essencial, sobre as consequências legais das práticas dos crimes praticados no ambiente virtual, corroborando com o aprimoramento ético no desempenho de sua profissão. A pesquisa está sendo realizada no IFMS *Campus* Dourados.

Ao final da pesquisa será apresentado um recurso pedagógico no formato de Podcast com o intuito de proporcionar que o estudante aprenda sobre as consequências legais acerca do cometimento dos crimes cibernéticos descritos na legislação brasileira. Buscando possibilidades de transformação das percepções identificadas no discurso dos participantes, que abordam o conhecimento prévio dos cibercrimes a partir da abordagem técnica para promover a aprendizagem.

Suas respostas são confidenciais e serão utilizadas de modo conjunto com os demais questionários, sem identificação do respondente. Para que possamos realizar análise de dados mais próxima ao real, necessitamos que responda com sinceridade às perguntas. Você poderá refletir se deseja participar desta pesquisa, consultando, se necessário, seus familiares ou outras pessoas que possam ajudá-lo na tomada de decisão livre e esclarecida. Salientamos que não há resposta certa ou errada, sinta-se à vontade para refletir em suas respostas.

Tendo em vista que as perguntas são pessoais, estas podem gerar algum incômodo. Porém, a decisão quanto a participação é totalmente sua. Assim, a qualquer momento pode interromper a participação, recusando-se a responder alguma pergunta. Ainda, conforme previstas na Cartilha dos Direitos Dos Participantes De Pesquisa, ficarão asseguradas, as seguintes proteções: a de receber assistência (integral e imediata) por danos, de forma gratuita; requerer indenização por danos; receber ressarcimento de gastos (incluindo os gastos de acompanhantes); ter acesso aos resultados dos exames realizados durante o estudo [...] (CONEP, 2021, p. 08).Também fica assegurado aos participantes da pesquisa as condições de acompanhamento, tratamento, assistência integral e orientação, conforme cada caso, enquanto estas se fizerem necessárias e em casos de despesas não previstas, decorrentes da participação na pesquisa. Conforme previsto no Código Civil (Lei nº 10.406 de 2002, artigos 927 a 954, Capítulos I (Da Obrigação de Indenizar) e II (Da Obrigação de Indenizar), Título IX (Da Responsabilidade Civil)), bem como na Resolução CNS n° 466 de 2012 (item IV.3), também fica garantida aos participantes da pesquisa indenização e reparação, tendo, assim, direito à indenização por parte do pesquisador [...] (CONEP, 2021, p. 09).

_____ _____

Rubrica responsável - participante Rubrica pesquisador