

EMENTA	
Área temática	II - Investigação policial
Disciplina	5 - Investigações especializadas
Módulo	j - Investigações de crimes cibernéticos
Código	II.5.j
<p>Mapa de competências</p> <p>A partir dos conhecimentos aplicados, embasados na relação ensino-aprendizagem, são competências decorrentes desse processo a compreensão pelo policial civil acerca dos crimes cibernéticos, e assim, da necessidade do estudo dos substratos para o seu enfrentamento, o domínio dos procedimentos operacionais, tecnologias e ferramentas próprias da apuração dessas infrações penais.</p>	
<p>Carga horária recomendada: 80 horas</p>	
<p>Descrição</p> <p>Tema que tem se tornado um desafio para a Polícia Judiciária, assim como para toda a sociedade, é o crime cibernético, e neste contexto, aduz Freitas¹ que:</p> <p style="padding-left: 40px;">A sociedade contemporânea é resultado de diversas transformações ocorridas ao longo do tempo e, por sua própria natureza, permanece em constante evolução. Nesse sentido, uma das ferramentas mais revolucionárias e transformadoras já criadas, que proporcionou a interação em tempo real entre pessoas e hoje, até entre coisas espalhadas pelo mundo, assim como a expansão e o desenvolvimento de quase todas as atividades atualmente realizadas, é a internet.</p> <p>O desenvolvimento da internet e o uso massivo da tecnologia, principalmente em decorrência de mudanças no modo de viver das pessoas, impulsionados por situações como globalização e pandemia, acelerou notadamente o uso da rede mundial de computadores para cometimento de infrações penais. Mudou-se o perfil do delinquente, mudou-se radicalmente o modus operandi e dessa forma, também se viu necessário mudar os mecanismos e técnicas investigativas para fazer frente à cibercriminalidade.</p> <p>Portanto, é fundamental para a Polícia Civil do Estado de Goiás a qualificação de seus servidores no que tange à investigação de crimes cibernéticos através de um processo de ensino-aprendizagem no ambiente corporativo.</p>	
<p>Objetivo</p> <p>Criar condições para que o policial civil possa:</p> <ul style="list-style-type: none"> ➤ ampliar conhecimentos para compreender os fatores que fomentam a criminalidade cibernética, os aspectos peculiares desses crimes, como a escalabilidade, o anonimato e a sensação de impunidade que gera no meio social; ➤ desenvolver e exercitar habilidades para implementar a repressão aos crimes cibernéticos através de modernos métodos e ferramentas disponíveis às forças policiais; ➤ fortalecer atitudes para despertar-se para a importância do conhecimento antecipado de fatores de risco e de oportunidades para a redução dos 	

¹ FREITAS, S. De S.; Cibercriminalidade: um “vírus” fortalecido pela pandemia. Direito Policial: temas atuais, org: BELIATO, A. M.; IBRAHIN, F. I. D. Salvador: Juspodvim, 2021. p. 523

Índices dos crimes cibernéticos.

Conteúdo Programático

1. História da internet
2. Protocolos de Internet
 - 2.1 IP
 - 2.1.1 IPv4
 - 2.1.2 IPv6
 - 2.2 HTTP / HTTPs
 - 2.3 Outros protocolos
3. Definições importantes
 - 3.1 Crime cibernético
 - 3.2 Vírus de computador
 - 3.3 *Hacker*
 - 3.4 *Cracker*
 - 3.5 Vírus de *boot*
 - 3.6 *Time bomb*
 - 3.7 *Worm*
 - 3.8 Cavalo de Tróia / *Trojans*
 - 3.9 Estado *Zombie*
 - 3.10 Vírus de Macro
 - 3.11 *Malware*
 - 3.12 *Ransomware*
 - 3.13 Antivírus
4. Delegacia estadual de repressão a crimes cibernéticos
 - 4.1 Criação
 - 4.2 Atribuições
5. Legislação aplicável ao crime cibernético
 - 5.1 Lei 9.296/1996
 - 5.2 Lei 9.613/1998
 - 5.3 Lei 12.683/2012
 - 5.4 Lei 12.737/2012
 - 5.5 Lei 12.965/2014
 - 5.6 Código Penal Brasileiro e suas atualizações
 - 5.7 Código de Processo Penal Brasileiro e suas atualizações
 - 5.8 Estatuto da Criança e do Adolescente
6. Tipos de ataques cibernéticos e identificação de origem
 - 6.1 Ataques de *malware*
 - 6.2 *Phishing*
 - 6.3 *Vishing*
 - 6.4 *Smishing*
 - 6.5 DoS - *Denial-of-Service*
 - 6.6 DDoS – *Distributed Denial-of-Service*
 - 6.7 *Cryptojacking*
 - 6.8 Kits de *Exploits*
 - 6.9 Outros
7. Crimes cibernéticos e procedimento de investigação
 - 7.1 Fraudes por e-mail e pela internet
 - 7.2 Subtração de dados financeiros e de identificação
 - 7.3 Subtração e venda de dados corporativos

- 7.4 Extorsão cibernética
- 7.5 Espionagem cibernética
- 7.6 Pedofilia
- 7.7 *Cyberbullying*
- 7.8 Outros
- 8. Investigação cibernética
 - 8.1 Evidência digital
 - 8.1.1 Identificação
 - 8.1.2 Preservação
 - 8.1.3 Formalização
 - 8.2 Identificação do perfil do usuário
 - 8.2.1 *Facebook*
 - 8.2.2 *Instagram*
 - 8.2.3 *Twitter*
 - 8.2.4 *Whatsapp*
 - 8.2.5 *Telegram*
 - 8.2.6 *Youtube*
 - 8.2.7 Outras redes sociais
 - 8.3 Solicitações cadastrais
 - 8.3.1 Operadoras de telefonia
 - 8.3.2 Provedores de internet
 - 8.3.3 Outras empresas
 - 8.4 Plataformas de solicitação para autoridades de aplicação da lei
 - 8.4.1 Cadastramento do investigador
 - 8.4.2 Funcionalidades disponíveis e sua utilidade na investigação
 - 8.4.2.1 Dados do usuário
 - 8.4.2.2 Telefone
 - 8.4.2.3 Endereço IP
 - 8.4.2.4 Endereço MAC
 - 8.4.2.5 Logs de acesso
 - 8.4.2.6 Mensagens trocadas entre usuários
 - 8.4.2.7 Mensagens instantâneas
 - 8.4.2.8 Páginas administradas pelos usuários
 - 8.4.2.9 Solicitação de preservação
 - 8.4.2.10 Outras funcionalidades
 - 8.4.3 Solicitações emergenciais
 - 8.4.4 Recebimento e análise das informações disponibilizadas
 - 8.5 Medidas cautelares judiciais
 - 8.5.1 Afastamento de sigilo telemático
 - 8.5.2 Interceptação de dados telemáticos
 - 8.5.3 Solicitação de bloqueio ou retirada de conteúdo
 - 8.5.4 Outras solicitações
 - 8.6 Local de Crime Cibernético
 - 8.6.1 Preservação de local
 - 8.6.2 Redução de danos e orientação à vítima
 - 8.6.3 *Softwares* de auxílio
 - 8.6.4 Apreensão de objetos e otimização da prova
 - 8.7 Infiltração virtual
 - 8.8 Outras técnicas de investigação
 - 8.9 Relatório policial de investigação de crimes cibernéticos

9. Perícia cibernética

9.1 Solicitação

9.2 Quesitos

9.3 Análise de laudo pericial

10. Origem criminosa em outro estado ou país

10.1 Competência Investigativa

10.2 Encaminhamento e recebimento de procedimentos

11. Relação Interinstitucional

11.1 Operadoras de telefonia

11.2 Provedores de conexão

11.3 Provedores de conteúdo

11.4 Ministério Público

11.5 Poder Judiciário

11.6 Outros

Bibliografia indicada

FREITAS, S. De S.; **Cibercriminalidade: um “vírus” fortalecido pela pandemia. Direito Policial: temas atuais**, org: BELIATO, A. M.; IBRAHIN, F. I. D. Salvador: Juspodvim, 2021.

Estratégias de ensino e aprendizagem

As estratégias de ensino e aprendizagem estão dispostas na MACPC/GO e devem ser escolhidas pelo facilitador, restringindo-se a métodos e técnicas adequados aos objetivos.

Avaliação de Aprendizagem

A avaliação do aluno seguirá as disposições do Regimento Interno da ESPC. Serão ainda utilizadas avaliações de aprendizagem diagnóstica, formativa e somativa, como forma de aperfeiçoamento do ensino.

Referências Bibliográficas

FREITAS, S. De S.; **Cibercriminalidade: um “vírus” fortalecido pela pandemia. Direito Policial: temas atuais**, org: BELIATO, A. M.; IBRAHIN, F. I. D. Salvador: Juspodvim, 2021.