Curso de Especialização em **Segurança e Inteligência Cibernética**
Estrutura Curricular – disciplina/carga horária.

CiberSecurity	
Segurança na TI BiModal	32 h/a
Projetos de Arquitetura e Tecnologias de Segurança	32 h/a
Criptografia e Certificados Digitais	32 h/a
Evolução das Ameaças	32 h/a
Carga horária total do módulo	*128h/a*
CiberIntelligence	
Next Generation Cyber Defense	32 h/a
Estratégia e Inteligência Cibernética	32 h/a
Governança da Segurança Cibernética	32 h/a
Resposta a Incidentes de Segurança	32 h/a
Carga horária total do módulo	*128h/a*
CiberHuman	
Ethical Hacker	32 h/a
Computação Forense	32 h/a
Criminalística e Legislação	32 h/a
Empreendedorismo Cibernético	32 h/a
Carga horária total do módulo	*128h/a*
Aplicação do Conhecimento	
Aplicação do Conhecimento	48h/a **a distância**
Carga horária total do módulo	*48h/a*
Total da carga horária do curso	**432h/a**

IDENTIFICAÇÃO DA DISCIPLINA (01)

1. **Nome da Disciplina:** Segurança na TI BiModal

2. **Carga Horária:** 32 horas/aula

3. **Ementa:** Segurança de Redes de Computadores com e sem fio. Processos de segurança da informação em Data Center, onde o novo modelo de processos funciona ao lado do modelo tradicional.

4. **Objetivo:** Apresentar aos alunos os fundamentos da segurança cibernética e da informação convivendo sempre o legado com o novo.

5. **Conteúdo Programático:** Pilares da segurança em redes de computadores: Confidencialidade, Integridade e Disponibilidade. Conceitos. Segurança nas Redes de Computadores com e sem fio. Segurança em Cloud Computing. Segurança em Data Center. Segurança em IoT. Ttipos de Arquitetura de redes. Protocolos de redes TCP/IP. Aspectos de segurança em cada camada da pilha e seus respectivos protocolos. Computação úbiqua e Pervasiva. Redes sem fio. Segurança em Cloud Computing. Tipos de Cloud.

6. **Bibliografia:**

   a. **Básica:**

BEAL, Adriana. Segurança da informação: princípios e melhores práticas para proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

SCHNEIER, Bruce. Segurança.com: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001

DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de janeiro: Axcel Books do Brasil, c2000

   b. **Complementar:**

FERREIRA, Fernando Nicolau Freitas,. Segurança da informação. Rio de Janeiro: Ciência Moderna, c2008

FONTES, Edison. Vivendo a segurança da informação – Orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

MENEZES, Josué das Chagas. Gestão da segurança da informação. Leme: J. H. Mizuno, c2006

GIL, Antonio de Loureiro. Segurança em informática: ambientes mainframe, wan, lan e conexões via edi com plataformas de informática de outras organizações, integração da segurança empresarial e de in. 2. ed., 2. tiragem São Paulo: Atlas, 1998.

CAVALCANTI, A. & LIRA, E. Grafoscopia Essencial. Porto Alegre; Editora Sagra,1996.

CENTURION, Virgílio. Excelência em biometria. São Paulo: Cultura Médica, 2006.

Biometric Systems, Technology, Design and Performance Evaluation , A. Ross, K. Nandakumar, and A. K. Jain, 2005, Springer

ABNT NBR ISO/IEC 27001:2006 - Sistemas de gestão de segurança da informação

ABNT NBR ISO/IEC 27002:2005 - Código de pratica para a gestão da segurança da informação

ABNT NBR 16167:2013 - Diretrizes para classificação, rotulação e tratamento da informação

IDENTIFICAÇÃO DA DISCIPLINA (02)

1. **Nome da Disciplina**: Projetos de Arquitetura e Tecnologias de Segurança
2. **Carga Horária:** 32 horas/aula

3. **Ementa:** Projetos de Arquitetura e Tecnologias de Segurança. Projetos de SOC.

4. **Objetivo:** Apresentar aos alunos os tipos de Projetos de Arquitetura e Tecnologias de Segurança desde a Borda e as necessárias para se controlar um SOC.

5. **Conteúdo Programático:** Infraestrutura de Segurança. Cabeamento fisico. Projetos de Arquitetura de Segurança. Implementação. Análise do tráfego de pacotes nas redes com e sem fio para verificar ataques e ameaças. Segurança em ambientes móveis. Segurança nas comunicações sem fio bluetooth, wi-fi, wi-max, zigbee. Projeto de Cloud Segura. Desenvolvimento Seguro.

6. **Bibliografia:**

   a. **Básica:**

COMER, Douglas E.; “Interligação em Redes com TCP/IP. Volume 1: Princípios, Protocolos e Arquitetura”. 2ª Edição, Editora Campus, 1998

TANENBAUM, Andrew S. Redes de Computadores, Editora Campus, Rio de Janeiro, 1997.

KUROSE, James F.; ROSS, Keith W. "Redes de Computadores e a Internet: Uma nova abordagem", Editora Pearson do Brasil, 2005.

COULOURIS, G. F. Distributed systems: concepts and design. 3nd. ed. London: Addison-Wesley, 2001.

ORAM, A. (Ed.) Peer-to-Peer: o poder transformador das redes ponto a ponto. São Paulo: Berkeley, 2001.

PERKINS, CHARLES E. Ad Hoc Networking. Addison-Wesley Pub Co; 1st edition, Dezembro, 2001.

b. Complementar:

STALLINGS W.," Wireless Communications and Networks ". Prentice Hall, 2002.

STALLINGS, W. Local and Metropolitan Area Networks. Prentice-Hall, 6th edition, 2000.

STALLINGS, W. “Data and Computer Communications”, 6th ed., Prentice Hall, 1999.

STALLINGS, W; "Criptography and Network Security"; Prentice Hall,2nd Edition, 1998.

STUART MCCLURE, JOEL SCAMBRAY & GEORGE KURTZ, "Hacking Exposed, Network Security Secrets & Solutions", Osborne / McGraw-Hill, 1999.

CHAPMAN D. BRENT; ZWICKY, ELIZABETH D. - Building Internet Firewalls, O’Reilly & Associates Inc., 1st Edition, September 1995.

GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo Corrêa. Segurança com redes privadas virtuais – VPNs. Rio de Janeiro: Brasport, 2006.

STINSON, D.; Cryptography Theory and Practice - CRC Press, ISBN: 1-584-88508-4, 2005;

IDENTIFICAÇÃO DA DISCIPLINA (03)

1. **Nome da Disciplina**: Criptografia e Certificados Digitais
2. **Carga Horária:** 32 horas/aula
3. **Ementa:** Criptografia e Certificados Digitais
4. **Objetivo:** Apresentar aos alunos os conceitos de algoritmos de criptografia e certificados digitais.
5. **Conteúdo Programático:** Algoritmos criptográficos. PGP. Conceitos de chaves publicas e privadas. PGP. CERT.BR. Topologias das Entidades Certificadoras. Certificados Digitais Aquisição, Revogação. Emissão interna e controle. Assinatura Digital.
6. **Bibliografia:**
   a. **Básica:**

STALLINGS, W; "Criptography and Network Security"; Prentice Hall,2nd Edition, 1998.

STINSON, D.; Cryptography Theory and Practice - CRC Press, ISBN: 1-584-88508-4, 2005;

   b. **Complementar:**

STALLINGS W.," Wireless Communications and Networks ". Prentice Hall, 2002.

STALLINGS, W. Local and Metropolitan Area Networks. Prentice-Hall, 6th edition, 2000.

IDENTIFICAÇÃO DA DISCIPLINA (04)

1. **Nome da Disciplina**: Evolução das Ameaças
2. **Carga Horária**: 32 horas/aula
3. **Ementa:** Evolução das Ameaças. **P**rincipais ameaças e tipos de ataques que ocorrem nas redes de computadores e as estratégias de segurança utilizadas para evitar ataques e minimizar os riscos de incidentes.
4. **Objetivo:** Apresentar aos alunos a Evolução das Ameaças e técnicas de análises de malware e engenharia reversa.
5. **Conteúdo Programático:** Análise de vulnerabilidades em estações, servidores e Cloud. Tipos de ataques e possíveis contramedidas. Testes de Invasão. Hardening. Análise de Malware. Engenharia Reversa. Desenvolvimento de exploits. Análise de Riscos**.** Histórico dos ataques. Formas de ataques. Modos de mitigação de ataques a Internet.
6. **Bibliografia**:
   a. **Básica:**

MORAZ, Eduardo. Windows hacking/ guia completo: descubra todos os segredos e ferramentas ocultas no Windows. São Paulo: Digerati, 2009.

KIZZA, Joseph Migga. Computer network security and cyber ethics. 2nd ed. Jefferson: McFarland & Company, c2006.

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", Editora Pearson do

b. 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.

MOBILE agents and security. Berlin: Springer, c1998. x, 256 p. (Lecture notes in computer science)

TANENBAUM, Andrew S.; WETHERALL, D. Computer networks. 5th ed. Boston, MA; Columbus, OH: Prentice Hall, c2011

IDENTIFICAÇÃO DA DISCIPLINA (05)

1. **Nome da Disciplina**: Next Generation Cyber Defense
2. **Carga Horária:** 32 horas/aula
3. **Ementa:** Arquitetura de Sistemas Seguros. Tecnologias de Desenvolvimento Seguro.
4. **Objetivo:** Desenvolver o conhecimento de arquitetura e infraestrutura de sistemas necessário para analisar e especificar controles de segurança para sistemas seguros.
5. **Conteúdo Programático**: Arquitetura de sistemas. Diferentes tecnologias de desenvolvimento e suas principais características. Componentes de um sistema distribuído. Aspectos de segurança dos sistemas distribuídos. Análise de segurança. Processo de desenvolvimento seguro. Top 10 OWASP. Testes de segurança em aplicações Web. Cloud computing: conceitos e aspectos de

segurança. Big Data. Analytics. Armazenamento Seguro.

6. Bibliografia:

a. Básica:

KIZZA, Joseph Migga. Computer network security and cyber ethics. 2nd ed. Jefferson: McFarland & Company, c2006.

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", Editora Pearson do

b. 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.

MOBILE agents and security. Berlin: Springer, c1998. x, 256 p. (Lecture notes in computer science)

TANENBAUM, Andrew S.; WETHERALL, D. Computer networks. 5th ed. Boston, MA; Columbus, OH: Prentice Hall, c2011

IDENTIFICAÇÃO DA DISCIPLINA (06)

1. **Nome da Disciplina**: Estratégia e Inteligência Cibernética

2. **Carga Horária:** 32 horas/aula

3. **Ementa:** Jogos de Estratégia. Conceitos de Inteligência. Jogos de Inteligência. Conceitos de Criptografia. Aplicação das tecnologias de criptografia como solução de proteção de dados. Infraestrutura de Chaves públicas (ICP). Ciclo de vida e Ciclo de Uso de Certificados Digitais.

4. **Objetivo:** 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.

5. **Conteúdo Programático**: Conceitos de inteligência. Conceitos de jogos. Conceitos de estratégias. Criptografia. Tipos de algoritmos: simétricos e assimétricos. Método bloco versus stream. Criptografia de Transporte. Diferentes formas de criptografia. Algoritmos de criptografia. Algoritmos de Hash. Assinatura Digital. Criptografia de Chave Pública. Criptoanálise. Esteganografia. Vulnerabilidades nos algoritmos criptográficos. Ferramentas de criptografia. Conceitos de PKI. Ciclo de vida dos certificados. Ciclo de uso dos certificados. Ferramentas de criptografia: HSM, token, smartcard.

6. **Bibliografia:**

   a. **Básica:**

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, c2002

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

b. Complementar:

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, c2001

IDENTIFICAÇÃO DA DISCIPLINA (07)

1. **Nome da Disciplina**: Governança da Segurança Cibernética
2. **Carga Horária**: 32 horas/aula
3. **Ementa:** Normas ABNT NBR ISO/IEC 27001 e 27002. Família de Normas ISO/IEC 27000. Sistema de Gestão de Segurança da Informação. Estruturação de Security Officer. Estruturação de Políticas, Normas e Procedimentos. Auditoria de Segurança e Padrões de Conformidade.
4. **Objetivo:** Apresentar aos alunos a importância e as melhores práticas das normas de segurança, estruturação de uma área de segurança e preparação para as auditorias.
5. **Conteúdo Programático**: Criação de um Sistema de Gestão de Segurança da Informação com base na Norma ABNT NBR ISO/IEC 27001. Melhores práticas de gestão de segurança da informação com base na ABNT NBR ISO/IEC 27002. Preparação para certificação e auditoria de segurança da informação. Elaboração de Normas, Políticas e Procedimentos. Estruturação de área de segurança (Security Officer). Práticas de auditoria e conformidade da estrutura de políticas. Conformidade de Fornecedores. Relação entre os modelos de Governança de TI e Governança de Segurança da Informação.

6. Bibliografia:

a. Básica:

FERREIRA, Fernando Nicolau Freitas,. Segurança da informação. Rio de Janeiro: Ciência Moderna, c2008

DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de janeiro: Axcel Books do Brasil, c2000

MENEZES, Josué das Chagas. Gestão da segurança da informação. Leme: J. H. Mizuno, c2006

b. Complementar:

MENEZES, Josué das Chagas. Gestão da segurança da informação. Leme: J. H. Mizuno, c2006

ABNT NBR ISO/IEC 27001:2006 - Sistemas de gestão de segurança da informação

ABNT NBR ISO/IEC 27002:2005 - Código de pratica para a gestão da segurança da informação

ABNT NBR ISO/IEC 27003:2011 – Diretrizes para implantação de um sistema de gestão da segurança da informação

ABNT NBR ISO/IEC 27007:2012 - Diretrizes para auditoria de sistemas de gestão da segurança da informação

IDENTIFICAÇÃO DA DISCIPLINA (08)

1. **Nome da Disciplina**: Resposta a Incidentes de Segurança
2. **Carga Horária:** 32 horas/aula
3. **Ementa:** Processo de Resposta a Incidentes de Segurança da Informação. **Objetivo:** Preparar o aluno a responder incidentes de segurança cibernética.
4. **Conteúdo Programático**: Processo de resposta a incidentes de segurança. A criação de um CSIRT. Honey Pot e Honey Tokens. Procedimentos de respostas a incidentes. Montar sala de guerra.
5. **Bibliografia:**

   a. **Básica:**

ASSUNÇÃO, Marcos Flávio A. Honeypots e honeynets. Florianópolis: Visual Books, 2009

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

VAN WYK, Kenneth; FORNO, Richard;Incident Response, O¿Reilly Media, 2001

PROSISE, Chris; MANDIA, Kevin; PEPE, Matt;Incident Response and Computer Forensics, Second Edition, McGraw-Hill/Osborne, 2003. 2 ed.

WHITMAN, Michael E.; MATTORD, Herbert J;Principles of Incident Response and Disaster Recovery, Course Technology, 2006

   b. **Complementar:**

CALOYANNIDES, Michael A. Privacy protection and computer forensics. 2nd ed. Boston; London: Artech House, c2004

MANDIA, Kevin; PEPE, Matt; PROSISE, Chris. Incident Response and Computer Forensics. Osborne: McGraw-Hill, 2003.

WALLACE, Michael; WEBBER, Lawrence;The Disaster Recovery Handbook, AMACOM, 2004

SNEDAKER, Susan;Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress, 2007

IDENTIFICAÇÃO DA DISCIPLINA (09)

1. **Nome da Disciplina**: Ethical Hacker
2. **Carga Horária**: 32 horas/aula
3. **Ementa:** Esta disciplina 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.
4. **Objetivo**: Capacitar os alunos na prevenção da engenharia social na segurança e conhecimentos dos aspectos do comportamento humano.
5. **Conteúdo Programático:** 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. 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. Estabelece 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.

6. **Bibliografia**:

a. Básica:

MITNICK, K.; SIMON, W. The Art of Deception" Controlling the human element of security, Wiley Publishing Inc, 2013.

MARCELO, A.; PEREIRA, M. - A Arte de Hackear Pessoas, Ed.Brasport, 2005

PEIXOTO, MÁRIO CÉSAR P. - Engenharia Social e Segurança da Informação na Gestão Corporativa, Ed. Brasport, 2006.

b. Complementar:

SOUZA, Fernando de Jesus. Perícia e investigação de fraude. 3.ª ed. – Goiânia: AB, 2006.

FERREIRA, Fernando Nicolau Freitas,. Segurança da informação. Rio de Janeiro: Ciência Moderna, c2008.

FONTES, Edison. Vivendo a segurança da informação – Orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

IDENTIFICAÇÃO DA DISCIPLINA (10)

1. **Nome da Disciplina**: Computação Forense
2. **Carga Horária**: 32 horas/aula
3. **Ementa**: Computação Forense. Análise Forense. Ferramentas Forense
4. **Objetivo**: Apresentar aos alunos técnicas de computação forense. Metodologia e técnicas de análise forense computacional.
5. **Conteúdo Programático:** Técnicas de Investigação Tecnológica. Realizar análises forenses computacionais. Captura de informações biométricas. Conceitos de computação forense. Metodologias de análise forense. Conceitos de recuperação de arquivos apagados. Ferramentas para análise forense. Ata notarial. Elaboração de laudo pericial.
6. **Bibliografia**:

   a. **Básica:**

CASTELLA, Eduardo Marcelo. Investigação criminal e informática – inteligência artificial x boletim de ocorrência. Curitiba: Juruá, 2005.

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: teoria e prática aplicada – Como investigar e esclarecer ocorrências no mundo cibernético. São Paulo: Pearson Prentice Hall, 2007.

MELO, Sandro. Computação forense com software livre: conceitos, técnicas, ferramentas e estudos de casos. São Paulo: Alta Books, 2009

   b. **Complementar:**

CAMARGO Aranha Filho, Adalberto José Queiroz Telles de; "Crimes na Internet e a legislação vigente"; artigo publicado na Revista Literária de Direito, no 44, p. 23, outubro-dezembro/2002.

IDENTIFICAÇÃO DA DISCIPLINA (11)

1. **Nome da Disciplina**: Criminalística e Legislação
2. **Carga Horária**: 32 horas/aula

3. **Ementa**: Abordar a questão da Criminalística e toda a Legislação pertinente.

4. **Objetivo**: Apresentar aos alunos as leis que auxiliam a segurança cibernética.

5. **Conteúdo Programático:** Fundamentos do Direito Digital e desafios atuais. Criminalística computacional. Legislação Civil e Penal. Processo Pericial. Ética, Privacidade e Anonimato. Responsabilidade civil e dano moral no Direito Digital. Legislação brasileira e internacional aplicável. O direito digital.

6.**Bibliografia**:

a.Básica:

BLUM, Renato Opice; BRUNO, Marcos da Silva Gomes; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 2006.

b.Complementar:

CAMARGO Aranha Filho, Adalberto José Queiroz Telles de; "Crimes na Internet e a legislação vigente"; artigo publicado na Revista Literária de Direito, no 44, p. 23, outubro-dezembro/2002.

PINHEIRO, Patricia Peck. Direito Digital, 5ª ed. São Paulo, Saraiva, 2013.

Código Civil Brasileiro

Código Penal Brasileiro

IDENTIFICAÇÃO DA DISCIPLINA (12)

1. **Nome da Disciplina**: Empreendedorismo Cibernético

2. **Carga Horária**: 32 horas/aula

3. **Ementa:** Esta disciplina aborda aspectos sociais, econômicos, legais e profissionais da segurança da informação. Aspectos do Mercado de trabalho do profissional de segurança. Terceirização. Responsabilidade Social. Sustentabilidade para garantia de preservação do meio ambiente para que futuras gerações possam usufruir de todos os recursos disponíveis hoje.

4. **Objetivo**: Capacitar os alunos para atuar nas diferentes frentes profissionais da segurança no mercado de trabalho e empreendedorismo na profissão.

5. **Conteúdo Programático:** Legislação Trabalhista. Empreendedorismo. Startups. Empresas de Garagem. Institutos de Pesquisa. Comportamento no ambiente Corporativo. Negociação. Certificações. Prestação de Serviço. Pesquisas. Blogs, sites pessoais e fóruns de discussão. Sustentabilidade.

6. **Bibliografia**:

a. **Básica:**

BLUM, Renato Opice; BRUNO, Marcos da Silva Gomes; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 2006.

MITNICK, K.; SIMON, W. The Art of Deception" Controlling the human element of security, Wiley Publishing Inc, 2013.

MARCELO, A.; PEREIRA, M. - A Arte de Hackear Pessoas, Ed.Brasport, 2005

PEIXOTO, MÁRIO CÉSAR P. - Engenharia Social e Segurança da Informação na Gestão Corporativa, Ed. Brasport, 2006.

b. Complementar:

SOUZA, Fernando de Jesus. Perícia e investigação de fraude. 3.ª ed. – Goiânia: AB, 2006.

FERREIRA, Fernando Nicolau Freitas,. Segurança da informação. Rio de Janeiro: Ciência Moderna, c2008.

FONTES, Edison. Vivendo a segurança da informação – Orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

IDENTIFICAÇÃO DA DISCIPLINA (13)

1. Componente Curricular: **Aplicação de Conhecimento**
2. Carga Horária: **48 horas/aula** na modalidade EAD
3. Ementa: A disciplina promove o desenvolvimento do Trabalho de Aplicação de Conhecimento, com base no método prático e aplicado, o qual direciona o aluno para a resolução de um desafio ou problema real vivenciado em um contexto institucional/pessoal, utilizando os conceitos e práticas abordados ao longo do curso.
4. Objetivo: Capacitar o participante para investigar, analisar e compreender as causas e as implicações dos desafios em um contexto institucional/pessoal;

e com base no diagnóstico e na pesquisa bibliográfica, propor soluções e ações detalhadas, visando à resolução de problemas ou oportunidades reais e pontuais enfrentadas nesse contexto institucional/pessoal.

5. Conteúdo Programático:

- Definição do problema/oportunidade/desafio a ser resolvido;
- Descrição das características gerais do contexto institucional/pessoal;
- Diagnóstico das origens e implicações do desafio a ser resolvido;
- Pesquisa bibliográfica sobre os temas relacionados com o desafio do contexto institucional/pessoal;
- Proposição de soluções e ações detalhadas para a resolução do desafio.

.

Bibliografia Básica:

MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597010770.

MARCONI, Marina de Andrade. **Técnicas de pesquisa.** 8. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597013535.

YIN, Robert K. **Estudo de caso :** planejamento e métodos. 5. Porto Alegre Bookman 2015 1 recurso online ISBN 9788582602324.

GIL, Antonio Carlos. **Estudo de caso :** fundamentação científica ; subsídios para coleta e análise de dados ; como redigir o relatório. São Paulo Atlas 2009 1 recurso online ISBN 9788522464753.

Bibliografia Complementar:

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. Rio de Janeiro Atlas 2017 1 recurso online ISBN 9788597012934.

FLICK, Uwe. **Introdução à pesquisa qualitativa.** 3. Porto Alegre ArtMed 2008 1 recurso online ISBN 9788536318523.

MATTAR, João. **Metodologia científica na era digital.** 4. São Paulo Saraiva 2017 1 recurso online ISBN 9788547220334.

FACHIN, Odília. **Fundamentos de metodologia.** 6. São Paulo Saraiva 2017 1 recurso online ISBN 9788502636552.

SILVA, Anielson Barbosa da. **Pesquisa qualitativa em estudos organizacionais :** pradigmas, estratégias e métodos. 2. São Paulo Saraiva 2011 1 recurso online ISBN 9788502125018.

THIOLLENT, Michel. **Metodologia da pesquisa-ação.** 10. ed. São Paulo: Cortez, 2000. 108 p. ISBN 8524900296

SEVERINO, Antonio Joaquim. **Metodologia do trabalho científico.** 24. ed. rev. e atual. São Paulo: Cortez, 2017. 317 p. ISBN 9788524924484.

Campus Higienópolis: Rua da Consolação, 896 – Edifício João Calvino - térreo ● Consolação ● São Paulo - SP ● CEP 01302-907
Tel. (11) 2114-8820 ● www.mackenzie.br ● **ccec.atendimento@mackenzie.br**