



PROJETO PEDAGÓGICO DE CURSO

Pós-Graduação *Lato Sensu*

Tecnologia e Segurança de Blockchain e *Smart Contracts*

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: Tecnologia e Segurança de Blockchain e Smart Contracts

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

Profissionais de Tecnologia da Informação e Comunicação (Analistas de Sistemas, Bacharéis em Sistemas de Informação, Ciência da Computação, Engenharia da Computação e Tecnólogos na área de Tecnologia),

Engenheiros Elétricos, Engenheiros de Redes, Tecnólogos em Telecomunicações, Administradores, gestores de negócios e demais profissionais de nível superior engajados ou que queiram se engajar na gestão de sistemas em blockchain e Smart Contracts.

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

A pressão para desenvolver uma nova economia está aumentando. As novas tecnologias melhoraram a capacidade dos usuários de aprimorar suas próprias capacidades, reduziram o atrito e estabeleceram conexões diretas com os usuários, aumentando assim a confiabilidade dos modelos de negócios e a confiança nas relações digitais.

O Blockchain é uma das plataformas de tecnologia mais promissoras para o desenvolvimento de aplicações e novos negócios, e será o pioneiro dessa nova economia. As tecnologias que viabilizam as criptomoedas, principalmente o Bitcoin, dão às pessoas maior confiança no relacionamento entre empresas e consumidores.

E isso é só o começo. Depois que a era da Internet se tornou uma plataforma para as empresas criarem formatos de negócios inovadores, estamos vivenciando uma nova revolução. Blockchain e contratos inteligentes permitem uma geração de plataformas, aplicativos e modelos de negócios a serem realizados, e essas plataformas, aplicativos e modelos de negócios mudarão as transações conduzidas por meio da rede.

6. Objetivos do Curso

6.1. Objetivo Geral

- Esse curso apresenta a tecnologia blockchain, os sistemas de registros distribuídos (DLT) e os contratos inteligentes, permitindo ainda a compreensão das criptomoedas e da tokenização, o que abre a mente dos participantes para um universo de possibilidades.

6.2. Objetivos Específicos

- Dominar e aplicar as tecnologias que estão transformando o universo da economia digital.
- Conhecer os protocolos do Bitcoin e do Ethereum.
- Entender sobre segurança cibernética, Web 3.0 e arquitetura de aplicações descentralizadas.
- Gerenciar dados e desenvolver aplicações em cenários descentralizados.
- Aplicar as tecnologias do Blockchain em cenários reais.

7. Competências e Habilidades do Egresso

Competências

Para atingir este objetivo, visa-se resolver aspectos relacionados a concepção de blockchain, evolução das tecnologias em geral e desenvolvimento de contratos inteligentes. Tem como objetivo fornecer aos alunos os fundamentos teóricos e práticos necessários para que possam compreender a aplicação do Blockchain e dos contratos inteligentes nos campos público e privado. Dessa forma, resolve os aspectos técnicos do ambiente de rede compartilhada, a prática e o uso de blockchain e ferramentas colaborativas, além de tratar de questões relacionadas às possibilidades e desafios das transações digitais no mundo atual.

Habilidades

- Compreender a concepção de Blockchain para diferentes plataformas.
- Compreender os mecanismos, frameworks e metodologias usadas no desenvolvimento de sistemas em Blockchain.
- Ser capaz de compreender as aplicações de contratos inteligentes (smart contracts) integrados a sistemas de informação e gerenciá-los.
- Capacitar o profissional em avaliar como o Blockchain melhorará um determinado processo ou como garantirá as transações financeiras.

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
Tecnologias descentralizadas	0 h	40 h	40 h
Função de criptografia hash	0 h	40 h	40 h
Criptografia hash e hacking	0 h	40 h	40 h
Certificação digital e blockchain	0 h	40 h	40 h
ECM, GED e contratos inteligentes	0 h	40 h	40 h
Lei Geral de Proteção de Dados	0 h	40 h	40 h
Cloud computing	0 h	40 h	40 h
Segurança em cloud computing	0 h	40 h	40 h
Monetização digital: criptomoedas e Nfts	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: Ensino a distância: características desta modalidade de estudo. A tecnologia e o ensino à distância. Legislação do Ensino a Distância no Brasil. Aspectos relacionados ao perfil no Ensino a Distância.

Competências e Habilidades:

- Compreender a modalidade de ensino a distância.
- Identificar uma relação entre tecnologia e educação no contexto do EAD;
- Discutir elementos da legislação do ensino a distância no Brasil;
- Refletir sobre o perfil do aluno em ensino a distância.

Conteúdo Programático 1: Introdução ao Ensino a Distância.

Conteúdo Programático 2: Tecnologia e educação.

Conteúdo Programático 3: Legislação do Ensino a Distância no Brasil.

Conteúdo Programático 4: Perfil do aluno no Ensino a Distância.

Bibliografia básica:

BRASIL. Ministério da Educação. **Lei de Diretrizes e Bases da Educação Nacional - Lei n. 9.394/96**. Brasília, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 6 dez. 2022.

BRASIL. Ministério da Educação. **Resolução CNE/CP n. 7, de 18 de dezembro de 2018**. Brasília, 2018. Disponível em: https://normativasconselhos.mec.gov.br/normativa/view/CNE_RES_CNECESN72018.pdf. Acesso em: 6 dez. 2022.

GIL, H. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0: potenciais consequências para uma 'humanização' em contexto educativo. 2014. **Boletim informativo Cybercentro Castelo Branco**. Castelo Branco, 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 6 dez. 2022.

MEYER, A. I. da S. (2022). Conceituando a Educação a Distância. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 1, p. 590-

601, [s. l.], 2022. Disponível em: <https://periodicorease.pro.br/rease/article/view/3835>. Acesso em: 6 dez. 2022.

VAZ, M. L. de L.; RIBEIRO, F.; COSTA, L. A. da. Os desafios da educação a distância on-line e a remotividade na nova engenharia educacional. **Brazilian Journal of Science**, v. 1, n. 4, p. 79-86. Goiás, 2022. Disponível em: <https://www.brazilianjournalofscience.com.br/revista/article/view/79>. Acesso em: 6 dez. 2022.

VIEIRA, D. M. L.; COSTA, L. A.; VAZ, M. L. L. Um novo olhar para a educação a distância. In: MACHADO, G. E.; COSTA, S. C.; SILVA, K. R. P. **Debates contemporâneos: perspectivas e reflexões atuais**. Santa Maria: Arco, 2021.

Bibliografia Complementar:

BAPTISTA, M. M. Internet: auxílio à educação. **BIBLOS - Revista do Instituto de Ciências Humanas e da Informação**, v. 16, p. 37- 44, [s. l.], 2004. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/23717>. Acesso em: 6 dez. 2022.

MOORE, M.; KEARSLEY, G. **Educação a distância: uma visão integrada**. São Paulo: Thomson Learning, 2007.

MORAN, J. M.; MASETTO, M. T.; BEHRENS, M. A. **Novas tecnologias e mediação pedagógica**. 21. ed. Campinas: Papirus, 2013.

PIVA, D. J.; PUPO, R.; GAMEZ, L. et al. **EAD na prática: planejamento, métodos e ambientes de educação on-line**. São Paulo: Elsevier, 2011.

Disciplina: Tecnologias Descentralizadas.

Ementa: Tecnologia Descentralizada. Bitcoin. Blockchain. Smart Contracts. Smart Cities. Aplicações de DLT ao registro de imóveis. Aplicações de DLT ao registro de pessoas. Aplicações de DLT a notas e títulos.

Competências e Habilidades:

- Aproximar o aluno da concepção da revolução tecnológicas nos próximos anos
- Compreender a tecnologia que sustenta as criptomoedas mais conhecidas.
- Fomentar a criação de novas possibilidade de produtos – jurídicos ou não.
- Capacitar o aluno a refletir sobre possíveis soluções tecnológicas utilizando tecnologia descentralizada.

Conteúdo Programático 1: Tecnologia Descentralizada

Conteúdo Programático 2: Blockchain. Bitcoin. Smart Contracts. Utilização de Blockchain nas juntas comerciais.

Conteúdo Programático 3: Smart Cities. Aplicações de DLT (Distributed Ledger Technology) ao registro de imóveis.

Conteúdo Programático 4: Uso de DLT (Distributed Ledger Technology) ao registro de pessoas e documentos estundantis. A DLT (Distributed Ledger Technology) e sua utilização em notas e títulos.

Bibliografia Básica:

MOUGAYAR, William. Blockchain para negócios: Promessa, prática e aplicação da nova tecnologia da Internet. Atlas Books. São Paulo. 2017

TAPSCOTT, Don, TAPSCOTT, Alex. Blockchain Revolution. Senai -SP. 2017.

CAMPOS, Emília Malgueiro. Criptomoedas e Blockchain. Lumen Juris. São Paulo. 2018.

LYRA, João Gomes. Blockchain e organizações descentralizadas. Brasport. 2019.

Bibliografia Complementar:

BLOCKCHAIN COMO SISTEMA DE CUSTÓDIA DE VALORES MOBILIÁRIOS NO ÂMBITO DO MERCADO DE CAPITAIS BRASILEIRO. Revista de Direito Bancário e do Mercado de Capitais | vol. 80/2018 | p. 93 - 106 | Abr - Jun / 2018 | DTR\2018\14473

PERSPECTIVAS PARA A TECNOLOGIA BLOCKCHAIN

Revista de Direito Bancário e do Mercado de Capitais | vol. 81/2018 | p. 141 - 158 | Jul - Set / 2018 | DTR\2018\19494

CONTRATOS INTELIGENTES, OAD E NOVA ECONOMIA INSTITUCIONAL: PERSPECTIVAS PARA A INTERPRETAÇÃO E APLICAÇÃO DE AJUSTES CELEBRADOS EM COMPUTAÇÃO DESCENTRALIZADA A PARTIR DE ESTUDO DE CASO SOBRE A VULNERABILIDADE DA CODIFICAÇÃO NO AMBIENTE DO ETHEREUM. Revista de Direito Civil Contemporâneo | vol. 18/2019 | p. 61 - 90 | Jan - Mar / 2019 | DTR\2019\27929.

Disciplina: Função de criptografia Hash.

Ementa: Técnicas clássicas de Criptografia. Conceitos básicos de teoria dos números e corpos finitos. Criptografia de chave pública. Funções de *hash* criptográficas. Autenticação. Assinaturas digitais.

Competências e Habilidades:

- Compreender o funcionamento das principais técnicas de criptografia.
- Diferenciar as técnicas de criptografia a partir de suas características.
- Adotar modelos de criptografia adequados à aplicação.
- Compreender a operação de algoritmos de autenticação de mensagens e de usuários.

Conteúdo Programático 1: Técnicas clássicas de Criptografia, teoria dos números e corpos finitos.

Conteúdo Programático 2: Criptografia de chave pública.

Conteúdo Programático 3: Funções de *hash* criptográficas.

Conteúdo Programático 4: Autenticação e Assinaturas digitais.

Bibliografia Básica:

GOODRICH, Michael T. **Introdução à segurança de computadores**. Porto Alegre Bookman 2012

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2015.

AUMASSON, Jean-Philippe. **Serious Cryptography**: A practical introduction to modern encryption. San Francisco: No Starch Press, 2017.

Bibliografia Complementar:

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

DIÓGENES, Yuri; MAUSER, Daniel. **Certificação Security+**: Da prática para o exame SYO-401. Rio de Janeiro: Editora Novaterra, 2016.

FRANCO, Pedro. **Understanding Bitcoin**: Cryptography, Engineering and Economics. Nova Jersey: John Wiley & Sons, 2014.

MARTINI, Renato da Silveira. **Tecnologia e cidadania digital**: tecnologia, sociedade e segurança: certificação digital, segurança da informação, governo eletrônico. Rio de Janeiro: Brasport, 2008.

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: 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 criptográficos 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 (inserir 3 bibliografias atuais):

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: ECM, GED e contratos inteligentes.

Ementa: Introdução à gestão da informação. Diferença entre *Enterprise Content Management* (ECM) e Gestão Eletrônica de Documentos (GED). ECM. GED. Ferramentas de GED. Contratos inteligentes.

Competências e Habilidades:

- Compreender as necessidades da gestão de informação corporativa.
- Conhecer as vantagens na utilização de Gestão eletrônica de documentos e contratos inteligentes.
- Tomar decisões quanto à ferramentas e processos na área de gestão da informação.

Conteúdo Programático 1: Introdução à gestão da informação.

Conteúdo Programático 2: *Enterprise Content Management* (ECM).

Conteúdo Programático 3: Gestão Eletrônica de Documentos (GED)

Conteúdo Programático 4: Contratos inteligentes.

Bibliografia Básica:

GLAZER, David; JENKINS, Tom; SCHAPER, Hartmut. **Enterprise Content Management Technology**: What you need to know. Canada: Open Text Corporation, 2005.

MOUGAYAR, William. **Blockchain para negócios**: Promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books Editora, 2017.

MULBERT, Ana Luísa... [et al.]. **Organizações do conhecimento**: infraestrutura, pessoas e tecnologia. 2. ed. São Paulo: Editora Saraiva, 2017.

Bibliografia Complementar:

BERGAMO FILHO, Clovis. **Ruptura no modelo tradicional das empresas: 10 grandes especialistas ajudam a desvendar as mudanças que estão impactando sua organização.** Rio de Janeiro: Brasport, 2019

CRUZ, Tadeu. **Gerência do Conhecimento.** Rio de Janeiro: E-papers, 2007.

FAUAT, Ana Matilde. **Comunicação da informação, gestão da informação e gestão do conhecimento.** Brasília: Ibict, 2018.

OLIVER, Paulo Roberto Costa. **Projetos de ECM/BPM: os segredos da construção.** São Paulo: Biblioteca24horas, 2010.

OLIVEIRA, Marcos Alberto de. **Estratégia empresarial e gestão da informação gerencial.** São Paulo: Editora Senac, 2018.

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.

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

Disciplina: Cloud computing.

Ementa: Introdução a *cloud computing* (nuvem). Arquitetura de *cloud computing*. Governança de TI e *cloud computing*. Infraestrutura de nuvem. Serviços de nuvem. Aplicações.

Competências e Habilidades:

- Conhecer as vantagens e desvantagens da computação em nuvem.
- Tomar decisões de projeto e aquisição de serviços em nuvem.
- Desenvolver serviços em nuvem cumprindo requisitos de segurança da informação.
- **Conteúdo Programático 1:** Introdução à *cloud computing*: Arquitetura e infraestrutura.
- **Conteúdo Programático 2:** Governança de TI e *cloud computing*.
- **Conteúdo Programático 3:** Serviços de nuvem.
- **Conteúdo Programático 4:** Principais aplicações e futuro em *cloud computing*.

Bibliografia Básica:

CHEE, Brian J. S.; FRANKLIN, Curtis. **Computação em nuvem:** cloud computing: tecnologias e estratégias. São Paulo: M. Books do Brasil, 2013.

DIÓGENES, Yuri; VERAS, Manoel. **Certificação Cloud Essentials:** guia preparatório para o exame CLO - 001. Rio de Janeiro: Novaterra, 2014.

VELTE, Anthony T.; VELTE, Toby J.; ELSENPETER, Robert. **Cloud computing:** computação em nuvem, uma abordagem prática. Rio de Janeiro: Alta Books, 2011.

Bibliografia Complementar:

MORAES, Alexandre Fernandes de. **Telemática convergência de dados, voz e imagem**. São Paulo: Erica, 2014.

TAURION, Cezar. **Cloud computing**: computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

VERAS, Manoel. **Cloud Computing**: nova arquitetura da TI. Rio de Janeiro: Brasport, 2012.

Disciplina: Segurança em cloud computing.

Ementa: Identificação de riscos e cenários vulneráveis em computação em nuvem. Planejamento de ações de continuidade de negócios, recuperação de desastres e mitigação de incidentes. Segurança operacional, ambiente de desenvolvimento e de dados. Proteção de dados e controle de acesso.

Competências e Habilidades:

- Analisar e mitigar os riscos de perda e indisponibilidade de ativos em ambientes de nuvem.
- Identificar e valorar o contingenciamento necessário para recuperar desastres ou minimizar incidentes.
- Elaborar planos de continuidade dos negócios, procedimentos de recuperação, trilhas de auditoria para as informações armazenadas na nuvem.
- Identificar, analisar ameaças e vulnerabilidades e seu potencial impacto nos ativos provisionados em *cloud computing*.

Conteúdo Programático 1: Riscos, identificação e cenários vulneráveis em computação em nuvem. Continuidade dos negócios virtuais e recuperação de desastres.

Conteúdo Programático 2: Segurança operacional e gestão de incidentes em ambientes virtualizados. Segurança no desenvolvimento de aplicações em ambientes de nuvem. Criptografia e gerenciamento de chaves de segurança.

Conteúdo Programático 3: Gestão de perfis de usuários nos ambientes virtuais. Projetos de controle de segurança nas máquinas virtuais e nos sistemas operacionais remotos.

Conteúdo Programático 4: Confidencialidade dos dados armazenados e processados em arquitetura *cloud computing*.

Bibliografia Básica:

LIMA, A. C. **Segurança na Computação em Nuvem**. São Paulo: Editora Senac, 2018. eBook.

FERREIRA, Sergio da Costa. **Sistemas de informação em segurança**. Londrina: Editora e Distribuidora Educacional, 2017

SANTOS, A. **Segurança em Soluções que utilizam Cloud Computing**. AWS, 2013.

Bibliografia Complementar:

ANTUNES, J. L. Amazon AWS. **Descomplicando a computação em nuvem**. São Paulo: Casa do Código, 2016.

SILVA, W. F. **Aprendendo Docker. Do básico à orquestração de contêineres**. São Paulo: Novatec, 2016.

LOPER, Adriene Aparecida; SILVA, Nathalia dos Santos; LOPES, Giancarlo Michelino Gaeta. **Projeto de redes e sistemas distribuídos**. Londrina: Editora e Distribuidora, 2019.

Disciplina: Monetização digital: criptomoedas e NFTs

Ementa: Princípios fundamentais do Blockchain. Principais moedas digitais. Criação de carteiras digitais. Forma correta de iniciar investimentos em NFTs. NFTs e o metaverso.

Competências e Habilidades:

- Conhecer a criação de carteiras digitais
- Conhecer como funciona os investimentos em Criptomoedas
- Entender sobre NFTs não fungíveis
- Compreender a relação e evolução das NFTs no Metaverso

Conteúdo Programático 1: Visão Geral do Blockchain

Conteúdo Programático 2: Visão Geral dos NFTs

Conteúdo Programático 3: Carteiras Digitais

Conteúdo Programático 4: Visão Geral das Criptomoedas

Bibliografia básica:

BARBARA, Mauricio. MOEDAS DIGITAIS E OS DESCAMINHOS DO CAPITALISMO. **Revista Mouro**, v. 12, n. 15, 2022.

TRICHES, Divanildo. Moedas digitais na ótica das finanças internacionais. 2022.

DA SILVA GONÇALVES, Luiz Antônio et al. Carteiras digitais: o futuro dos pagamentos móveis. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 1, p. 377-393, 2022.

Bibliografia Complementar:

ANDRADE, Lia; CENDÃO, Fabio. **Direito, Metaverso e NFTs: Introdução aos desafios na Web3**. Saraiva Educação SA, 2022.

AFONSO, José Roberto Rodrigues; DA NÓBREGA, Marcos Antônio Rios; DE CASTILHOS, Núbia Nette Alves Oliveira. Criptomoedas e Moedas Digitais dos Bancos Centrais—Desafios e Perspectivas da Tributação no Brasil. **Direito Público**, v. 19, n. 102, 2022.

FIDELIS, Mateus André et al. Um estudo sobre Non-Fungible Token (NFT). 2022.

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.

