



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
Computação forense e perícia digital

Sumário

1. Nome do Curso e Área do Conhecimento.....	3
2. Características Técnicas do Curso.....	3
3. Público-Alvo	3
4. Critérios de Seleção	4
5. Justificativa do Curso	4
6. Objetivos do Curso	4
7. Competências e Habilidades do Curso	5
8. Metodologia de Ensino e Aprendizagem	5
9. Estágio Não Obrigatório.....	8
10. Matriz Curricular	10
11. Carga Horária.....	11
12. Conteúdo Programático.....	11
13. Infraestrutura Física e Pedagógica.....	20

1. Nome do Curso e Área do Conhecimento

Nome do Curso: Computação forense e perícia digital

Área de Avaliação (CAPES): CIÊNCIA DA COMPUTAÇÃO

Grande Área (CAPES): 10000003 CIÊNCIAS EXATAS E DA TERRA

Área do Conhecimento (CAPES): 10300007 CIÊNCIA DA COMPUTAÇÃO

Classificação OCDE: Computação e Tecnologias da Informação e Comunicação (TIC)

2. Características Técnicas do Curso

Modalidade: Educação a Distância

Número máximo de vagas por Polo/Unidade: 1000 alunos

Período de Oferecimento: O curso possui entrada intermitente, respeitadas as datas de início e de fim cadastradas na oferta, bem como observado o período indicado para a sua integralização.

Limitações legais

Resolução CNE/CES Nº 1, de 06 de abril de 2018, que estabelece normas para o funcionamento de cursos de pós-graduação lato sensu.

O candidato deverá ser graduado com diploma devidamente registrado segundo as normas estabelecidas pelo MEC.

3. Público-alvo

Destinado aos profissionais com curso superior nas áreas coligadas à Tecnologia da Informação, Sistemas de Informação, Engenharia e Ciência da Computação, ou que possuam notório saber em T.I.C., com curso superior de

graduação reconhecido pelo MEC que desejem atuar como Assistente Judicial e ou Investigador Corporativo com características multidisciplinares nas áreas legais, normativas, regulamentares e tecnológicas.

4. Critérios de Seleção

O ingresso na pós-graduação será realizado por meio de inscrição no portal da Instituição e entrega dos documentos solicitados. Em seguida, analisados pela área competente.

5. Justificativa do Curso

O uso de dispositivos digitais na vida cotidiana cresce à medida que as pessoas integram a tecnologia em suas vidas. Concomitante ao grande aumento da interconectividade aliado aos diversos recursos e dispositivos computacionais ligados a Internet, traz como reflexo direto a sociedade o aumento exponencial de crimes e delitos, onde o computador ou celular é usado como agente facilitador de tais ações. Esse domínio dos dispositivos eletrônicos na sociedade é equiparado à crescente presença de provas coletadas por dispositivos digitais em casos cíveis, trabalhistas e criminais.

Os crimes e contravenções podem ter várias testemunhas digitais, sendo seus atos registros por celulares, câmeras, CFTV dentre outros, sendo que este número de eventos versus aparatos aumenta se contarmos com a coleta de outros fatos diversos, como a confirmação de uma simples aceite em um contrato digital, ou a validação de uma foto ou postagem em uma rede social, onde o computador pode ser usado como meio o fim de execução de um evento, que pode ou não ser ilícito. Diante de tal cenário, faz-se necessário, impreterivelmente, a atuação de um profissional multidisciplinar, que transite harmonicamente entre as áreas da Tecnologia e do Direito, e que possa dar “vida” a estas evidências digitais.

Como acontece com outras provas físicas, o maior desafio então, é saber, qual o correto uso dos métodos aplicados para que possam virar provas futuras em

um Tribunal, protocolos, procedimentos e ferramentais adequadas, perfazendo a íntegra irrefutável da aquisição, das coletas e preservação dos indícios e materiais obtidos num local de crime.

As evidências que as formaram, bem como a manutenção de sua integridade, são vitais para que os processos resistam aos desafios jurídicos das quais serão submetidas, e é de responsabilidade do Perito Judicial determinar como as evidências serão coletadas, processadas, preservadas e apresentadas.

6. Objetivos do Curso

6.1. Objetivo Geral

Preparar o profissional para atuar nas esferas Cível, Trabalhistas e Criminal como auxiliar da justiça com bases técnicas-jurídicas nas demandas contenciosa e consensual, emitindo Laudos, Manifestações e Pareceres suportando o juízo em suas decisões.

6.2. Objetivos Específicos

- Aprender a modular a Ciência Forense como Método Científico multidisciplinar.
- Entender o e escopo de atuação do Perito Judicial e Assistente Técnico Forense.
- Aplicar procedimentos válidos para extração, coleta e preservação de indícios digitais para formar prova válida em um tribunal.
- Examinar, analisar e correlacionar as evidências, formatando-as no relatório final consubstanciado no Laudo Técnico Pericial.
- Familiarizar-se com as práticas anti-forense apresentadas, para que possam virar provas futuras em um Tribunal.”

7. Competências e Habilidades do Egresso

Competências

Atuar como Perito e ou Assistente Técnico, quando demandado pela Justiça para oferecer laudos e pareceres com bases técnicas-científicas em processos judiciais em que se envolvam pessoas jurídicas, físicas e órgãos públicos, onde o resultado de seu trabalho passa a constar uma das peças que compõem um processo judicial. Também pode atuar em uma organização privada ou pública como profissional responsável pela investigação em crimes digitais.

Habilidades

- Formatar conhecimento jurídico específico capaz de compreender os processos legais básicos e questões jurídicas, incluindo as regras de provas oriundas o Código de Processo Pena e Código de Processo Civil.
- Aplicar técnicas e procedimentos para questionar em alto nível e se dispor a investigar opiniões e ou fatos que podem sugerir ocultação, ofuscação de provas ou sugerir fraude processual.
- Aplicar padrões aceitos internacionalmente, a exemplo da ISO-IEC, NIST, e IEEE-RFC na identificação, coleta, aquisição, e preservação dos indícios e provas.
- Criar relatórios técnico com bases metodológicas a exemplo da ABNT, que apresentem de forma robusta e simples, o resultado de seus exames e análises para o juízo ou tribunal.
- Utilizar ferramentais forenses, seja de forma nativa em um sistema Operacional, GPL ou proprietárias para aplicar nos procedimentos de aquisição, coleta, exame e análise.

8. Metodologia de Ensino e Aprendizagem

O desenvolvimento das disciplinas do curso se dará no ambiente virtual, onde o aluno cumprirá 40 horas por disciplina.

Estas 40 horas são compostas pelo estudo dos diversos insumos pedagógicos disponibilizados, como:

- ✓ materiais de leitura;
- ✓ videoaulas;
- ✓ slides;
- ✓ podcasts;
- ✓ indicações de leituras extras como artigos e capítulos de livros.

Como parte do modelo acadêmico, também contabilizamos:

- ✓ a interação com os tutores para esclarecimentos de dúvidas pedagógicas (via Fórum);
- ✓ a realização da avaliação disciplinar pelo aluno.

Vale ressaltar que cada aluno é único e tem seu próprio tempo para aprendizagem. Alguns conseguem assimilar o conteúdo com mais agilidade, outros precisam retomar as leituras e videoaulas para tornar sua aprendizagem efetiva.

O tempo gasto pelo aluno para o entendimento de cada disciplina depende também da sua familiaridade com o tema, ou seja, o conhecimento prévio que o aluno tem em relação a temática abordada.

No ambiente virtual, o aluno encontrará o conteúdo das disciplinas, organizados em temas/webaulas.

Para cada um deles, o aluno realizará um conjunto de atividades baseadas em leitura de textos de fundamentação teórica e acesso a recursos audiovisuais.

Um tutor apoiará as atividades realizadas no ambiente virtual, atendendo o aluno nas suas dúvidas por meio de ferramentas de comunicação.

O aluno, ao iniciar os seus estudos, terá um encontro presencial para acolhida/ambientação; esse encontro terá como objetivos:

- ✓ Integrar o aluno ao curso de Pós-Graduação.
- ✓ Dialogar e esclarecer as dúvidas sobre a proposta pedagógica do curso e as regras acadêmicas.
- ✓ Apresentar ao aluno o Ambiente Virtual de Aprendizagem (o primeiro acesso; o envio de documentos; os serviços de secretaria e financeiro; a disciplina Ambientação; a tutoria online; o boletim acadêmico; as disciplinas e seus conteúdos; a biblioteca virtual; entre outros).
- ✓ Proporcionar um momento de Network aos pós-graduandos.

Avaliação do Desempenho do Aluno

O aluno deverá realizar as atividades propostas no ambiente virtual. A realização das atividades irá compor sua frequência no curso, que será considerada para a sua aprovação.

A atividade avaliativa que o aluno realizará para compor a sua média é a Avaliação Virtual (AV); essa atividade é obrigatória e estará disponível no Ambiente Virtual de Aprendizagem – AVA, conforme cronograma de seu curso.

Para a aprovação em cada uma das disciplinas, o aluno deverá obter frequência de, no mínimo, 75% (setenta e cinco por cento) e nota igual ou superior a 7,0 (sete).

As notas devem ser expressas no intervalo de 0 (zero) a 10 (dez).

O aluno que obtiver média inferior a 7,0 (sete) nas disciplinas terá direito ao Programa de Dependência e Recuperação – PDR, mediante a solicitação de requerimento e respeitando o período de jubramento do curso.

O PDR será realizado no ambiente virtual de aprendizagem, sendo que o aluno terá acesso ao conteúdo da disciplina e realizará uma Avaliação Virtual - AV, e a nota obtida substituirá a média do aluno.

Para a obtenção do **Certificado** de Pós-graduação *Lato Sensu* – especialização, o aluno deverá cumprir todas as condições seguintes:

- ✓ Frequência mínima de 75% (setenta e cinco por cento) em todas as disciplinas;
- ✓ Nota igual ou superior a 7,0 (sete) em todas as disciplinas.

Certificação

O Certificado de conclusão de curso de Especialização será acompanhado por histórico escolar, em cumprimento às exigências da Resolução CNE/CES nº1, de 06 de abril de 2018, da Câmara de Educação Superior do Conselho Nacional de Educação.

Composição do Corpo Docente

O corpo docente do curso é constituído por profissionais qualificados, com comprovado saber em sua área de atuação, conforme Resolução CNE/CES nº1, de 06 de abril de 2018, sendo integrado, no mínimo, por 30% (trinta por cento) de portadores de título de pós-graduação *stricto sensu*, isto é, portadores de títulos de Mestrado e Doutorado, obtidos em programas de pós-graduação *stricto sensu* devidamente reconhecidos pelo poder público em território nacional, ou revalidados, conforme legislação vigente. Os demais docentes são certificados em nível de especialização, pós-graduação *lato sensu*, de reconhecida capacidade técnico-profissional.

9. Estágio Não Obrigatório

O estágio curricular não obrigatório tem como finalidade estimular o aluno a desenvolver atividades extracurriculares, para que possa inter-relacionar os conhecimentos teóricos e práticos adquiridos durante o curso e aplicá-los na solução de problemas reais da profissão, proporcionando o desenvolvimento da análise crítica e reflexiva para os problemas socioeconômicos do país, de acordo com a Resolução de Estágio curricular não obrigatório vigente na Instituição.

O estágio curricular não obrigatório do curso de Pós-Graduação *Lato Sensu* segue as diretrizes estabelecidas pela Lei Nº 11.788/2008.

Os principais objetivos da prática do estágio curricular não obrigatório são:

I. proporcionar o exercício do aprendizado comprometido com a realidade socioeconômica-política do país;

II. propiciar a realização de experiências de ensino e aprendizagem visando à educação profissional continuada, alicerçada no desenvolvimento de competências e habilidades e ao exercício do pensamento reflexivo e criativo; e

II. incentivar o trabalho de pesquisa e investigação científica, visando ao desenvolvimento da ciência, da tecnologia e da cultura.

A carga horária é definida pela concedente de estágio, não podendo ultrapassar a carga horária máxima de 6 (seis) horas diárias e 30 (trinta) horas semanais, as quais podem ser realizadas em empresas públicas ou privadas, instituição de pesquisa, órgãos governamentais e não governamentais, e as próprias unidades da Universidade, desde que sigam às condições adequadas para que o estagiário possa aprofundar os seus conhecimentos teóricos e práticos adquiridos no curso.

Para o Curso de Pós-Graduação EAD, a prática do estágio curricular não obrigatório é permitida durante a vigência do curso, não podendo exceder em um mesmo campo de estágio o período de 2 (dois) anos.

Os estágios curriculares não obrigatórios devem estar apoiados em Termo de Compromisso e de comum acordo com a Instituição, devendo explicitar não somente os aspectos legais específicos, como também os aspectos educacionais e de compromisso com a realidade social.

O Planejamento do Estágio Curricular Não Obrigatório é de responsabilidade do coordenador de curso/professor orientador e também do Departamento de Estágios.

10. Matriz Curricular

DISCIPLINAS	CH PRÁTICA	CH TEÓRICA	CH TOTAL
Ambientação	0 h	0 h	0 h
Introdução à computação forense	0 h	40 h	40 h
Cibercrimes, responsabilidade penal e civil	0 h	40 h	40 h
Segurança em redes de computadores	0 h	40 h	40 h
Lei Geral de Proteção de Dados	0 h	40 h	40 h

Criptografia hash e hacking	0 h	40 h	40 h
Procedimentos, técnicas e ferramentas forenses	0 h	40 h	40 h
Auditoria de Sistemas	0 h	40 h	40 h
Práticas periciais em registros audiovisuais	0 h	40 h	40 h
Investigação remota de sistemas e técnicas de evasão	0 h	40 h	40 h

11. Carga Horária

A carga horária de 360h constitui o conteúdo ministrado em 9 (nove) disciplinas.

12. Conteúdo programático

Disciplina: Ambientação

Ementa: Histórico da Educação a Distância. Legislação da Educação a Distância no Brasil. Potencialidades da Educação a Distância. Flexibilidade de Acesso. Tecnologias para apoio à pesquisa. Aprendizagem colaborativa. Características do aluno na EAD. Boa convivência virtual: netiquetas.

Competências e Habilidades:

- Identificar as características do aluno da modalidade de educação a distância;
- Utilizar ferramentas tecnológicas de apoio a pesquisa;
- Comunicar-se com clareza e assertividade oralmente e por escrito;

- Gerenciar tempo e atividades de estudo.

Conteúdo Programático 1: Histórico da Educação a Distância.

Conteúdo Programático 2: Legislação da Educação a Distância no Brasil.

Conteúdo Programático 3: Potencialidades da Educação a Distância.

Conteúdo Programático 4: Flexibilidade de Acesso.

Conteúdo Programático 5: Tecnologias para apoio à pesquisa.

Conteúdo Programático 6: Aprendizagem colaborativa.

Conteúdo Programático 7: Características do aluno na EAD.

Conteúdo Programático 8: Boa convivência virtual: netiquetas.

Bibliografia básica:

GOTTARDI, M. de L. A autonomia na aprendizagem em educação a distância: competência a ser desenvolvida pelo aluno. **Associação Brasileira de Educação a Distância**, São Paulo, v. 14, n. 8, p. 110-123, dez, 2015.

MORAN, J. M. MASETTO, M. T. BEHRENS, M. A. **Novas Tecnologias e Mediação Pedagógica**. 21. ed. Campinas, SP: Papirus, 2013.

PIVA, D. J. PUPO, R. GAMEZ, L. OLIVEIRA, S. **EAD na Prática: Planejamento, métodos e ambientes de educação online**. São Paulo: Elsevier, 2011.

Bibliografia Complementar:

ALVES, L. Educação a distância: conceitos e história no Brasil e no mundo. **Associação Brasileira de Educação A Distância**, São Paulo, v. 10, n. 7, p.85-92, out. 2011.

MAIA, Carmen; MATTAR, João. **ABC da EaD: a educação a distância hoje**. São Paulo: Prentice Hall, 2007.

MOORE, Michael G., **Educação a distância**: sistemas de aprendizagem on-line. 3. ed., São Paulo: Cengage Learning, 2013.

Disciplina: Introdução à computação forense.

Ementa: Introdução à computação forense. Computação forense para segurança digital. Processos de Análise Forense. Identificação de Ataques. Reconstituição de Ataques. Recuperação de desastres

Competências e Habilidades:

- Conhecer os principais aspectos de análise forense para identificação de ataques.
- Conhecer as ferramentas, procedimentos e técnicas utilizados para identificação de ataques.
- Compreender a importância de se reconstituir o sistema e preservar os dados e as provas após um ataque.

Conteúdo Programático 1: Computação forense para segurança digital.

Conteúdo Programático 2: Processos de Análise Forense.

Conteúdo Programático 3: Identificação e reconstituição de ataques.

Conteúdo Programático 4: Recuperação de desastres.

Bibliografia Básica:

ATHAYDE, Vallim Adriano Penedo de. **Forense computacional e criptografia**. São Paulo: Editora Senac, 2019

FARMER, Dan. **Perícia forense computacional**: teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2007.

MELO, Sandro. **Computação Forense com Software Livre**. Rio de Janeiro: Editora Alta Books, 2009.X

Bibliografia Complementar:

BONI, Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Grupo GEN Editora Forense, 2018.

GALVAO, Ricardo Kléber M. **Introdução à análise forense em redes de computadores**. São Paulo: Editora Novatec, 2013.

NORTHCUTT, Stephen. **Como detectar invasão em redes: Um guia para analistas**. Rio de Janeiro: Ciência Moderna, 2000.

Disciplina: Cibercrimes , responsabilidade penal e civil

Ementa: Cibercriminologia e a fenomenologia dos delitos informáticos os reflexos da globalização no direito penal tradicional. A sociedade virtual do risco. A criminalidade complexa do século XXI. A engenharia social a serviço do crime. Regulação legislativa no âmbito penal nacional e internacional. Sobre cibercrimes. Breves considerações sobre a convenção internacional de budapest sobre cibercriminalidade. O tratamento legislativo no brasil relacionado aos delitos informáticos e a lei nº 12.737/2012 (lei carolina dieckman). A legislação penal mundial no combate e prevenção da delinquência informática. Conceito, características e a classificação dos cibercrimes. Conceito e evolução dos delitos informáticos. A classificação dos cibercrimes e o direito penal. O bem jurídico tutelado pelo direito penal. Tempo e lugar do crime. Dos crimes. Invasão ilegal à sistemas e dispositivos informáticos. A criação de vírus informático para fins ilícitos. O crime de pedofilia na internet e o estatuto da criança e do adolescente. Revenge porn ou sexting. A criminalização da fake news. Sequestro de dados na internet (ransomware). Dano informático.

Competências e Habilidades:

- Aprimorar a discussão acerca dos crimes virtuais
- Abordar as consequências dos atos praticados no ambiente virtual - responsabilidade penal e civil.
- Capacitar o aluno a compreensão da fase de investigação de um ilícito virtual

- Desenvolver a habilidade de produção de provas em ambiente virtua

Conteúdo Programático 1: Cibercriminologia e a fenomenologia dos delitos informáticos. Os reflexos da Globalização no Direito Penal Tradicional. A Sociedade Virtual do Risco. A Criminalidade Complexa do Século XXI. A Engenharia Social a serviço do crime.

Conteúdo Programático 2: Regulação legislativa no âmbito penal nacional e internacional. Sobre cibercrimes. Breves considerações sobre a Convenção Internacional de Budapest sobre Cibercriminalidade. O tratamento legislativo no Brasil relacionado aos delitos informáticos e a Lei nº 12.737/2012 (Lei Carolina Dieckman). A legislação penal mundial no combate e prevenção da delinquência informática. Responsabilidade Penal e Civil.

Conteúdo Programático 3: Conceito, características e a classificação dos cibercrimes. Conceito e evolução dos Delitos Informáticos. A classificação dos Cibercrimes e o Direito Penal. O Bem Jurídico Tutelado pelo Direito Penal. Tempo e Lugar do Crime

Conteúdo Programático 4: Dos crimes. Invasão ilegal à sistemas e dispositivos informáticos. A criação de vírus informático para fins ilícitos. O crime de pedofilia na Internet e o Estatuto da Criança e do Adolescente. Revenge Porn ou Sexting. A criminalização da Fake News. Sequestro de Dados na Internet (Ransomware). Dano informático.

Bibliografia Básica:

WENDT, Emerson. Direito e TI - CyberCrimes. Livraria do advogado. Rio de Janeiro:2019.

COLLI, Maciel. Cibercrimes. Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Juruá. 2019.

BARRETO, Alessandro; BRASIL, Beatriz. Manual de Investigação Cibernética. À Luz do Marco Civil da Internet. Brasport. 2016

Bibliografia Complementar:

JORGE, Vigor Vinícios Nogueira. Investigação Criminal Tecnológica - Volume 1. Brasport. 2018.

NORAT, Markus, et. Al. Direito Digital. Responsabilidade Civil e Criminal na Internet. Clube dos Autores. 2018

BREWER, Russell, et. Al. Cybercrime Prevention: Theory and Applications. Palgrave Pivot; Edição: 1st ed. 2019

Disciplina: Segurança em redes de computadores

Ementa: Introdução à arquitetura de redes. Protocolos de comunicação. Ameaças, Falhas e Vulnerabilidades. Ferramentas de Segurança e de recuperação de desastre. Segurança em redes sem fio. Código criptográficos e os princípios da segurança da Informação

Competências e Habilidades:

- Conhecer as vulnerabilidades e principais formas de ataques nas diferentes camadas de rede.
- Atuar na prevenção e reação à ataques cibernéticos.
- Atuar na garantia de privacidade e segurança no fluxo de informações das organizações.

Conteúdo Programático 1: Introdução à arquitetura de redes e protocolos de comunicação e segurança em redes sem fio.

Conteúdo Programático 2: Criptografia e princípios da segurança da Informação.

Conteúdo Programático 3: Ameaças, falhas e vulnerabilidades

Conteúdo Programático 4: Ferramentas de segurança e recuperação de desastre

Bibliografia Básica:

BROWN, Lawrie; STALLINGS, William. **Segurança de Computadores:** Princípios e Práticas. Rio de Janeiro: Elsevier Brasil, 2017.

CERT.br.- **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <https://www.cert.br/>. Acesso em 26 nov. 2019.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

STALLINGS, William. **Criptografia e Segurança de Redes**. 4. ed. - São Paulo: Pearson Prentice Hall, 2008

Bibliografia Complementar:

BARRETO, Jeanine dos Santos [et al.]. **Fundamentos de segurança da informação**. Porto Alegre: SAGAH, 2018.

COOLINS, Michael. **Network Security Through Data Analysis**. 2. ed. O'Reilly Media, 2014.

GOODRICH, Michael T; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP**. 3. ed. Rio de Janeiro: Alta Books, 2017.

NUNAN, Angelo Eduardo; FARIAS, Frank Douglas Cruz de; SANTIAGO, Marcos Fabiano P. **Segurança de redes**. Manaus: UEA Edições, 2010.

TANENBAUM, Andrew S.; WHETERHALL, David. **Redes de Computadores**. São Paulo, Pearson Prentice Hall, 2011.

Disciplina: Lei Geral de Proteção de Dados.

Ementa: Direitos humanos. Direitos fundamentais. Direito à vida privada. Direito à proteção de dados. Legislação brasileira de proteção de dados: Marco Civil da Internet, Lei do Cadastro Positivo e Lei de Acesso à Informação. Regulamento Europeu de proteção de dados – GDPR. Privacy by design. Lei Geral de Proteção de Dados Pessoais - LGPD. Agentes de tratamento. Controlador. Operador. Responsabilidades. Bases Legais de tratamento de dados. Ressarcimentos de danos. Encarregado pelo Tratamento de Dados – DPO. Segurança da Informação. Boas práticas e governança. Autoridade Nacional de Proteção de Dados. Fiscalização. Sanções administrativas.

Competências e Habilidades:

- Compreender as legislações nacionais e internacionais de proteção de dados pessoais. Compreender as implicações da LGPD no Direito Empresarial. Desenvolver a habilidade de analisar violações de dados pessoais, avaliar riscos e propor soluções. Capacitar o aluno para que possa prestar consultoria ou analisar sua própria empresa em busca de uma adequação legal. Propiciar um conhecimento amplo sobre a proteção de dados pessoais e suas implicações nas empresas.

Conteúdo Programático 1: Direitos humanos. Direitos fundamentais. Direito à vida privada. Direito à proteção de dados pessoais. Background da legislação de proteção de dados pessoais. Legislação da União Europeia de proteção de dados (GDPR),

Conteúdo Programático 2: Princípios da Lei Geral de Proteção de Dados Pessoais. Fundamentos da LGPD. Âmbito de Aplicação. Encarregado de Dados pessoais. Conceito e atribuições.

Conteúdo Programático 3: Conceitos gerais da Lei Geral de Proteção de Dados Pessoais - LGPD. Bases Legais para o Tratamento de dados pessoais, de dados pessoais sensíveis. Tratamento de dados pessoais de crianças e de adolescentes. Tratamento de dados pessoais pelo poder público. Agentes de tratamento. Controlador. Operador.

Conteúdo Programático 4: Autoridade Nacional de Proteção de Dados. Fiscalização. Sanções administrativas. Boas práticas e governança. Registro de Operações de tratamento de dados. Incidente de Segurança. Segurança da Informação. *Privacy by design*.

Bibliografia Básica:

DONEDA, Danilo ... [et al.]. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

PALHARES, Felipe; PRADO, Luiz Fernando e VIDIGAL, Paulo. Compliance Digital e LGPD. São Paulo: Thomson Reuters Brasil, 2021 (Coleção Compliance; coordenação Irene Patrícia Diom Nohara, Luiz Eduardo de Almeida).

PALHARES, Felipe (coord). Temas Atuais de Proteção de Dados. Thomson Reuters Brasil, 2020.

TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. Lei Geral de Proteção de Dados Pessoais comentada artigo por artigo. 4 ed. São Paulo: Saraiva, 2022.

Bibliografia Complementar:

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

TEIXEIR, Tarcisio... [et al]. DPO – Encarregado de Dados Pessoais [recurso eletrônico] – São Paulo: Expressa, 2022.

Disciplina: Criptografia hash e hacking.

Ementa: Geradores pseudoaleatórios. Cifras de fluxo. Cifras de bloco simétricas e modos de operação. Resumos criptográficos. Teoria dos Números e criptografia assimétrica. Autenticação de mensagens. Assinaturas digitais. Protocolos criptográficos. Funções HASH. Hacking e quebra de sigilo. Aborda aspectos do elemento humano da segurança. Aspectos do Comportamento Humano. Psicologia Comportamental. Aspectos sociais, econômicos, legais e profissionais da segurança da informação. Aspectos estratégicos do controle da tecnologia. Mercado de trabalho do profissional de segurança. Ética profissional. Responsabilidade Social. Sustentabilidade para garantia de preservação do meio ambiente para que futuras gerações possam usufruir de todos os recursos disponíveis hoje. Engenharia Social. Esta disciplina apresenta os mecanismos de segurança utilizados na prevenção de ataques e incidentes que prejudicam a segurança em redes de computadores.

Competências e Habilidades:

- Atuar na análise criptográfica, com aplicação de protocolos criptográficos em conformidade com as normas considerando a autenticação de mensagens;
- Ser capaz de implementar procedimentos e técnicas que subsidiem a utilização de criptografia como HASH para criptografia em sistemas;

- Analisar a atuação hacking os sistemas da informação;
- Ser capaz de atuar na prevenção da engenharia social na segurança e influenciar aspectos do comportamento humano.

Conteúdo Programático 1: Geradores pseudoaleatórios. Cifras de fluxo. Cifras de bloco simétricas e modos de operação. Resumos criptográficos. Teoria dos Números e criptografia assimétrica. Autenticação de mensagens. Assinaturas digitais. Protocolos criptográficos. Funções HASH. Hacking e quebra de sigilo

Conteúdo Programático 2: Engenharia Social. Hackerismo. Conscientizando colaboradores sobre a segurança da informação. Liberdade de expressão, Redes Sociais. Blogs, sites pessoais e fóruns de discussão

Conteúdo Programático 3: Conceitos de pentest. Ferramentas do hacker ético. Tipos de pentest. Elaboração de relatório de pentest

Conteúdo Programático 4: Novas formas de lidar com a informação, com a segurança e privacidade de dados. Lei Geral de Proteção de Dados. BYOD (Bring Your Own Device) e seus desafios para a segurança da informação.

Bibliografia Básica:

KATZ, J.; LINDELL, Y. **Introduction to Modern Cryptography**. Boca Raton: Chapman&Hall/CRC, 2008.

MAO, W. **Modern Cryptography: theory and practice**. Upper Saddle River: Prentice Hall, 2004.

MARCELO, A.; PEREIRA, M. **A Arte de Hackear Pessoas**. São Paulo: Ed.Brasport, 2005.

MITNICK, K.; SIMON, W. **The Art of Deception: Controlling the human element of security**, Wiley Publishing Inc, 2013.

PEIXOTO, MÁRIO CÉSAR P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. São Paulo: Ed. Brasport, 2006.

SANTOS, P. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2010.

STINSON, D. **Cryptography: theory and practice**. Boca Raton: Chapman&Hall/CRC, 2006.

TALBOT, J.; WELSH, D. **Complexity and Cryptography: an introduction**. Cambridge: Cambridge University Press, 2006.

TRAPPE, W.; WASHINGTON, L. **Introduction to Cryptography with coding theory**. Upper Saddle River: Prentice Hall, 2006.

Bibliografia Complementar:

ANDREWS, G. **Number Theory**. New York: Dover Publications, 1994.

BALDONI, M.; CILIBERTO, C.; CATTANEO, G. **Elementary Number Theory, Cryptography and Codes**. Berlin-Heidelberg: Springer-Verlag, 2009.

BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E. **Post-Quantum Cryptography**. Berlin-Heidelberg: Springer-Verlag, 2009.

CATALANO, D. et al. **Contemporary Cryptology**. Basel: Birkhäuser, 2005.

CORMEN, L.; RIVEST, S. **Algoritmos - Teoria e Prática**. Rio de Janeiro: Campus, 2002.

DASGUPTA, S.; PAPADIMITRIOU, C. H.; VAZIRANI, U. V. **Algoritmos**. Porto Alegre: McGraw-Hill/Artmed, 2009.

FERREIRA, Fernando Nicolau Freitas. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2008.

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

GOLDREICH, O. **Fundamentals of Cryptography**, vol. I: Basic Tools. Cambridge: Cambridge University Press, 2001.

GOLDREICH, O. **Fundamentals of Cryptography**, vol. II: Basic Applications. Cambridge: Cambridge University Press, 2004.

HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H. **An Introduction to Mathematical Cryptography**. New York: Springer-Verlag, 2008.

SHOUP, V. A. **Computational Introduction to Number Theory and Algebra**. Cambridge: Cambridge University Press, 2005.

SIPSER, M. **Introdução à Teoria da Computação**. São Paulo: Thomson Learning, 2007.

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

Disciplina: Procedimentos, técnicas e ferramentas forenses

Ementa: Legislação aplicada aos crimes de informática ou cibernético. Introdução e Conceitos. Antecedentes da forense computacional. Diferenças em perícia, sindicância, auditoria e investigação. Documentos processuais: Exordial, quesitos, laudo pericial e parecer técnico. Ata notarial. Papel e atuação do Perito em demandas judiciais. Índícios, evidências e provas digitais. Exame e análise forense. Cadeia de custódia. Identificação e catalogação da prova pericial. Local de Crime. Procedimento Operacional Padrão. Coleta de dados voláteis. Análise post mortem. Ferramentas de coleta e análise. Imagem forense. Investigação de Crimes pela Internet. Sistemas de Arquivos. Recuperação de Dados e fragmentos em dispositivos de armazenamento. Ações Anti-forense.

Competências e Habilidades:

- Compreender os pedidos do juízo, promotor de justiça e partes em uma demanda judicial.
- Compreender e aplicar os corretos métodos para identificação, aquisição, coleta e preservação de evidências.
- Aplicar o método científico para a correta execução dos procedimentos de exames e análises sob as evidências coletadas e a fim de formar a prova.
- Confecção sistemática do Laudo, Manifestação ou Parecer Técnico para que seja apreciado como um elemento de prova em uma solicitação judicial.

Conteúdo Programático 1: Elementos históricos. Forense na ficção e na vida real. Abrangência da forense computacional. Introdução e Conceitos Básicos de Computação e Perícia Forense. Fundamentos da forense computacional. Definições e conceituação de terminologias básicas na prática forense. Função e atuação do Perito Criminal e Judicial.

Conteúdo Programático 2: Metodologia Forense. Fases da Perícia Forense Computacional (Coleta, preservação, exame, análise e apresentação dos resultados). Fonte das evidências e provas. Requisitos de uma Evidência Digital. Coleta de evidências físicas e eletrônicas. Recepção da evidência. Análise e aplicação de procedimentos forenses. Integridade da evidência (Imagens e *Hashing*). Catalogação das evidências. Cadeia de custódia.

Conteúdo Programático 3: Montagem de imagens de perícia. Análise dos dados. Análise de processos. Linha do tempo e cronologia dos fatos. Recuperação e garimpagem de dados. Eliminação segura de dados. Acesso forçado e quebra de senhas.

Conteúdo Programático 4: Ferramentas necessárias a um Perito. Análise de protocolos e *live* forense. Sistemas de arquivos. Chaves de Registro. Estudo de caso aplicado. Prática laboratorial. Coleta, preservação, exame, análise e apresentação resultados em um caso simulado. Erros em procedimentos investigativos. Anti-forense. Engenharia Reversa. Certificações em Forense Computacional. Elaboração de Laudo Pericial.

Bibliografia Básica:

ATHAYDE, Vallim Adriano Penedo de. **Forense computacional e criptografia**. São Paulo: Editora Senac, 2019

FARMER, Dan. **Perícia forense computacional: teoria e prática aplicada**. São Paulo: Pearson Prentice Hall, 2007.

MELO, Sandro. **Computação Forense com Software Livre**. Rio de Janeiro: Editora Alta Books, 2009.

Bibliografia Complementar:

NORAT, Markus, et. Al. Direito Digital. Responsabilidade Civil e Criminal na Internet. Clube dos Autores. 2018

Código de Processo Civil. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm. Consultado em 09 de novembro de 2020.

Vecchia, Evandro Dalla. Perícia digital: da investigação à análise forense. 2.ed- Campinas, SP. Millennium Editora, 2019.

Disciplina: Auditoria de sistemas.

Ementa: Auditoria de Sistemas. Conceitos, características e riscos de auditoria. Modelo de segurança em ambiente de processamento de dados. Segurança Lógica e Física. O processo de auditoria de sistemas. Planejamentos dos

trabalhos em ambiente computacional. Execução da auditoria aplicável no gerenciamento e controle dos aplicativos: Programas, procedimentos e técnicas aplicáveis. Conceito e objetivos da auditoria de sistemas de informação. Técnicas de auditoria em sistemas de informação. Softwares de auditoria. Estrutura da função de auditoria de sistemas de informação nas organizações.

Competências e Habilidades:

- Atuar na auditoria de sistemas, com aplicação de políticas em conformidade com as normas considerando a segurança lógica e física;
- Ser capaz de implementar procedimentos e técnicas que subsidiem a auditoria em sistemas da informação, analisar os sistemas da informação;
- Aplicar as melhores práticas para gerenciar a auditoria em redes computacionais;
- Identificar e planejar auditoria em equipamentos e sistemas;
- Utilizar, propor e gerir ferramentas e tecnologias de auditoria visando auditar a segurança e reduzir os riscos nas organizações.

Conteúdo Programático 1: Introdução e Conceitos Básicos de Auditoria da Tecnologia da Informação. Definições. Conceituação Básica. Palavras-chave. Função do Auditor de T.I.

Conteúdo Programático 2: Auditoria do Desenvolvimento e Manutenção de Sistemas. Controles do Desenvolvimento de Sistemas. Controles da Manutenção de Sistemas

Conteúdo Programático 3: Auditoria da Administração e Operação de Redes. Administração da Rede. Segurança Lógica e Física da Rede. Plano de Contingência. Operação da Rede.

Conteúdo Programático 4: Auditoria dos Controles de Banco de Dados. Controles da Administração de Dados. Controles da Administração de Banco de Dados. Acesso ao B.D. Disponibilidade do B.D. Integridade do B.D.

Bibliografia Básica:

CARUSO, Carlos A. A.; STEFFEN, Flávio D. **Segurança em Informática e de Informações**. 2. ed. rev. e ampl. São Paulo: Senac, 1999.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books do Brasil, 2000.

Manual de auditoria de sistemas -

<http://www.tcu.gov.br/SAUDI/Download/AuditSistemas.doc>

Bibliografia Complementar:

INSTITUTO BRASILEIRO DE CONTADORES. **Auditoria em Ambientes de Internet**. São Paulo: Atlas, 2001.

GIL, Antonio Loureiro. **Auditoria de Computadores**. São Paulo: Atlas, 1999.

TERADA, Routh. **Segurança de Dados**. São Paulo: Ed. Edgar Blücher, 2000.

INSTITUTO BRASILEIRO DE CONTADORES. **Auditoria por meios eletrônicos**. São Paulo: Atlas, 1999.

ARIMA. Carlos Hideo; SCHMIDT. Paulo e SANTOS, José Luiz dos. **Fundamentos de Auditoria de Sistemas**. São Paulo: Atlas, 2006.

Disciplina: Práticas periciais em registros audiovisuais.

Ementa: Conceitos e definições. Formação de imagens e áudios. Ondas e espectro de luz visível. *Magic Numbers* de arquivos. Metadados, atributos intrínsecos e extrínsecos. Estrutura dos dispositivos gravadores de imagem e som. Detecção de edições e montagens. Ampliação, interpolação e hiper resolução. Restauração de imagens. Ajuste de foco e movimentos. Distorções. Ruídos.

Competências e Habilidades:

- Diferencia entre áudio, imagem e vídeo e os seus respectivos diferentes padrões e formatos.
- Aplicar os métodos e ferramentais na busca por edições, montagens, supressões de dados em arquivo contendo áudio, imagem e vídeos.
- Correlacionar os métodos de aplicação de imagem, sem distorções, e para identificação, aquisição, coleta e preservação de evidências.

- Aplicar o método científico para a correta execução dos procedimentos de exames e análises sob as evidências coletadas e a fim de formara prova.
- Transcrição Fonográfica e Fonética.

Conteúdo Programático 1: Diferença digital entre áudio, imagem e vídeo. Os diferentes padrões e formatos. Exame e imagens e áudio. Criptografia e Esteganografia. Análise de Fourier.

Conteúdo Programático 2: Ajuste de qualidade de Imagens. Técnicas de interpolação. Super posição e resolução. Ruído periódico. Distorção e ajuste de foco e lente.

Conteúdo Programático 3: Ajuste de qualidade de áudio. Ruídos e classificações. Meios e métodos de reprodução.

Conteúdo Programático 4: Fonética forense. Transcrição de diálogos. Identificação de falantes. Análise acústica e audiométrica.

Bibliografia Básica:

FERNANDES, Clemente Maia da Silva. **Análise das reconstruções faciais forenses digitais caracterizadas utilizando padrões de medidas lineares de tecidos moles da face de brasileiros e estrangeiros.** Tese de Doutorado. 2010.

MACHADO, Aline. **Uso de técnicas acústicas para verificação de locutor em simulação experimental.** 2011.

GILLIER, Raissa. **O disfarce da voz em fonética forense.** Tese de mestrado, Linguística, Universidade de Lisboa, Faculdade de Letras, 2011. Disponível em <<http://hdl.handle.net/10451/4131>>.

Bibliografia Complementar:

FERNANDES, J.R. **Perícias em Áudios e Imagens Forenses.** Ed. Millenium. 2014.

POLIDO A.M, Martins MASUR, Hanayama EM. **Percepção do envelhecimento vocal na terceira idade.** Rev. CEFAC; 2005; 7(2):241-51.

BARROS APB, Carrara-De Angelis E. **Análise acústica da voz**. Em: Dedivits RA, Barros APB. Métodos de avaliação e diagnóstico de laringe e voz. São Paulo: Louvise; 2002. p. 201-21.

Vecchia, Evandro Dalla. Perícia digital: da investigação à análise forense. 2.ed- Campinas, SP. Millennium Editora, 2019.

Disciplina: Investigação remota de sistemas e técnicas de evasão

Ementa: Conceitos e definições. Sistemas Embarcados. Sistemas proprietários. Sistemas distribuídos. Tipos e modelos. Limitações físicas. Restrições computacionais e temporais. Computação e nuvem. Modelos de serviços. FaaS - Forensic as a Service ou computação forense como serviço e forense distribuída. Internet das Coisas. Aspectos técnicos da investigação em celulares e dispositivos móveis.

Competências e Habilidades:

- Compreender os desafios da forenses para estes dispositivos.
- Elaborar a correta aquisição e coleta de dispositivos não convencionais.
- Identificar o ambiente possível cenário de um crime e seus pontos de acesso por dispositivos não convencionais.
- Capturar o conteúdo da memória RAM destes dispositivos.

Conteúdo Programático 1: Princípios da computação embarcada. Categorização dos sistemas. Métodos e coleta e preservação de indícios. Complexidade de sistemas embarcados e suas interfaces de coleta. Especificidade.

Conteúdo Programático 2: *OpenStack* – plataforma de computação em nuvem Open Source para criação de nuvens públicas ou privadas. *Forensics OpenStack Tools (Frost)*. Aplicação de *MapReduce*.

Conteúdo Programático 3: Dispositivos IoT. Vazamentos de dados. Invasão ou infiltração a sistemas. Acesso remotos. Manipulação de processos

Conteúdo Programático 4: Posse, detenção ou apreensão do dispositivo celular. Cadeia de custódia. Clonagem de celular. Extração de memória. *Rooting. Brute force. Data Carving.* Sanitização e recuperação. Estação de conversas de WhatsApp e Telegram.

Bibliografia Básica:

DIDONÉ, Dener. RUY, José Guerra Barreto de Queiroz. **Computação em nuvem: desafios e oportunidades para a forense computacional.** Universidade Federal de Pernambuco. 2011. Disponível em <https://repositorio.ufpe.br/handle/123456789/2745>.

JESUS, Antonio Velho et al (Org.). **Tratado de Computação Forense.** Campinas. São Paulo: Milennium, 2016. 606 p.

MANRAL, B. SOMANI, G. A. **A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions.** *ACM Comput. Surv.* 52, 6, Article 124. November 2019. Disponível em <https://dl.acm.org/doi/fullHtml/10.1145/3361216>.

Bibliografia Complementar:

PERES. J.R, SLEIMAN, C.M. **IoT – Investigação Forense Digital: Fundamentos e Guia de Referências.** São Paulo: Ed. do Autor, 2017. Recurso Digital - Formato PDF 3,9 Mb.

GALVAO, Ricardo Kléber M. **Introdução à análise forense em redes de computadores.** São Paulo: Editora Novatec, 2013.

NORTHCUTT, Stephen. **Como detectar invasão em redes:** Um guia para analistas. Rio de Janeiro: Ciência Moderna, 2000.

13. Infraestrutura Física e Pedagógica

O aluno encontrará todo o conteúdo do curso e assistirá às aulas gravadas no ambiente virtual. Para assistir às aulas é fundamental que as especificações abaixo sejam obedecidas, possibilitando, assim, uma recepção de maior qualidade dos vídeos.

Hardware:

- Processador Intel Core 2 Duo ou superior.
- 2Gb de Memória RAM.
- Placa de vídeo com resolução 1024x768, qualidade de cor 32 bits e compatível com Microsoft DirectShow.
- Microsoft DirectX 9.0c ou posterior.

Software:

- Navegador: Firefox, Google Chrome, Internet Explorer (sempre atualizado).
- Sistema Operacional: Windows XP ou posterior.
- Adobe Flash Player (atualizado).
- *Plugin* de vídeos SilverLigth (atualizado)

Rede:

- Conexão com a Internet banda larga de no mínimo 2 MB.
- Em caso de acesso em ambientes corporativos além da velocidade, é necessário verificar as condições de segurança de rede de sua empresa e se certificar que o site não estará bloqueado.

Adicionalmente, é prevista a utilização da biblioteca virtual para consultas bibliográficas e pesquisa de assuntos referentes às disciplinas ministradas.

