

Curso: Cibercrimes 2.0: Novas Ameaças para um Mundo Conectado

Modalidade: à distância

Período: 01 de outubro a 07 de novembro de 2019.

Carga Horária: 30 horas.

Coordenação/Tutoria: Walter Capanema

PROGRAMA

Ambientação – 1^a a 3 de outubro

Módulo I – 4 a 10 de outubro

Carga horária: 6 horas

Conteúdo Programático:

Tema 1: Atualizações sobre os cibercrimes I

Tema 2: Atualizações sobre os cibercrimes II

Objetivos Específicos:

- Avaliar as novidades legislativas, fáticas e jurídicas dos cibercrimes;
- Aplicar, no caso concreto, as novas leis sobre cibercrimes.

Metodologia: Metodologia participativa por meio de debates virtuais realizados no Fórum de Discussão (fatos reais do dia a dia, jurisprudência, questões complexas propostas para discussão).

Avaliação de aprendizagem: Questão Formativa apresentada ao final de cada unidade e baseada na discussão teórica/prática dos temas propostos. Estudo de Casos.

Bibliografia:

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 cybercrime underground. Estados Unidos: Broadway, 2011.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos.** Rio de Janeiro: Brasport, 2012.

Módulo II – 11 a 17 de outubro

Carga horária: 6 horas

Conteúdo Programático:

Tema 1: Perícia Forense em imagens digitais

Tema 2: Perícia Forense em Sistemas Windows

Tema 3: Perícia Forense em redes de computadores

Tema 4: Perícia Forense em Dispositivos móveis

Tema 5: Antiforense digital

Objetivos Específicos:

- Assinalar as principais espécies de perícia forense computacional
- Formular quesitos para perícias forenses computacionais

Metodologia: Metodologia participativa por meio de debates virtuais realizados no Fórum de Discussão (fatos reais do dia a dia, jurisprudência, questões complexas propostas para discussão).

Avaliação de aprendizagem: Questão Formativa apresentada ao final de cada unidade e baseada na discussão teórica/prática dos temas propostos. Estudo de Casos.

Bibliografia:

FARMER, Dan; VENEMA, Wietse. **Perícia forense computacional:** teoria e prática aplicada. São Paulo: Pearson, 2011.

VELHO, Jesus Antonio (Org.). **Tratado de Computação Forense.** Campinas: Millennium, 2016.

Módulo III – 18 a 24 de outubro

Carga horária: 6 horas

Conteúdo Programático:

Tema 1: Investigação na *Deep Web*

Tema 2: Investigação avançada em smartphones

Tema 3: Investigação avançada no *Whatsapp*

Tema 4: Investigação avançada em fontes abertas

Tema 5: Outras Investigações avançadas

Objetivos Específicos:

- Identificar as principais espécies de investigação em cibercrimes
- Avaliar os requisitos das investigações sobre Cibercrimes

Metodologia: Metodologia participativa por meio de debates virtuais realizados no Fórum de Discussão (fatos reais do dia a dia, jurisprudência, questões complexas propostas para discussão).

Avaliação de aprendizagem: Questão Formativa apresentada ao final de cada unidade e baseada na discussão teórica/prática dos temas propostos. Estudo de Casos.

Bibliografia:

BARRETO, Alessandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme.

Investigação Digital em Fontes Abertas. 2. ed. São Paulo: Brasport, 2017.

TANENBAUM, Andrew S.. **Redes de computadores. 1 ed. 4ª tiragem.** Rio de Janeiro: Campus, 2003.

Módulo IV – 25 a 31 de outubro

Carga horária: 6 horas

Conteúdo Programático:

Tema 1: Introdução à Segurança da Informação

Tema 2: Cuidados com a Segurança da Informação

Objetivos Específicos:

- Identificar as principais regras de segurança da informação
- Aplicar, na atividade profissional e na vida pessoal, as normas de segurança da informação.

Metodologia: Metodologia participativa por meio de debates virtuais realizados no Fórum de Discussão (fatos reais do dia a dia, jurisprudência, questões complexas propostas para discussão).

Avaliação de aprendizagem: Questão Formativa apresentada ao final de cada unidade e baseada na discussão teórica/prática dos temas propostos. Estudo de Casos.

Bibliografia:

CABRAL, Carlos; CAPRINO, Willian Okuhara (Org.). **Trilhas em Segurança da**

Informação: caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

FONTES, Edilson. **Políticas e Normas para a Segurança da Informação.** Rio de Janeiro: Brasport, 2012.

Avaliação Final – 01 a 07 de novembro

Carga horária: 6 horas

Questão formativa sobre os temas desenvolvidos ao longo do curso.

FORMADORES:

Tutor:

Walter Aranha Capanema

Advogado e professor. Professor Responsável pelo EAD/EMERJ. Pós-graduado pela EMERJ-UNESA. Professor com certificados FOFO (presencial e EAD).

Docentes vídeo-aula:

Módulo 1: Walter Aranha Capanema

Advogado e professor. Professor Responsável pelo EAD/EMERJ. Pós-graduado pela EMERJ-UNESA. Professor com certificados FOFO (presencial e EAD).

Módulo 2: Gilberto Neves Sudre Filho

Perito forense computacional.

Módulo 3: Guilherme Caselli de Araujo

Delegado de Polícia.

Módulo 4: Lincoln Werneck Araújo Vaz

Analista em Segurança da Informação.