



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
Segurança da Informação

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: Segurança da informação.

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: 200 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 se destina a profissionais graduados nas áreas de Análise e

Desenvolvimento de Sistemas, Arquivologia, Biblioteconomia, Ciência da Computação, Ciência da Informação, Engenharia de Computação, Redes de Computadores, bem como à profissionais que trabalham com servidores de dados, provedores de internet e com sistemas de informação de todas as áreas.

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

As informações são recursos econômicos e gerenciais indispensáveis nas organizações, de modo que proteger os dados no ambiente corporativo contribui para a empresa se manter competitiva na era da Informação.

Com a constante evolução da tecnologia e a necessidade de atuar dentro das exigências legais no que tange à segurança de dados, cada vez mais existirão oportunidades para profissionais com conhecimento em segurança de dados. Além do mais, crimes cibernéticos também evoluem em estratégia, técnica e tecnologia, tornando o cenário desafiador para empresas, instituições governamentais e para as pessoas de uma forma geral.

O curso de Segurança da Informação busca atender a demanda do mercado por profissionais aptos para desenvolver e atuar com ferramentas computacionais e políticas de gerenciamento de dados específicas para segurança da informação. Os conteúdos abordados no curso são multidisciplinares, envolvendo algoritmos, novas tecnologias em redes de comunicação e gestão de tecnologia da informação, pautados nos aspectos legais mais recentes da Segurança da Informação.

6. Objetivos do Curso

6.1. Objetivos Gerais

Capacitar profissionais para atuarem em empresas de TI, setores de TI de médias e grandes empresas, provedores de internet, *cloud computing* e *data centers*, com foco na tomada de decisões em gestão de informações e estratégias de segurança da informação para proteção de dados.

6.2. Objetivos Específicos

- Apresentar os conceitos gerais acerca dos pilares da segurança da informação: confiabilidade, integridade, disponibilidade, autenticidade e irrefutabilidade.
- Apresentar os processos e técnicas mais recentes quanto à legislação de proteção de dados.
- Proporcionar os conhecimentos acerca de técnicas e algoritmos relacionados à criptografia, redes de computadores e gestão eletrônica de documentos.
- Elencar as políticas e as tendências mais atuais no armazenamento e compartilhamento de informações.

7. Competências e Habilidades do Curso

Competências

Atuar na tomada de decisão quanto às estratégias de proteção de dados pessoais, corporativos e governamentais, avaliando algoritmos, ferramentas e políticas de segurança da informação.

Habilidades

- Identificar ameaças, invasões, *softwares* maliciosos e demais formas de ataques cibernéticos;
- Aplicar as técnicas e algoritmos de criptografia de dados e gerenciamento eletrônico de documentos visando manter os padrões

de segurança da informação;

- Aplicar técnicas de gestão de informação e governança de TI para proteger os dados das empresas, como forma de diferencial competitivo nas organizações.

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 compromissado 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

III. 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	0h	0h	0h
Governança em TI	0h	40h	40h

Gestão de riscos em TI	0h	40h	40h
Segurança em redes de computadores	0h	40h	40h
Lei Geral de Proteção de Dados	0h	40h	40h
ECM, GED e contratos inteligentes	0h	40h	40h
Função de criptografia HASH	0h	40h	40h
<i>Cloud computing</i>	0h	40h	40h
Políticas de segurança e classificação da informação	0h	40h	40h
Introdução à computação forense	0h	40h	40h

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: 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: Gestão de riscos em TI

Ementa: Introdução à Gestão de Riscos em TI. Contexto. Identificação de riscos. Análise de riscos. Avaliação de riscos. Tratamento e aceitação de riscos. Monitoramento dos riscos.

Competências e Habilidades:

- Conhecer as normas de gestão de segurança e de riscos.
- Atuar na identificação, análise e avaliação de riscos em TI.
- Manter estratégias de tratamento e aceitação de riscos em TI.

Conteúdo Programático 1: Introdução à Gestão de riscos.

Conteúdo Programático 2: Contexto e Identificação de riscos.

Conteúdo Programático 3: Análise e Avaliação de riscos.

Conteúdo Programático 4: Tratamento, aceitação e monitoramento dos riscos.

Bibliografia Básica:

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.

WESTERMAN, George; HUNTER, R. **IT Risk:** Turning Business Threats Into Competitive Advantage. Massachusetts: Harvard Business School Press, 2007.

Bibliografia Complementar:

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

CABRAL, Carlos; CAPRINO, Willian. **Trilhas em Segurança da Informação:** caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

HARKINS, Malcolm W. **Managing Risk and Information Security:** Protect to Enable. California: Apress Open, 2016.

MANOEL, Sergio da Silva. **Governança de Segurança da Informação:** como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014.

POMPON, Raymond. **IT Security Risk Control Management:** An Audit Preparation Plan. Apress Berkely, CA, 2016.

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: 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: 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: 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: 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: 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: 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..

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.

