



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
MBA em Segurança 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 Egresso.....	5
8.	Metodologia de Ensino e Aprendizagem	6
9.	Estágio Não Obrigatório	9
10.	Matriz Curricular	10
11.	Carga Horária.....	10
12.	Conteúdo programático	10
13.	Infraestrutura Física e Pedagógica	27

1. Nome do Curso e Área do Conhecimento

Nome do Curso: MBA em Segurança digital

Área de Avaliação (CAPES): Ciência da Computação

Grande Área (CAPES): Ciências Exatas e da Terra (10000003)

Área do Conhecimento (CAPES): Ciência da Computação (10300007)

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

O curso é recomendado para profissionais graduados em tecnologia da informação, segurança da informação, ciência da computação, análise de

sistemas e demais profissionais que queiram aprimorar os conhecimentos nas tecnologias e políticas de segurança digital.

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 curso atende as perspectivas do mercado que demanda por profissionais com competências voltadas não só para a importância da segurança digital e suas tecnologias, mas também na governança de TI e políticas de segurança, com foco em sistemas e segurança, políticas de segurança e classificação da informação, certificação digital e blockchain, criptografia hash e hacking, cybersecurity, segurança em cloud computing e lei geral de proteção de dados, amparados por um conteúdo programático diferenciado.

6. Objetivos do Curso

6.1. Objetivo Geral

- O curso de MBA em Segurança Digital visa atender as novas perspectivas do mercado, promovendo formação diferenciada. Tem o objetivo de desenvolver e especializar o profissional em tecnologias utilizadas na área de segurança digital com conhecimentos gerais sobre governança de TI. As tecnologias aprimoradas são: Sistemas e segurança, certificação digital, blockchain, criptografia hash e hacking, cybersecurity e cloud computing.

6.2. Objetivos Específicos

- Aprofundar o domínio da gestão e proteção de dados com conhecimentos de governança TI e tecnologias de segurança de dados.
- Compreender as políticas de segurança e melhores práticas de governança de TI.
- Preparar para elaborar plano, analisar e avaliar práticas de certificação digital, blockchain e criptografia.
- Oferecer conhecimentos específicos essenciais sobre privacidade, proteção e governança de dados.
- Preparar profissionais para analisar e avaliar políticas de segurança e governança de dados e orientar sobre melhores práticas.
- Proporcionar conhecimento para elaboração de projetos que protejam os dados e os negócios de organizações.
- Aprofundar os conhecimentos técnicos ligados a cloud computing e cybersecurity.

7. Competências e Habilidades do Egresso

Competências

O especialista em Segurança Digital desenvolve um conjunto de competências voltadas para gestão, governança e assessoria técnica para a proteção de dados e sistemas. Para tal, o curso abordará visão ampla e integrada a temas atuais acerca de sistemas e segurança, políticas de segurança e classificação da informação, certificação digital e blockchain, criptografia hash e hacking, cybersecurity, segurança em cloud computing e lei geral de proteção de dados.

Habilidades

- Compreender a dinâmica e a interação da governança de TI com a segurança digital.
- Definir políticas de segurança e classificação da informação.
- Analisar e recomendar uso de tecnologias de certificação digital, blockchain e criptografias hash e hacking.
- Compreender e planejar políticas de segurança em cloud computing.
- Criar estratégias e planos de proteção de dados e negócios da organização.
- Compreender e demonstrar capacidade de avaliar questões relacionadas a lei geral de proteção de dados.

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 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.

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
Governança de dados	0 h	40 h	40 h
Governança em TI	0 h	40 h	40 h
Sistemas e segurança	0 h	40 h	40 h
Políticas de segurança e classificação da informação	0 h	40 h	40 h
Certificação digital e blockchain	0 h	40 h	40 h
Criptografia hash e hacking	0 h	40 h	40 h
Cybersecurity	0 h	40 h	40 h
Segurança em cloud computing	0 h	40 h	40 h
Lei Geral de proteção de dados	0 h	40 h	40h

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: Governança de dados

Ementa: Visão geral da gestão de dados, governança de dados, gestão da arquitetura de dados, desenvolvimento de dados, gestão de dados mestre e dados de referência.

Competências e Habilidades:

- Compreender o ciclo de vida do dado e o papel da governança
- Elaborar projetos usando princípios de governança de dados
- Esquematizar arquitetura de dados
- Aplicar princípios da gestão de dados

Conteúdo Programático 1: Introdução à governança de dados. Dado como ativo corporativo. Ciclo de vida do dado. Gestão de dados. O profissional de governança de dados.

Conteúdo Programático 2: Visão geral da gestão de dados. Missão, princípios e objetivos. Funções e atividades. Papéis e responsabilidades. Tecnologias.

Conteúdo Programático 3: Conceito de governança de dados. Conceitos e atividades. Detalhes de atividades da governança de dados. Desenvolvimento de dados. Estilos de modelagem de dados. Design de dados. Implementação de dados.

Conteúdo Programático 4: Arquitetura de dados. Gestão da arquitetura de dados. Conceitos e atividades. Princípios gerais. Gestão de dados mestre. Conceitos de dado mestre e dado de referência. Integração de dados. Gestão de mudanças.

Bibliografia Básica:

BRACKETT, Michael; EARLEY, Production Susan. **The DAMA Guide to The Data Management Body of Knowledge** (DAMA-DMBOK Guide), 2009.

BARBIERI, Carlos. **Governança de Dados:** Práticas, conceitos e novos caminhos. Alta Books, 2020.

RÊGO, Bergson Lopes. **Gestão e governança de dados:** promovendo dados como ativo de valor nas empresas. Brasport, 2013.

SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. **Business Intelligence e Análise de Dados para Gestão do Negócio**. Porto Alegre: Bookman, 2019.

Bibliografia Complementar:

HASHEM, I. A. T.; YAQOOB, I.; ANUAR, N.B.; MOKHTAR, S.; GANI, A.; KHAN, S.U. **The rise of “big data” on cloud computing: review and open research issues**. Information Systems 47 (2015), 98 - 115.

LOSHIN, David. **Master data management**. Morgan Kaufmann, 2010.

BAKSHI, Kapil. Considerations for big data: Architecture and approach. In: **2012 IEEE aerospace conference**. IEEE, 2012. p. 1-7.

Disciplina: Governança em TI

Ementa: Conceitos de Governança Corporativa e de TI. Normas, processos e indicadores de desempenho para a área de TI. Conceitos das melhores práticas em processos e serviços de TI – Guias de governança: COBIT (Control Objectives for Information and Related Technology) e ITIL (Information Technology Infrastructure Library), SCRUM, Métodos ágeis, ISO 38500 e PMI, em contraponto.

Competências e Habilidades:

- Entender os fundamentos que sustentam a governança em TI;
- Aplicar modelos de governança, adequados para cada contexto;
- Dominar a visão geral da ITIL;
- Compreender as aplicações de métodos ágeis na implantação de práticas de governança e *compliance*;
- Absorver a visão geral de *compliance*: COSO e resultados.

Conteúdo Programático 1: Fundamentos da governança de TI.

Relacionamento entre governança de TI e governança corporativa. Governança corporativa e recomendações de *compliance*.

Conteúdo Programático 2: Um modelo proposto para governança de TI: alinhamento estratégico, entrega de valor, gerenciamento de recursos. *Compliance*. ISO 38500/2018.

Conteúdo Programático 3: Visão geral da ITIL: gerenciamento de serviços de TI. A fase de estratégia de serviço.

Conteúdo Programático 4: ITIL: a fase de desenho de serviço e transição de serviços. A fase de operação de serviço. A fase de melhoria contínua de serviço.

Conteúdo Programático 5: Visão geral do COBIT: propósito do COBIT. A estrutura do COBIT: *framework* integrado único. O modelo de processos do COBIT. Diretrizes de implementação do COBIT.

Conteúdo Programático 6: Métodos ágeis: SCRUM e gestão de projetos (PMBOK).

Conteúdo Programático 7: Visão geral de *compliance*: COSO e resultados.

Bibliografia Básica:

ABNT. NBR ISO/IEC 38500:2018: Governança Corporativa de Tecnologia da Informação. Associação Brasileira de Normas Técnicas, 2009.

IBGC. Código das Melhores Práticas de Governança Corporativa. 4. ed. Instituto Brasileiro de Governança Corporativa, 2000.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. 4. ed. São Paulo: Saraiva, 2014.

Disciplina: Sistemas e Segurança

Ementa: Redes de Computadores: principais aspectos. Tipos de redes de computadores. Topologias Físicas das Redes de Computadores. Modelos de Referência. Segurança de Redes: principais aspectos. Criptografia. Segurança da Informação. Protocolos de Autenticação. Proteção de da Dados.

Competências e Habilidades:

-Identificar os principais tipos de redes de computadores e suas respectivas arquiteturas;

- Avaliar os modelos de referência de arquiteturas de redes computadores;
- Definir protocolos de redes de computadores aplicáveis em situações específicas;
- Reconhecer as principais técnicas de segurança de redes de computadores;
- Avaliar as técnicas de segurança de redes de computadores aplicáveis em situações específicas.

Conteúdo Programático 1: Redes de Computadores. O Uso de Redes de Computadores. Tipos de redes de computadores. Arquitetura de Redes de Computadores. Exemplos de Redes.

Conteúdo Programático 2: Modelos de Referência de Redes de Computadores. O Modelo OSI da ISO. O Modelo de Referência TCP/IP. Protocolos de Redes de Computadores.

Conteúdo Programático 3: Segurança de Redes de Computadores. Criptografia. Algoritmos de Chave Simétrica. Algoritmos de Chave Pública. Assinaturas Digitais. Gerenciamento de Chaves Públicas.

Conteúdo Programático 4: Conexões Seguras. Protocolos de Autenticação. Técnicas de comunicação segura. Redes Privadas Virtuais.

Bibliografia:

MENDES, Douglas Rocha. Redes de Computadores: teoria e prática. 2. ed. São Paulo: Editora Novatec, São Paulo, 2015.

OLIVEIRA, Roberto Carlos Queiroz. Segurança em Redes de Computadores. São Paulo: Editora SENAC, 2018.

STALLINGS, William. Criptografia e Segurança de Redes: princípios e práticas. 6. ed. São Paulo: Editora Pearson, 2014.

TANENBAUM, Andrew S. Redes de Computadores. 4. ed. São Paulo: Editora Pearson, 2011.

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.

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:

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: 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: 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: 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: 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.

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.

