



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
MBA em Cybersecurity e cybercrimes

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: MBA em Cybersecurity e cybercrimes

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 TIC, com curso superior de

graduação reconhecido pelo MEC que desejem atuar como especialistas e consultores, com características multidisciplinares, em crimes cibernéticos (Cybercrime) e segurança na informática (Cybersecurity).

4. Critérios de Seleção

O ingresso na pós-graduação será realizado por meio de inscrição no Portal Pós, entrega da documentação pessoal e do diploma da graduação autenticado. Em seguida, analisados pela Instituição.

5. Justificativa do Curso

O Curso é inspirado na fala do legendário cracker e hoje celebrado autor Kevin Mitnick - "O fator humano é o elo mais fraco da segurança"- publicada no livro A Arte de Enganar, e destina-se aos interessados nos temas Segurança Cibernética, Vazamento de Informações Confidenciais, Espionagem e Contraespionagem, diferenciando-se pela abordagem comportamental em detrimento da tecnológica, revelando como as vulnerabilidades humanas são exploradas e como concorrentes injustos e imorais, cibercriminosos e terroristas as usam perigosamente para prejudicar nossos interesses.

De acordo com o relatório Internet Security Threat (ISTR), o Brasil é o sétimo país do mundo mais afetado por ataques cibernéticos. Esses dados revelam o motivo pelo qual o mercado de trabalho se expandiu de forma abrangente e deverá apresentar tendência de alta nos próximos anos. Empresas de todos os tamanhos têm empregos em grandes centros de cidades e centros de produção em todo o país.

Como a evolução digital continua mudando em escala global, é vital proteger os dados e as informações de ataques, vazamentos e fraudes. Com o objetivo de formar talentos na indústria de segurança cibernética, o curso tem como foco alta qualificação e empregabilidade.

6. Objetivos do Curso

6.1. Objetivo Geral

- Compreender conceitos, normas e modelos de gestão, assim como fazer uso de ferramentas e recursos de Segurança da Informação em ambientes computacionais; implantar modelos de Gestão de Segurança da Informação, baseados em normas e modelos de melhores práticas; e aplicar mecanismos e controles que permitam minimizar os impactos relacionados a falhas na Segurança da Informação.

6.2. Objetivos Específicos

- Apresentar modernas técnicas de interação humana utilizadas pela inteligência e pela Espionagem para a obtenção de informações protegidas, em plena 4ª Revolução Industrial;
- Discorrer sobre as técnicas de Contrainteligência e Contraespionagem na proteção de nossos ativos materiais e imateriais, e sobre como anular as ações da Inteligência e da Espionagem hostis;
- Sensibilizar as pessoas para a necessidade de aprender e aplicar medidas de proteção para suas informações pessoais e profissionais, especialmente as de conteúdo sensível;
- Educar os profissionais dos setores público e privado, que lidam com informações importantes, na aplicação das melhores práticas de proteção;
- Desenvolver anticorpos para fazer frente às ameaças vindouras nos instáveis ambientes cinético e cibernético.

7. Competências e Habilidades do Egresso

Competências

Por meio de uma formação de caráter reflexivo, crítico e criativo, além dos tipos de crimes cibernéticos e criminologia do crime digital, você também aprenderá sobre inteligência policial e contra-espionagem, investigação criminal, análise de dados de segurança e análise de ameaças, riscos e vulnerabilidades em todos os aspectos, além das principais questões em segurança da informação. Estas questões são baseadas em aspectos teóricos, estudos de caso e ferramentas necessárias para alcançar um desempenho preciso, seguro e de alta qualidade. Atuará desempenhando um papel na detecção, investigação, avaliação, prevenção e defesa do crime cibernético, e também terá um papel na segurança organizacional, contra-espionagem ativa e inteligência. Você também pode atuar como consultor, pesquisador e professor nesta área.

Habilidades

- Realizar levantamento prévio das necessidades de segurança de uma organização;
- construir a segurança da informação, adotando padrões, políticas e práticas;
- compor equipes de projetos na área de segurança da informação;
- implementar melhorias contínuas do processo de segurança da informação;
- planejar a segurança da informação, medindo riscos e entendendo impactos.

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 jubileamento 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
Revolução industrial 4.0	0 h	40 h	40 h
Segurança em redes de computadores	0 h	40 h	40 h
Criptografia hash e hacking	0 h	40 h	40 h
Cibercrimes, responsabilidade penal e civil	0 h	40 h	40 h
Lei Geral de Proteção de Dados	0 h	40 h	40 h
Certificação digital e blockchain	0 h	40 h	40 h
Introdução à computação forense	0 h	40 h	40 h
Cybersecurity	0 h	40 h	40 h
Políticas de segurança e classificação da informação	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: Revolução industrial 4.0

Ementa: A sociedade da informação. Redes de computadores. Criptografia. A internet. E-commerce. Redes sociais. Inteligência artificial. Bancos de dados. Big Data. Deep web. Comportamento das gerações X, Y e Z. Inovações disruptivas e seus desafios para o Direito. Produção coletiva de conhecimento e de software. Compartilhamento de arquivos peer-to-peer. Uso de aplicativos (Veículos autônomos. Prestação de serviços médicos pela internet. Espaços de co-working. Serviços em nuvem. Internet das coisas. Impressão 3D. Drones. Jogos eletrônicos e realidades sintéticas.

Competências e Habilidades:

- Apresentar ao aluno os principais temas sobre serviços e produtos digitais com impactos na área jurídica
- Despertar o senso crítico ao expor as inovações disruptivas e o conflito de velocidade entre as inovações e o Direito.
- Empregar conceitos apreendidos em sala de aula na construção de novas ideias.
- Identificar fenômenos jurídicos nas relações tecnológicas

Conteúdo Programático 1: A sociedade da informação. Redes de computadores. Criptografia. A internet. Deep web. E-commerce. Inteligência artificial.

Conteúdo Programático 2: Bancos de dados. Big Data. Comportamento das gerações X, Y e Z. Inovações disruptivas e seus desafios para o Direito.

Conteúdo Programático 3: Produção coletiva de conhecimento e de software. Compartilhamento de arquivos peer-to-peer.. Aplicativos de mensagens. Redes Sociais.

Conteúdo Programático 4: Veículos autônomos. Aplicativos transporte, viagem e hospedagem, navegação, de relacionamento e outros aplicativos de aluguel. Prestação de serviços médicos pela internet. Espaços de co-working. Serviços em nuvem. Internet das coisas. Impressão 3D. Drones. Jogos eletrônicos e realidades sintéticas.

Bibliografia Básica:

SHWAB, Klaus. **A quarta Revolução industrial**. São Paulo. Edipro: 2016.

SHWAB, Klaus. **Aplicando a Quarta Revolução Industrial**. São Paulo. Edipro: 2016.

PARENTONI, Leonardo; MIRANDA, Bruno. **Direito, Tecnologia e Inovação**. DPlácido. 2018.

Bibliografia Complementar:

CHISTENSEN CLAYTON M. **O Dilema da Inovação**. Quando as novas tecnologias levam as empresas ao fracasso. M Books. São Paulo. 2019

HOWE, Jeff; ITO, Joi. **Disrupção e Inovação**. Alta Books. São Paulo. 2017.

MAGALDI, Sandro; SALIBI NETO, José. **Gestão do Amanhã**: Tudo o que você precisa saber sobre gestão, inovação e liderança para vencer na 4ª Revolução Industrial. Gente. São Paulo. 2018.

Disciplina: Segurança em redes de computadores.

Ementa: Introdução à arquitetura de redes. Protocolos de comunicação. Ameaças, Falhas e Vulnerabilidades. Ferramentas de Segurança. Segurança em redes sem fio. 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: Princípios da segurança da Informação.

Conteúdo Programático 3: Ameaças, falhas e vulnerabilidades.

Conteúdo Programático 4: Ferramentas de segurança.

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.

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.

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. Cultura. Hackerismo. Ética Profissional. Comportamento no ambiente Corporativo. Negociação. Evangelizando com as diretrizes de segurança da informação. Campanhas de Conscientização de usuários. Liberdade de expressão Redes Sociais. Blogs, sites pessoais e fóruns de discussão.

Conteúdo Programático 3: Conceito de Psicologia e suas aplicações. As principais correntes psicológicas (Behaviorismo, Gestalt e Psicanálise) e suas metodologias. Personalidade, Psicologia dos grupos, relacionamento intra e interpessoal. O processo de autoconhecimento e autoanálise, técnicas de controle e autocontrole.

Conteúdo Programático 4: Novas formas de lidar com a informação, com a segurança, invasão da privacidade e com direitos autorais. Potencial da internet para reunir grupos em torno de uma causa. Transparência na gestão da segurança. Lixo eletrônico. Responsabilidade Social. Sustentabilidade.

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: 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 virtual

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. **Ciber Crimes**: 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: 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: Certificação digital e blockchain.

Ementa: Algoritmos criptográficos, algoritmos de assinatura digital, algoritmos de resumo, certificação digital e ferramentas que servem de suporte para a criptografia Conceitos básicos de criptografia aplicados à criptomoedas. Funções Hash. Conceitos de PKI. Ciclo de vida dos certificados. Ciclo de uso dos certificados. Ferramentas de criptografia: HSM, *token*, *smartcard*. Curvas elípticas e seu uso na Bitcoin. Introdução ao Bitcoin e sua história. O white paper do Bitcoin. Proof of work e formação de consenso. Blockchain como registro irreversível. A plataforma Ethereum. Smart-contracts. A linguagem Solidity. Desenvolvimento e deploy de smart-contracts

Competências e Habilidades:

- Atuar na análise das curvas elípticas e bitcoin, com aplicação de protocolos criptograficos para certificação digital em conformidade com as normas considerando a autenticação;
- Ser capaz de implementar procedimentos e técnicas que subsidiem a utilização de linguagem *solidity* para desenvolvimento e *smart contracts*.

Conteúdo Programático 1: Criptografia de Chave Simétrica. Gerenciamento de Chaves Simétricas. Criptografia Baseada em Senha. Criptografia de Chave Pública: algoritmos: El Gamal, RSA

Conteúdo Programático 2: Assinatura Digital: resumos de mensagens com algoritmos Hash: MD5 e SHA-1, MAC com SHA-1, assinaturas verificáveis com DSA.

Conteúdo Programático 3: Infra-estrutura de chaves públicas: porque certificados digitais. Exemplos de ataques à chaves públicas. Padrão de certificados X.509, estrutura de PKI, protocolos de comunicação em PKI. Revogação de certificados. Outros conceitos. ICP-Brasil: Infra-estrutura de chaves públicas no Brasil.

Conteúdo Programático 4: Curvas elípticas e seu uso na Bitcoin. Introdução ao Bitcoin e sua história. O white paper do Bitcoin. Proof of work e formação de consenso. Blockchain como registro irreversível. A plataforma Ethereum. Smart-contracts. A linguagem Solidity. Desenvolvimento e deploy de smart-contracts.

Bibliografia Básica:

Burnett, S, Paine, S. **Criptografia e Segurança:** o Guia Oficial RSA. Editora Campus, RSA Press, 2002.

Bibliografia Complementar:

TANEBAUM, Andrew S. **Redes de Computadores.** 8 ed. São Paulo: Editora Campus, 2003.

FORRISTAL, Jeff; TRAXIER, Julie. **Site Seguro:** Aplicações Web. Syngress (Alta Books), 2002.

FRIEDLMAIER, Maximilian; TUMASJAN, Andranik; WELPE, Isabell. **Disrupting industries with blockchain:** The industry, venture capital funding, and regional distribution of blockchain ventures. 2016.

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.

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: Cybersecurity.

Ementa: Arquitetura de Sistemas Seguros. Tecnologias de Desenvolvimento Seguro.

Competências e Habilidades:

- Desenvolver o conhecimento de arquitetura e infraestrutura de sistemas necessário para analisar e especificar controles de segurança para sistemas seguros;
- Desenvolver o conhecimento de estratégia e inteligência através de jogos e desenvolvimento de mecanismos de criptografia, aplicação da tecnologia e uso de certificados digitais e acesso a *deep web*.

Conteúdo Programático 1: Arquitetura de sistemas. Diferentes tecnologias de desenvolvimento e suas principais características.

Conteúdo Programático 2: Componentes de um sistema distribuído. Aspectos de segurança dos sistemas distribuídos. Análise de segurança.

Conteúdo Programático 3: Processo de desenvolvimento seguro. Top 10 OWASP. Testes de segurança em aplicações Web. Cloud computing: conceitos e aspectos de segurança.

Conteúdo Programático 4: Big Data Analytics. Armazenamento Seguro. Conceitos de inteligência. Conceitos de jogos.

Bibliografia Básica:

KIZZA, Joseph Migga. **Computer network security and cyber ethics**. 2nd ed. Jefferson: McFarland & Company, 2006.

RAY, John. **Maximum Linux security**: a hackers guide to protecting your Linux server and workstation]. 2nd ed. Indianapolis: SAMS, 2001.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet:** Uma nova abordagem. São Paulo: Editora Pearson, 2017.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. São Paulo: Pearson Education do Brasil, 2010.

BENANTAR, Messaoud. **Introduction to the public key infrastructure for the Internet.** Upper Saddle River, N.J.: Prentice-Hall: PTR, 2002.

SINGH, Simon; CALIFE, Jorge Luiz. **O livro dos códigos.** São Paulo: Record, 2007.

Bibliografia Complementar:

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. São Paulo: Pearson Education do Brasil, 2010.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers expostos/ segredos e soluções para a segurança das redes.** São Paulo: Makron Books, 2000.

TANENBAUM, Andrew S.; WETHERALL, D. **Computer networks.** 5th ed. Boston, MA; Columbus, OH: Prentice Hall, 2011.

CORDEIRO, Luiz Gustavo. **Certificação digital:** conceitos e aplicações: modelos brasileiro e australiano. Rio de Janeiro: Ciência Moderna, 2008.

BUCHMANN, Johannes A. **Introduction to cryptography.** New York: Springer-Verlag, 2001

Disciplina: Políticas de segurança e classificação da informação.

Ementa: Introdução à política de segurança da informação. ITIL e COBIT na política de segurança da informação. Governança de segurança da informação. Classificação da informação. Políticas, normas e procedimentos práticos.

Competências e Habilidades:

- Compreender a necessidade de estabelecer políticas e normas para a segurança da informação.
- Desenvolver, implantar e manter regulamentos para a segurança da informação nas organizações.
- Atuar nas estratégias e ações para a proteção da informação em cenários corporativos.

Conteúdo Programático 1: Introdução à política de segurança da informação.

Conteúdo Programático 2: ITIL, COBIT e governança na política de segurança da informação.

Conteúdo Programático 3: Classificação da informação.

Conteúdo Programático 4: Políticas, normas e procedimentos práticos.

Bibliografia Básica:

HANS BAARS. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Editora Brasport, 2018.

LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação.** São Paulo: Editora Senac, 2018.

PONTES, Edison. **Políticas e normas para a segurança da informação:** como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

Bibliografia Complementar:

AGUILERA, Fernandes Edson. **Padrões, normas e política de segurança da informação.** São Paulo: Editora Senac, 2019.

FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

HINTZBERGEN, Jule...[et al.]. **Fundamentos de segurança da informação:** com base na ISSO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2018.

VALLE, Rogerio. **Análise e modelagem de processos de negócio foco na notação bpmn** (business process modeling notation). São Paulo: Atlas, 2013.

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.

