



PROJETO PEDAGÓGICO DE CURSO
Pós-Graduação *Lato Sensu*
Segurança de redes

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	9
10. Matriz Curricular	10
11. Carga Horária.....	11
12. Conteúdo Programático.....	11
13. Infraestrutura Física e Pedagógica.....	32

1. Nome do Curso e Área do Conhecimento

Nome do Curso: Segurança de redes.

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 é destinado a bacharéis em Engenharia da Computação; Cientistas da Computação; Tecnólogos em Análise de Sistemas, Desenvolvimento WEB, Banco de Dados, Analistas na área de gestão da Tecnologia da

Informação, assim como a empreendedores interessados em implementar ferramentas para prevenção e solução de problemas e gestão de Segurança da Informação.]

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 ABES (Associação Brasileira de Empresas de Software) apresenta os resultados do Estudo deste mercado e mostra que o Brasil tem se mantido em 9º lugar no *ranking* mundial de investimentos em Tecnologia da Informação, de acordo com o estudo “Mercado Brasileiro de Software e Serviços”, da ABES em conjunto com o IDC, divulgada abril de 2018. O documento, que utiliza dados do IDC referentes ao último ano, mostra que os investimentos em TI (*software*, *hardware* e serviços) no Brasil superaram as expectativas para 2018, chegando a US\$47 bilhões, um crescimento de 9,8% em relação a 2017, mais que o dobro da previsão para o ano, que foi de 4,1%.

O crescimento dos investimentos em TI destaca o fato da necessidade de soluções de segurança para que as empresas se beneficiem dos recursos para que estejam disponíveis, íntegros e confiáveis, para sua utilização com facilidade, flexibilidade e dinamismo. Possibilitar a análise de ferramentas que aumentem a tranquilidade da utilização de tecnologias inovadoras e de alta performance.

O curso busca atender a demanda por conhecimento e ferramentas de segurança, que visem eficiência, para profissionais e gestores, que buscam aprofundamento ou atualização na área de segurança de redes para desenvolvimento de produtos e projetos. Assim, a formação tem foco na agilização de planos, organização, controle de processos e projetos de

segurança. Para tanto, os conteúdos versam sobre as técnicas e processos de segurança propriamente dita.

Os conceitos, metodologias e técnicas apresentadas ao longo do curso têm origem de diferentes segmentos corporativos, com sua abrangência do comércio, indústria, serviços entre outras.

6. Objetivos do Curso

6.1. Objetivos Gerais

O Curso de Especialização em Segurança de Redes, tem por objetivo geral atualizar e instrumentalizar o discente para desenvolvimento de atividades específicas e normatizadas para subsidiar a tomada de decisão, elaboração de estratégias inovadoras adaptadas as constantes mudanças dos cenários econômicos, tecnológicos e sociais, formar gestores de segurança da informação éticos e técnicos, com perfil proativo, dinâmico e crítico, capaz e atuar no mercado.

6.2. Objetivos Específicos

- Identificar as melhores práticas de identificação de riscos e implantação de controles a partir da implantação de soluções normatizadas.
- Implantar Núcleo/Escritório de Segurança de Redes, bem como entender quais são as atividades rotineiras que precisam ser executadas para garantir um ambiente seguro.
- Definir e implantar arquiteturas rígidas para redução das vulnerabilidades.
- Utilizar tecnologia, processos e pessoas no parque tecnológico para que possa proporcionar níveis elevados de proteção, minimizando os riscos.

7. Competências e Habilidades do Curso

Competências

O egresso deverá atuar em segurança, com aplicação de políticas em conformidade com as normas considerando a disponibilidade, integridade e confidencialidade da Informação.

Habilidades

O egresso deverá ser capaz de:

- Implementar políticas e procedimentos de segurança informática, analisar de riscos;
- Aplicar as melhores práticas para implantar arquiteturas de segurança em redes computacionais;
- Identificar e planejar testes de segurança em equipamentos e sistemas;
- Utilizar, propor e gerir ferramentas e tecnologias de identificação e acessibilidade.

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.

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:

- ✓ Leitura de textos de fundamentação teórica.
- ✓ Acesso às videoaulas.
- ✓ Aprofundamento dos seus conhecimentos, acessando elementos extratextuais.

- ✓ Desafio Profissional, com resolução para autoestudo.
- ✓ Realização de questões de autoestudo, para verificação de seu desempenho.

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
- 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 obedeçam 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 em conjunto com o professor orientador e também do Departamento de Estágios, devendo conter os seguintes dados:

- I. matrícula regular especificando o semestre;
- II. disciplinas ou habilidades imprescindíveis ao seu desenvolvimento;
- III. atividades a serem desenvolvidas;
- IV. supervisor de campo;
- V. seguradora e apólice de seguro;
- VI. bolsa-auxílio ou contraprestação;
- VII. auxílio-transporte;
- VIII. período de realização;
- IX. período (s) de recesso; e

X. carga horária diária e semanal.

A orientação de estágio curricular pelo Departamento de Estágios deverá ser realizada por meio de orientação indireta mediante relatórios e, sempre que possível, visitas ao campo de estágio, além da utilização das tecnologias de informação e comunicação para contato das partes envolvidas.

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
Lei Geral de Proteção de Dados	0h	40h	40h
Auditoria de sistemas	0h	40h	40h
Infraestrutura e conectividade de redes	0h	40h	40h
Análise de dados	0h	40h	40h
Criptografia <i>hash</i> e <i>hacking</i>	0h	40h	40h
Certificação digital e <i>blockchain</i>	0h	40h	40h
Cybersecurity	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 ISO 27001 e na ISO 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: 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: Auditoria de sistemas

Ementa: Auditoria de Sistemas. Conceitos, características e riscos de auditoria. Modelo de segurança em ambiente de processamento de dados. Segurança Lógica e Física. O processo de auditoria de sistemas. Planejamentos dos trabalhos em ambiente computacional. Execução da auditoria aplicável no gerenciamento e controle dos aplicativos: Programas, procedimentos e técnicas aplicáveis. Conceito e objetivos da auditoria de sistemas de informação. Técnicas de auditoria em sistemas de informação. Softwares de auditoria. Estrutura da função de auditoria de sistemas de informação nas organizações

Competências e Habilidades:

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

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

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

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

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

Bibliografia Básica:

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

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

Manual de auditoria de sistemas -

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

Bibliografia Complementar:

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

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

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

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

ARIMA, Carlos Hideo; SCHMIDT, Paulo e SANTOS, José Luiz dos.

Fundamentos de Auditoria de Sistemas. São Paulo: Atlas, 2006.

Disciplina: Infraestrutura e conectividade de redes

Ementa: Conceito e história (infraestrutura e cabeamento). Cabeamento estruturado e redes Wifi. Arquiteturas e protocolo. *Switching* e roteamento.

Competências e Habilidades:

- Atuar na infraestrutura e interconexão, com aplicação de políticas em conformidade com as normas considerando a disponibilidade, integridade e confidencialidade;
- Ser capaz de implementar políticas e procedimentos que subsidiem a análise de segurança da infraestrutura e interconexão, analisar conexões;
- Aplicar as melhores práticas para implantar arquiteturas e infraestrutura em redes computacionais;
- Identificar e planejar testes de conexão em equipamentos e sistemas;
- Utilizar, propor e gerir ferramentas e tecnologias de identificação e acessibilidade.

Conteúdo Programático 1: Conceito e história (infraestrutura e cabeamento).

Conteúdo Programático 2: Cabeamento estruturado e redes Wifi.

Conteúdo Programático 3: Arquiteturas e protocolo.

Conteúdo Programático 4: *Switching* e roteamento.

Bibliografia Básica

BRISA (Sociedade Brasileira para Interconexão de Sistemas Abertos). Gerenciamento de redes: uma abordagem de sistemas abertos. 1. Ed. São Paulo: Makron Book, 1993.

FEIT, Sidnie. **SNMP**: A guide to Network Management. 1. Ed. São Paulo: McGraw-Hill, 1995.

HARNEDY, Sean. **Total SNMP**: Exploring the Simple Network Management Protocol. São Paulo: Prentice-Hall, 1997.

LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S. **Melhores práticas para gerência de redes de computadores**. 1. Ed. São Paulo: Campus, 2003.

MARIN, Paulo Sérgio. **Cabeamento Estruturado**. 3. Ed. São Paulo: Érica, 2010.

Bibliografia Complementar:

PERKINS, Avid. **Understanding SNMP MIBs**. 2. Ed. São Paulo: Prentice-Hall, 1993.

ROSE, Marshall. **The Simple Book**. 2. Ed. São Paulo: Prentice-Hall, 1996.

ROSE, M.; McCLOGHRIE, K. **How to Manage your Network Using SNMP – The Network Management Practicum**. São Paulo: Prentice Hall, 1995.

SCHMIDT, Mauro. **Essential SNMP**. 2. Ed. O' Reilly, 2005.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3 e RMON 1 e 2**. 3. Ed. Addison-Wesley, 1999.

STALLINGS, William. **Data and Computer Networks**. São Paulo: Prentice-Hall, 2004.

STEVENS, W. Richard; WRIGTH, Gary R. **TCP/IP Illustrated**. Vols. 1 e 2. São Paulo: Prentice Hall, 1998.

TANENBAUM, Andrew S. **Rede de Computadores**. São Paulo: Editora Campus, 2003.

CCNA ICND Exam Certification Guide (CCNA Self-Study, 640-811, 640-801).

CCNP BCRAN Exam Certification Guide (CCNP Self-Study, 642-821) 2 ed.

Inc. Cisco Systems. *Internetworking Technologies Handbook*. 2 ed., Cisco Press, 2000.

Disciplina: Análise de dados

Ementa: Apresentação do conceito de desenho de pesquisa como ponto de partida para o ensino de métodos quantitativos. A disciplina passará por noções básicas de análise de dados e estatística, como a definição de população e amostra e construção de hipóteses. Também será feita uma introdução às inferências bivariadas e à distinção entre associação e causalção.

Competências e Habilidades:

- Ser consciente em relação à importância de um desenho de pesquisa robusto, assim como em relação às análises realizadas por meio dos métodos quantitativos;
- Ser capaz de realizar pesquisas empíricas com testes de hipótese e inferência bivariada;
- Saber a diferença entre associação entre duas ou mais variáveis e a ideia de causalção.

Conteúdo Programático 1: Desenho de pesquisa: o que é um desenho de pesquisa? E por que ele é importante? Noções de análise de dados: população e amostra; distribuições comuns; variáveis dependente, independente e de controle; mensuração de variáveis; confiabilidade e validade; erros de mensuração aleatórios e sistemáticos; estrutura dos dados.

Conteúdo Programático 2: Estatística descritiva: medidas de tendência central (média, moda e mediana); valores máximo e mínimo; medidas de dispersão (alcance, variância e desvio padrão); Introdução aos testes de hipótese: hipótese nula e hipótese alternativa.

Conteúdo Programático 3: Testes de hipótese bivariados: teste-t (para amostras independentes e emparelhadas); correlação; por que inferência não significa causalidade? Metodologia: aulas expositivas, com apresentações teóricas e práticas. As aulas apresentarão os métodos de maneira intuitiva, de forma a tornar a estatística mais amistosa aos que não são familiarizados com os temas.

Conteúdo Programático 4: As teorias serão apresentadas de forma aberta às intervenções dos discentes. Em termos práticos, serão utilizados dados reais e/ou de simulação para análise em *software* livre.

Bibliografia Básica:

AGRESTI, Alan; FINLAY, Barbara. **Métodos Estatísticos para as Ciências Sociais**. 4. Ed. Porto Alegre: Penso, 2012.

DANCEY, Christine P.; REIDY, JOHN. **Estatística sem Matemática para Psicologia**. 5. Ed. Porto Alegre: Penso, 2013.

KELLSTEDT, Paul M.; WHITTEN, Guy D. **Fundamentos da Pesquisa em Ciência Política**. São Paulo: Blucher. 2015.

TRIOLA, Mario. **Introdução à Estatística**. 12. ed. São Paulo: Grupo GEN. 2017.

WOOLDRIDGE, Jeffrey. **Introdução à Econometria**. Uma abordagem moderna. 3. Ed. São Paulo: Cengage Learning, 2017.

Bibliografia Complementar:

BOX-STEFFENSMEIER, Janet M.; BRADY, Henry E.; COLLIER, DAVID. **The Oxford Handbook of Political Methodology**. Oxford, UK: Oxford University Press, 2010.

BRADY, Henry E.; COLLIER, David (Editors). **Rethinking Social Inquiry: Diverse tools, shared standards**. 2nd ed. Lanham, MD: Rowman & Littlefield. 2010.

HAIR, Joseph F. et al. **Análise Multivariada de Dados**. 6. Ed. Porto Alegre: Bookman, 2009.

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney. **Designing Social Inquiry: Scientific inference in qualitative research**. Princeton, NJ: Princeton University Press, 1994.

LATTIN, James; CARROLL, Douglas J.; GREEN, Paul E. **Análise de Dados Multivariados**. São Paulo: Cengage Learning, 2010.

POLLOCK, Philip. **The Essentials of Political Analysis**. 5th ed. Washington, DC: CQ Press, 2015.

VAN EVERA, Stephen. **Guide to Methods for Students of Political Science**. Ithaca, NY: Cornell University Press, 1997.

WHEELAN, Charles. **Estatística**. O que é, para que serve, como funciona. Rio de Janeiro: Zahar, 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: 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: 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

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.

