

Curso de Cibercrimes – TJBA
Prof. Walter Aranha Capanema

1. Descrição do Conteúdo do Curso:

Módulo I: Módulo 1: Introdução aos Cibercrimes

Tema: Introdução aos Cibercrimes.

Ementa: Arquitetura da Internet. Características dos crimes eletrônicos. Mitos.

Carga Horária: 20 Horas.

Conteúdo Programático:

Tema 1: Arquitetura da Internet: Números IP. Nomes de domínio. Servidores. Classificação. Cookies. Proxies. Cloudcomputing. Registros (logs). Conceitos tecnológicos no Marco Civil.

Tema 2: Crimes eletrônicos: conceito, classificação. Tipificação de condutas. Autoria. Materialidade. Local do Crime.

Tema 3: Características e mitos dos crimes eletrônicos

Módulo 2: Cibercrimes em espécie

Tema: Cibercrimes em espécie

Disciplina: Direito Penal, Direito Processual Penal, Direito Constitucional

Ementa:

Tema 1: Crimes contra a honra. Pornografia de vingança (*revengeporn*).

Tema 2: Crimes contra a Honra. Pornografia de Vingança. Crimes de ódio. “Lei Lola”. Apologia de crime. Incitação ao crime.

Tema 3: Inserção de dados falsos em sistemas de informação. Modificação ou alteração não autorizada em sistemas de



informações.

Tema 4: Falsa identidade. Divulgação de segredo.

Tema 5: Pirataria (de dados e de software).

Tema 6: Fraudes bancárias (*phishingscam*). Ransomware.
Estelionato

Tema 7: Pornografia infantil.

Tema 8: “Lei Carolina Dieckmann” e “Lei Azeredo

Módulo 3: Provas em ambiente Digital

Tema: Provas em ambiente digital

Disciplina: Direito Penal, Direito Processual Penal, Direito Constitucional, Perícia Forense Computacional

Ementa:

Tema 1: Provas em ambiente digital. Introdução. Provas em ambientes virtuais

Tema 2: Interceptação de dados telemáticos

Tema 3: Infiltração de Agentes

Tema 4: Perícia Forense computacional

Tema 5: Investigação em fontes abertas.

2. Bibliografia:

CARVALHO, Luis Gustavo Grandinetti Castanho de. Processo Penal e (em face da) Constituição: Princípios constitucionais do Processo Penal. 3. ed. Rio de Janeiro: Lumen Juris, 2004.

CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003. 19

CONSELHO DA EUROPA. Convention on Cybercrime. Disponível



em: . Acesso em: 17 out. 2012.

VENÂNCIO, Pedro Dias. Lei do cibercrime: anotada e comentada. Portugal: Coimbra, 2011.

FERREIRA, Érica Lourenço de Lima. Internet: Macrocriminalidade e jurisdição internacional. Curitiba: Juruá, 2007.

GLENNY, Misha. Mercado Sombrio: o cibercrime e você. São Paulo: Companhia Das Letras, 2011.

MITNICK, Kevin D.; Simon, William L. A arte de enganar. São Paulo: Pearson Makron Books, 2003.

POULSEN, Kevin. Kingpin: how one hacker took over the billion-dollar cibercrime underground. Estados Unidos: Broadway, 2011.

RODRIGUES, Benjamim Silva. Direito Penal Especial: Direito Penal informático-digital. Portugal: Coimbra, 2009. (Tomo I).

SARLET, Ingo Wolfgang (org). Direitos Fundamentais, Informática e Comunicação: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007.

CAPANEMA, Walter Aranha. A Interceptação de Dados Informáticos no Direito Brasileiro. Disponível em: . Acesso em: 8 out. 2012.

_____. O vírus de computador e o crime de dano. Disponível em: . Acesso em: 8 out. 2012. 20 FARMER, Dan;

VENEMA, Wietse. Perícia forense computacional: teoria e prática aplicada. São Paulo: Pearson, 2011. GOMES, Luiz Flávio;

SANCHES, RaúlServini. Interceptação Telefônica: Lei 9,296, De 24.07.96. São Paulo: Revista dos Tribunais, 1997.

GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. Disponível em: . Acesso em: 17out. 2012.

PRADO, Geraldo. Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça. 2. ed. Rio de Janeiro: Lumen Juris, 2006.



TURNER, David. Para os filhos dos filhos de nossos filhos: uma visão da sociedade Internet. São Paulo: Plexus Editora. 1999.

3. Programação:

1º dia – 28/3
8:00 – 8:15: credenciamento e boas vindas
8:15 – 10:00: Módulo I
10:00 – 10:15: Intervalo
10:15 – 12:00: Módulo I
12:00 – 14:00: intervalo para almoço
14:00 – 16:00: Módulo I (continuação)
16:00 – 16:15: Intervalo
16:15 - 17:30: Módulo I (continuação)

2º dia – 29/3
8:00 – 10:00: Módulo II (continuação)
10:00 – 10:15: Intervalo
10:15 – 12:00: Módulo II (continuação)
12:00 – 14:00: intervalo para almoço
14:00 – 16:00: Módulo III
16:00 – 16:15: Intervalo
16:15 - 17:30: avaliação dos alunos



Informações Pedagógicas:

Metodologia empregada: ativa, com a discussão de casos concretos.

Avaliação:

- Participação durante as aulas
- Avaliação final (estudo de caso)

Objetivo Geral: O magistrado, ao concluir o curso, será capaz de tipificar as condutas criminosas que ocorrem no ambiente digital por meio da apresentação e estudo dos novos fatos jurídicos criminosos que ocorrem na Internet, bem como meios de investigação e suas consequências.

Objetivos Específicos:

- O magistrado será capaz de aplicar o conteúdo de forma que desenvolva o pensamento crítico para repensar sua missão de julgar a partir do aperfeiçoamento das suas virtudes fundamentais a legislação;
- Desenvolver esses conhecimentos voltados para um estudo que o faça conhecer os detalhes dos principais cibercrimes.
- Empregar em casos concretos Através do estudo o magistrado deverá usar na prática jurídica as principais técnicas e os procedimentos da investigação



Proposta:

Para a ministração do Curso de Cybercrimes de 20 horas de duração no Tribunal de Justiça do Estado da Bahia, a ser realizado nas datas de 28 e 29 de março, de 2019, com o fornecimento de material didático (arquivos de Powerpoint e apostila), estimo os honorários em **R\$ 7.620,00 (sete mil e seiscentos e vinte reais)**.

Rio de Janeiro, 3 de fevereiro de 2019



Walter Aranha Capanema
Representante – Smart3 Consultoria e Treinamento LTDA.

