UNIVERSIDADE PRESBITERIANA MACKENZIE

PRÓ-REITORIA DE EXTENSÃO E EDUCAÇÃO CONTINUADA

Coordenadoria de Cursos de Educação Continuada

Curso de especialização em **Computação Forense**

Estrutura Curricular – disciplina/carga horária.

Computação Forense: Direito e Segurança	
Atos Ilícitos e Crimes Eletrônicos	32h/a
Fundamentos do Processo Civil e Penal	32h/a
Técnicas de Segurança Computacional	32h/a
Gestão de Segurança da Informação	32h/a
Carga horária total	**128h/a**
Computação Forense: Auditoria e Perícia	
Fraudes Corporativas	32h/a
Perícia Forense Computacional – Teoria	32h/a
Legislação Aplicada à Perícia Forense Computacional	32h/a
Auditoria em Sistemas de Informação	32h/a
Carga horária total	**128h/a**
Computação Forense: Biometria e Investigações	
Investigação de Sistemas	32h/a
Perícia Forense Computacional – Prática	32h/a
Técnicas de Evasão	32h/a
Fundamentos das Aplicações Biométricas	32h/a
Carga horária total	**128h/a**
Módulo: Aplicação do Conhecimento	**48h/a online**

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

IDENTIFICAÇÃO DA DISCIPLINA (01)

1. Nome da Disciplina: Atos Ilícitos e Crimes Eletrônicos

2. Carga Horária: 32 h

3. Ementa: A disciplina estuda os atos ilícitos do campo cível e os crimes tipificados no Código Penal e em legislação especial, que antes eram praticados no mundo físico, e passaram a ser realizados através do mundo eletrônico, como é o caso das transferências ilícitas nos serviços conhecidos como "Internet Banking" e "Mobile Banking". Além disso, traz a discussão sobre novas condutas ilícitas que ainda não são tipificadas em legislação pátria, como a invasão de sistemas ou a disseminação de vírus, mas constituem objeto de Projeto de Lei dos Crimes da Informática.

4. Objetivo: Proporcionar ao aluno conhecimento para lidar com os atos ilícitos e com os crimes praticados através dos meios eletrônicos (internet, mobile, ATMs, etc), especialmente para poder entender os novos mecanismos para a comprovação da autoria e materialidade delitivas neste novo ambiente.

5. Conteúdo Programático: Teoria dos atos no Direito Civil. Classificações e meios onde são praticados. Criminologia nos meios eletrônicos. Crimes contra o patrimônio. Crimes contra a honra. Crimes contra a pessoa. Fraudes eletrônicas. Interceptação de dados telemáticos e informáticos. Inviolabilidade de dados informáticos. Pedofilia na rede. Crimes contra a propriedade imaterial. Concorrência desleal. Local e tempo do crime. Classificação jurídico-penal de condutas. Convenção de Budapeste para o combate de crimes eletrônicos. Projeto de Lei dos Crimes da Informática.

6. Bibliografia Básica:

BLUM, Renato Opice; BRUNO, Marcos da Silva Gomes; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 2006.

LUCCA, Newton; SIMÃO FILHO, Adalberto. Direito e Internet - aspectos jurídicos relevantes. São Paulo: Edipro, 2000.

ROSSINI, Augusto. Informática, Telemática e Direito Penal, Memória Jurídica, São Paulo:2004.

7. Bibliografia Complementar:

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

CASTRO, Carla Rodrigues Araújo de. Crimes de Informática. Rio de Janeiro: Lumen Juris, 2001.

INELLAS, Gabriel Cesar Zaccaria de, Crimes na Internet, Juarez de Oliveira, São Paulo: 2004.

REINALDO FILHO, Demócrito. Direito da Informática – Temas polêmicos. Bauru: Edipro, 2002.

IDENTIFICAÇÃO DA DISCIPLINA (02)

1 Nome da Disciplina: Fundamentos do Processo Civil e Penal

2 Carga Horária: 32 h

3 Ementa: Durante o curso, serão descritos os procedimentos gerais adotados na produção de provas do Processo Civil e em uma investigação criminal, desde a abertura do inquérito policial, com a análise e compreensão da cena do crime, o requerimento e a determinação de busca e apreensão, o transporte de equipamento e o seu envio à perícia. Serão estudados também os requisitos legais previstos para essa fase.

4 Objetivo: Familiarizar os alunos com o procedimento de produção de provas civil e com a investigação criminal.

5 Conteúdo Programático: Produção de provas no Processo Civil. Inquérito policial. Peculiaridades sobre a cena do crime computacional. Busca e apreensão. Possibilidades: duplicação pericial e transporte de equipamento. Requisitos para a licitude da prova.

6 Bibliografia Básica:

BLUM, Renato Opice; BRUNO, Marcos da Silva Gomes; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 2006.

CARNEIRO, José Reinaldo Guimarães. O Ministério Público e suas investigações independentes. São Paulo: Malheiros, 2007.

SOUZA, Fernando de Jesus. Perícia e investigação de fraude. 3.ª ed. – Goiânia: AB, 2006.

7. Bibliografia Complementar:

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

CASTELLA, Eduardo Marcelo. Investigação criminal e informática – inteligência artificial x boletim de ocorrência. Curitiba: Juruá, 2005.

CHOUKR, Fauzi Hassan. Garantias constitucionais na investigação criminal. 3.ª ed. – Rio de Janeiro: Lumen Juris, 2003.

TUCCI, Rogério Lauria. Ministério Público e Investigação Criminal. São Paulo: RT, 2004.

IDENTIFICAÇÃO DA DISCIPLINA (03)

1. Nome da Disciplina: Técnicas de Segurança Computacional

2. Carga Horária: 32 h

3. Ementa: Análise dos controles criptográficos: sistemas criptográficos, assinatura digital, gerência de chaves e *Public Key Infrastucture*. Avaliação dos mecanismos que promovem a segurança em sistemas distribuídos: autenticação, autorização e controle de acesso. Análise da segurança corporativa: política de senhas, revisão de perfis de acesso, monitoramento, segurança de ativos e cultura de segurança: *disclaimers* e avisos. Estudo de casos envolvendo tecnologias de segurança de sistemas computacionais.

4. Objetivo: Expor a importância da garantia do funcionamento das tecnologias de segurança em sistemas computacionais.

5. Conteúdo Programático: Controles criptográficos: sistemas criptográficos, assinatura digital, gerência de chaves e PKI. Segurança em Sistemas Distribuídos: autenticação, autorização e controle de acesso. Segurança corporativa: política de senhas, revisão de perfis de acesso, monitoramento, segurança de ativos e cultura de segurança: *disclaimers* e avisos. Estudo de casos - tecnologias de segurança de sistemas computacionais.

6. Bibliografia Básica:

CALOYANNIDES, Michael A. Privacy protection and computer forensics. 2.ª ed. – Massachusetts: Artech House, 2004.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

FONTES, Edison. Vivendo a segurança da informação – Orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

7. Bibliografia Complementar:

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo Corrêa. Segurança com redes privadas virtuais – VPNs. Rio de Janeiro: Brasport, 2006.

JONES, Keith J.; BEJTLICH, Richards; ROSE, Curtis W. Real Digital Forensics. Computer Security and Incident Response: Massachusetts: Addison Wesley, 2006.

MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Olivier de; MCKEMMISH, Rod. Computer and intrusion forensics. Massachusetts: Artech House, 2003.

IDENTIFICAÇÃO DA DISCIPLINA (04)

1. Nome da Disciplina: Gestão de Segurança da Informação

2. Carga Horária: 32 h

3. Ementa: Estudo da gestão de segurança da informação: mecanismos, modelos, normas, políticas e propriedades. Análise da motivação e dos meios para evitar a ocorrência das fraudes. Estudo de casos envolvendo a gestão de segurança da informação. Estudo de casos envolvendo tecnologias de segurança de sistemas computacionais.

4. Objetivo: Expor a importância da gestão das tecnologias de segurança em sistemas computacionais.

5. Conteúdo Programático: Fundamentos de gestão da segurança computacional: propriedades, políticas, violações, modelos, serviços e mecanismos. Estudo de casos sobre gestão de segurança da informação.

6. Bibliografia Básica:

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

CALOYANNIDES, Michael A. Privacy protection and computer forensics. 2.ª ed. – Massachusetts: Artech House, 2004.

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

FONTES, Edison. Vivendo a segurança da informação – Orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

7. Bibliografia Complementar:

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo Corrêa. Segurança com redes privadas virtuais – VPNs. Rio de Janeiro: Brasport, 2006.

JONES, Keith J.; BEJTLICH, Richards; ROSE, Curtis W. Real Digital Forensics. Computer Security and Incident Response: Massachusetts: Addison Wesley, 2006.

MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Olivier de; MCKEMMISH, Rod. Computer and intrusion forensics. Massachusetts: Artech House, 2003.

IDENTIFICAÇÃO DA DISCIPLINA (05)

1. Nome da Disciplina: Fraudes Corporativas

2. Carga Horária: 32 h

3. Ementa: Demonstrar os crimes e as fraudes em geral atualmente praticados no mundo corporativo. Abordar os tipos mais comuns, as condutas de risco, os mecanismos de proteção e o perfil dos criminosos e fraudadores.

4. Objetivo: Proporcionar aos alunos o conhecimento para enfrentar e lidar com os ilícitos praticados em corporações.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

5. Conteúdo Programático: Introdução às fraudes corporativas. Os números das fraudes corporativas. Gerenciamento de risco. O uso da tecnologia. Auditoria contínua. Monitoramento de processos. Os tipos mais comuns. Perfil do funcionário fraudador.

6. Bibliografia Básica:

CASEY, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools & Technology. Boston, MA: Academic Press, 2002.

CASEY, Eoghan. Digital evidence and computer crime. Boston, MA: Academic Press, 2000.

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Massachusetts: Addison-Wesley Professional, 2001.

7. Bibliografia Complementar:

KURTZ, George; McCLURE, Stuart; SCAMBRAY, Joel. Hacking Exposed: Network Security Secrets & Solutions. Computing McGraw-Hill, 1999.

MANDIA, Kevin; PEPE, Matt; PROSISE, Chris. Incident Response and Computer Forensics. Osborne: McGraw-Hill, 2003.

MELO, Sandro. Computação Forense com Software Livre. Editora Alta Books, 2008.

NG, Reynaldo. Forense Computacional Corporativa. Rio de Janeiro: Editora Brasport, 2007.

PARODI, Lorenzo. Manual das Fraudes. Rio de Janeiro: Editora Brasport, 2008.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

IDENTIFICAÇÃO DA DISCIPLINA (06)

1. Nome da Disciplina: Legislação Aplicada à Perícia Forense Computacional

2. Carga Horária: 32 h

3. Ementa: Estudo das normas, políticas e leis nacionais e internacionais concernentes à Perícia Forense Computacional dos atos ilícitos e dos crimes praticados nos meios eletrônicos, bem como a mais recente jurisprudência que lhes diga respeito.

4. Objetivo: Informar os alunos sobre toda a legislação nacional e internacional existente sobre o tema, além das mais recentes decisões dos tribunais.

5. Conteúdo Programático: A Perícia Forense Computacional no Direito Brasileiro: Constituição Federal, Código de Processo Civil, Código de Processo Penal, Consolidação das Leis do Trabalho, Código de Defesa do Consumidor e leis extravagantes. Perícia Forense Computacional no Direito Internacional e no Direito Comparado. Jurisprudência nacional e estrangeira.

6. Bibliografia Básica:

BLUM, Renato Opice; BRUNO, Marcos da Silva Gomes; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 2006.

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

INELLAS, Gabriel Cesar Zaccaria de, Crimes na Internet, Juarez de Oliveira, São Paulo: 2004.

7. Bibliografia Complementar:

REINALDO FILHO, Demócrito. Direito da Informática – Temas polêmicos. Bauru: Edipro, 2002.

ROSA, M.V.F. Perícia Judicial – Teoria e Prática. Porto Alegre: Sérgio Antônio Fabris Editor, 1999.

YEE, Z. C. Perícia Civil - Manual Prático. Curitiba; Editora Juruá, 2002.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

IDENTIFICAÇÃO DA DISCIPLINA (07)

1. Nome da Disciplina: Perícia Forense Computacional – Teoria

2. Carga Horária: 32 h

3. Ementa: Apresentação dos elementos essenciais da perícia forense computacional (identificação, preservação, análise das evidências e apresentação da análise), cadeia de custódia, suas ferramentas e duplicação pericial. Análise da recuperação de dados em disco, local das evidências, senhas e proteções, técnicas de identificação de autoria no protocolo TCP/IP, pela análise de registros (LOG), em redes de IP, na análise de pacotes e de arquivos. Análise do laboratório de Computação Forense e das técnicas na elaboração do laudo pericial.

4. Objetivo: Estudar os princípios básicos da Ciência Forense e áreas de atuação. Apresentar as novas tecnologias disponíveis nas áreas de Computação Forense, permitindo aos alunos a identificação de ferramentas tecnológicas para processamento e análise de evidências, bem como o desenvolvimento de sistemas de apoio às áreas de Computação Forense.

5. Conteúdo Programático: Perícia forense: conceito e elementos. Identificação das evidências. Preservação das evidências. Análise das evidências. Apresentação da análise. Cadeia de custódia. Ferramentas. Duplicação pericial. Recuperação de dados em disco. Local das evidências. Senhas e proteções. Identificação de autoria. Laboratório de Computação Forense. Laudo pericial.

6. Bibliografia Básica:

CARVEY, Harlan. Windows Forensics and Incident Recovery. Massachusetts: Addison-Wesley, 2005.

CASEY, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools & Technology. Boston, MA: Academic Press, 2002.

CASEY, Eoghan. Digital evidence and computer crime. Boston, MA: Academic Press, 2000.

7. Bibliografia Complementar:

COSTA, Marcelo Antonio Sampaio Lemos. Computação Forense. Campinas: Millennium, 2003.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Massachusetts: Addison-Wesley Professional, 2001.

KURTZ, George; McCLURE, Stuart; SCAMBRAY, Joel. Hacking Exposed: Network Security Secrets & Solutions. Computing McGraw-Hill, 1999.

MANDIA, Kevin; PEPE, Matt; PROSISE, Chris. Incident Response and Computer Forensics. Osborne: McGraw-Hill, 2003.

IDENTIFICAÇÃO DA DISCIPLINA (08)

1. Nome da Disciplina: Auditoria em Sistemas de Informação

2. Carga Horária: 32 h

3. Ementa: Compreensão das regras de conduta emitidas por todo o mundo (Sarbanes-Oxley, Basiléia II, NBR 17799, etc) cujos textos revelam a preocupação com a segurança da informação, em todos os setores da economia. Análise da sua aplicabilidade no monitoramento dos atos praticados pelos funcionários nos computadores das empresas, no controle de acesso a aplicativos, conteúdos e sistemas, além da videovigilância e outras tecnologias.

4. Objetivo: Ensinar aos alunos os princípios e regras concernentes às auditorias em sistemas de informação, desenvolver uma posição crítica à adoção de medidas de controles eletrônicos por parte das empresas aos seus empregados, a fim de diminuir os riscos operacionais corporativos.

5. Conteúdo Programático: Regulamento interno de segurança da informação. Gestão de Riscos. Ensurance. Regras da ABNT (17799, 27001). Direito Comparado (58/2002/CE, SOX, Basiléia II e etc). Monitoramento dos atos dos funcionários das empresas. Videovigilância. Termos de uso de e-mail. Privacidade em ambiente corporativo.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

6. Bibliografia Básica:

BELMONTE, Alexandre Agra – O monitoramento da correspondência eletrônica nas relações de trabalho, São Paulo : LTr, 2004.

BLUM, Renato M.S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coordenadores) – Manual de Direito Eletrônico e Internet, São Paulo: Aduaneiras, 2006.

JONES, Keith J.; BEJTLICH, Richards; ROSE, Curtis W., Real Digital Forensics. Computer Security and Incident Response, Addison Wesley, Massachusetts, 2006.

7. Bibliografia Complementar:

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Massachusetts: Addison-Wesley Professional, 2001.

KURTZ, George; McCLURE, Stuart; SCAMBRAY, Joel. Hacking Exposed: Network Security Secrets & Solutions. Computing McGraw-Hill, 1999.

MANDIA, Kevin; PEPE, Matt; PROSISE, Chris. Incident Response and Computer Forensics. Osborne: McGraw-Hill, 2003.

IDENTIFICAÇÃO DA DISCIPLINA (09)

1. **Nome da Disciplina:** Investigação de Sistemas
2. **Carga Horária:** 32 h
3. **Ementa:** Analisar-se-ão os processos em execução, portas abertas, análise dos arquivos de logs, investigação dos registros e compartilhamentos em Windows, Linux, Microsoft IIS, servidores Web e e-mails. Em seguida, serão examinadas as técnicas para identificação dos usuários do sistema operacional e para a recuperação de arquivos. Também será analisada a identificação dos *sites* acessados, arquivos temporários da internet, histórico e favoritos.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

4. **Objetivo:** Ensinar os alunos a identificar os principais vestígios em um sistema operacional referentes aos aspectos técnicos, usuários, arquivos e sites acessados.

5. **Conteúdo Programático:** Investigação em Windows e em Linux: sistema, usuário, arquivo e Web. Microsoft IIS: versões e arquivos de log. Investigação em servidores Web: aviso, sondagem, ataques e outras ocorrências. Investigação de e-mails: cabeçalho, corpo e leitores de e-mails.

6. **Bibliografia Básica:**

BENNETT, Geoff. Designing TCP/IP internetworks. New Jersey: John Wiley & Sons, 1996.

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo Corrêa. Segurança com redes privadas virtuais – VPNs. Rio de Janeiro: Brasport, 2006.

7. Bibliografia Complementar:

MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Olivier de; MCKEMMISH, Rod. Computer and intrusion forensics. Massachusetts: Artech House, 2003.

NEMETH, Evi; SNYDER, Garth; SEEBASS, Scott; HEIN, Trent R. UNIX Administration Handbook. 3.ª ed. – Prentice Hall, 2000.

NEMETH, Evi; SNYDER, Garth; HEIN, Trent R. Manual complete do Linux: guia do administrador. Pearson Education do Brasil / Prentice Hall, 2003.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

IDENTIFICAÇÃO DA DISCIPLINA (10)

1. Nome da Disciplina: Técnicas de Evasão

2. Carga Horária: 32 h

3. Ementa: Apresentar as dificuldades existentes na detecção de intrusos. Explicar os fundamentos dessa detecção. Estudar as regras para análise das assinaturas de ataques. Determinar as formas existentes de burlar sistemas de detecção de intrusos. Analisar a criptografia e a esteganografia. Analisar a interceptação de dados no hardware e softwares que desempenham essa função, bem como a extração de dados do *sniffer*. Entender como funcionam os firewalls e os IDS, baseados em assinaturas e em eventos. Aprender a detectar a origem dos ataques e estudar os ataques polimórficos e '0 DAY'.

4. Objetivo: Instruir os alunos acerca da detecção de intrusão, com o estudo dos ataques e dos meios para detectá-los.

5. Conteúdo Programático: Anatomia, mecanismo e origem dos ataques. Criptografia e esteganografia. Interceptação de dados: o hardware e o software. Extração de dados do *sniffer*. Ataques polimórficos e '0 DAY'. Firewall *versus* IDS. Tipos de IDS: HIDS, NIDS, IDS ativo e IDS passivo. IDS baseados em assinaturas e em eventos. Proteção do IDS. Problemas com detecção de intrusão.

6. Bibliografia Básica:

CAVALCANTI, A. & LIRA, E. Grafoscopia Essencial. Porto Alegre; Editora Sagra,1996.

CALOYANNIDES, Michael A. Privacy protection and computer forensics. 2.ª ed. – Massachusetts: Artech House, 2004.

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

7. Bibliográfica Complementar:

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Massachusetts: Addison-Wesley Professional, 2001.

MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Olivier de; MCKEMMISH, Rod. Computer and intrusion forensics. Massachusetts: Artech House, 2003.

IDENTIFICAÇÃO DA DISCIPLINA (11)

1. Nome da Disciplina: Fundamentos das Aplicações Biométricas

2. Carga Horária: 32 h

3. Ementa: Análise da Biometria, visando a identificar as etapas de um sistema computacional para reconhecimento/verificação dos seguintes elementos: digitais, face, voz, íris, retina, veias, mão, pé, assinaturas e manuscritos.

4. Objetivo: Estudar a área de Biometria, com a finalidade de explorar as aplicações da biometria no controle de acesso e autenticação de usuários em aplicações computacionais e suas implicações legais.

5. Conteúdo Programático: Identificação das tecnologias biométricas digitais (face, voz, íris, retina, veias, mão, pé, assinaturas e manuscritos) utilizadas no controle de acesso e autenticação de usuário sem aplicações computacionais. Benefícios e fragilidades das tecnologias biométricas. Padrões internacionais de troca de informações biométricas. Análise dos padrões internacionais de desenvolvimento de aplicações biométricas. Leis que protegem as pessoas, empresas e a sociedade em geral sobre a captura, armazenamento e troca de informações biométricas, no que diz respeito à segurança e à privacidade. Dicas para peritos em avaliações em sistemas computacionais que utilizam tecnologias biométricas.

6. Bibliografia Básica:

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

CAVALCANTI, A. & LIRA, E. Grafoscopia Essencial. Porto Alegre; Editora Sagra,1996.

CENTURION, Virgílio. Excelência em biometria. São Paulo: Cultura Médica, 2006.

REBELLO FILHO, Hidelbrando Magno; FALAT, Luiz Roberto Ferreira. Fraudes Documentais – Como Ocorrem. Curitiba: Juruá, 2004.

7. Bibliografia Complementar:

VIGLIAZZI, Douglas. Biometria – Medidas de Segurança. 2.ª ed. Visual Books, 2006.

JUSTINO, E. J. R., BORTOLOZZI, F., SABOURIN, R. A Autenticação de Manuscritos Aplicada à Análise Forense de Documentos In: TIL- 1o. Workshop em Tecnologia da Informação e da Linguagem Humana. São Carlos, 2003.

TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan A. Tecnologias Biométricas Aplicadas a la Seguridad. Madrid: Ra-Ma, 2005.

IDENTIFICAÇÃO DA DISCIPLINA (12)

1. **Nome da Disciplina:** Perícia Forense Computacional – Prática
2. **Carga Horária:** 32 h
3. **Ementa:** Verificação prática dos elementos essenciais da perícia forense computacional (identificação, preservação, análise das evidências e apresentação da análise), cadeia de custódia, suas ferramentas e duplicação pericial. Análise laboratorial da recuperação de dados em disco, local das evidências, senhas e proteções, técnicas de identificação de autoria no protocolo TCP/IP, pela análise de registros (LOG), em redes de IP, na análise de pacotes e de arquivos. Análise do laboratório de Computação Forense e das técnicas na elaboração do laudo pericial em casos concretos.
4. **Objetivo:** Testar a aplicabilidade dos princípios básicos da Ciência Forense e áreas de atuação. Manusear as novas tecnologias disponíveis nas áreas de Computação Forense, permitindo aos alunos a familiarização com as ferramentas tecnológicas para processamento e análise de evidências, bem como o desenvolvimento prático de sistemas de apoio às áreas de Computação Forense.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

5. **Conteúdo Programático:** Perícia forense: elementos práticos. Identificação das evidências. Preservação das evidências. Análise das evidências. Apresentação da análise. Cadeia de custódia. Ferramentas. Duplicação pericial. Recuperação de dados em disco. Local das evidências. Senhas e proteções. Identificação de autoria. Laboratório de Computação Forense. Laudo pericial.

6. **Bibliografia Básica:**

CARVEY, Harlan. Windows Forensics and Incident Recovery. Massachusetts: Addison-Wesley, 2005.

CASEY, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools & Technology. Boston, MA: Academic Press, 2002.

CASEY, Eoghan. Digital evidence and computer crime. Boston, MA: Academic Press, 2000.

7. **Bibliografia Complementar:**

COSTA, Marcelo Antonio Sampaio Lemos. Computação Forense. Campinas: Millennium, 2003.

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática: ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

KRUSE, Warren G.; HEISER, Jay G. Computer forensics: incident response essentials. Massachusetts: Addison-Wesley Professional, 2001.

KURTZ, George; McCLURE, Stuart; SCAMBRAY, Joel. Hacking Exposed: Network Security Secrets & Solutions. Computing McGraw-Hill, 1999.

MANDIA, Kevin; PEPE, Matt; PROSISE, Chris. Incident Response and Computer Forensics. Osborne: McGraw-Hill, 2003.

SANS InfoSec Reading Room (SANS Institute) - http://www.sans.org/rr

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

IDENTIFICAÇÃO DA DISCIPLINA (13)

1. **Nome da Disciplina:** Aplicação do Conhecimento

2. **Carga Horária:** 48 h

3. **Ementa:** A disciplina promove o desenvolvimento do Trabalho de Aplicação de Conhecimento, com base no método prático e aplicado, o qual direciona o aluno para a resolução de um desafio ou problema real vivenciado em um contexto institucional/pessoal, utilizando os conceitos e práticas abordados ao longo do curso.

4. **Objetivo:** Capacitar o participante para investigar, analisar e compreender as causas e as implicações dos desafios em um contexto institucional/pessoal; e com base no diagnóstico e na pesquisa bibliográfica, propor soluções e ações detalhadas, visando à resolução de problemas ou oportunidades reais e pontuais enfrentadas nesse contexto institucional/pessoal.

5. **Conteúdo Programático:**

   - Definição do problema/oportunidade/desafio a ser resolvido;
   - Descrição das características gerais do contexto institucional/pessoal;
   - Diagnóstico das origens e implicações do desafio a ser resolvido;
   - Pesquisa bibliográfica sobre os temas relacionados com o desafio do contexto institucional/pessoal;
   - Proposição de soluções e ações detalhadas para a resolução do desafio.

6. **Bibliografia:**

   Básica:

MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597010770.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**

MARCONI, Marina de Andrade. Técnicas de pesquisa. 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597013535.

YIN, Robert K. Estudo de caso : planejamento e métodos. 5. Porto Alegre Bookman 2015 1 recurso online ISBN 9788582602324.

GIL, Antonio Carlos. Estudo de caso : fundamentação científica ; subsídios para coleta e análise de dados ; como redigir o relatório. São Paulo Atlas 2009 1 recurso online ISBN 9788522464753.

Complementar:

MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597010770.

MARCONI, Marina de Andrade. Técnicas de pesquisa. 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597013535.

YIN, Robert K. Estudo de caso : planejamento e métodos. 5. Porto Alegre Bookman 2015 1 recurso online ISBN 9788582602324.

GIL, Antonio Carlos. Estudo de caso : fundamentação científica ; subsídios para coleta e análise de dados ; como redigir o relatório. São Paulo Atlas 2009 1 recurso online ISBN 9788522464753.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● **www.mackenzie.br** ● **ccec.atendimento@mackenzie.br**