PLANO DE ENSINO

Projeto: 1° SEMESTRE 2022

Disciplina: Segurança e Auditoria de Sistemas

Carga Horária: 70 horas

Ementa:

Conceitos de segurança da informação. Ataques em segurança da Informação. Medidas de segurança físicas, tecnológicas e não tecnológicas. Segurança de redes de computadores, redes sem fio e em nuvem. Criptografia. Noções de auditoria, metodologia e técnicas de auditoria.

Objetivos:

Geral: Capacitar o aluno com instrumentos que ajudem a garantir a segurança da Informação em sua organização, por meio da compreensão de conceitos básicos de ativos, riscos, vulnerabilidades e ameaças, complementados por ferramentas que atuem nas esferas lógicas, físicas, ambientais e culturais da organização.

Especificos:

1.Orientar sobre a importância da informação no meio pessoal e profissional.

2. Identificar os conceitos e princípios de segurança da informação, as principais vulnerabilidades dos sistemas computacionais.

3. Orientar na criação das políticas de segurança e auditoria.

Conteúdo Programático:

Unidade 1 - Segurança da Informação e Redes

Seção 1 - Introdução à segurança da informação

Princípios de Segurança da Informação - Confidencialidade, Integridade, Disponibilidade, Vulnerabilidade, Ameaça e Exploit

Elementos a Serem Protegidos: Pessoas, Informação e Ativos. Gerenciamento de contas e senhas

Mecanismos de Defesa: Processos, Tecnologia, Prevenção

Riscos em segurança da informação

Identificação de fatores de risco (Ameaças não tecnológicas: desastres, falhas, terrorismo)

Seção 2 - Segurança de Redes

Vulnerabilidades de Rede: hardware, software, protocolos, aplicações

Ameaças e ataques à Rede: pessoas (hackers), malware, DoS, DDoS, ataque de força bruta, homem do meio

Proteção à Rede (Firewall, IPS, Antimalware)

Ferramentas de proteção das informações: Tokens, Biometria, Filtros de Conteúdo.

Seção 3 -Criptografia

Introdução, Conceitos, Criptografia ao longo da História

Principais técnicas : chave privada, chave pública, esteganografia

Soluções de Chave Pública: Diffie-Hellman, RSA, assinatura digital, key-escrow

Aplicações de Criptografia: cartões de banco, tunelamento VPN, SSL, HTTPS

Unidade 2 - Política e Cultura de segurança

Seção 1 - Gestão e Políticas de segurança

Conceitos de Políticas de segurança.

Normas para a segurança da informação.

Família ISO 27.000 e LGPD. ISO 27.001 e 27.002

Tecnologias para segurança da informação

Seção 2 - Cultura de Segurança

Gerenciamento e aspectos operacionais da segurança de sistemas (éticos e legais).

Ambiente de desenvolvimento seguro.

Termos de ciência e contratos de confidencialidade.

Tendências e futuro em segurança da informação (Tecnologias Emergentes e Ameaças Emergentes)

Seção 3 -Armazenamento de Dados
Navegação em dados criptografados
Mascaramento e gestão de acesso de dados
Anonimização de dados, classificação, retenção e destruição da informação (ciclo de vida dos dados/tratamento de dados).
Confiabilidade de segurança de dados em cloud

Unidade 3 - Segurança na internet, dispositivos móveis e testes de intrusão
Seção 1 -Segurança na internet
Segurança em transações Web
Golpes na internet
Uso seguro de internet
Privacidade na Web
Seção 2 -Proteção para Dispositivos Móveis
Ameaças e segurança em dispositivos móveis.
Ataques e defesas em dispositivos móveis
Ataques de camadas de aplicações e antivírus para dispositivos móveis
Engenharia social (acesso as informações pessoais) de dispositivos móveis
Seção 3 -Análise de vulnerabilidade e Pentest
Análise de vulnerabilidade
Definição de Pentest
Metodologias de Pentest
Blackbox vs. Whitebox

Unidade 4 - Auditoria de Sistemas e Segurança
Seção 1 -Fundamentos de Auditoria de Sistemas
Introdução à auditoria e auditoria de sistemas: conceitos, princípios.
O papel do auditor de sistemas
As fases do processo de auditoria de Sistema de Informação.
Técnicas de auditoria de TI
Seção 2 - Controles gerais de auditoria de sistemas
Controles organizacionais, relacionados a segurança, continuidade do serviço
Controles de software de sistema, controles de acesso, controles de desenvolvimento e alteração de softwares aplicativos
Controles lógicos
Controles físicos
Seção 3 -Técnicas e Ferramentas para auditoria de sistemas
Introdução às técnicas e tipos de ferramentas para auditoria de sistemas.
Principais técnicas e ferramentas para auditoria de sistemas.
Aplicabilidade das técnicas e ferramentas para auditoria de sistemas.
Cases de auditoria em sistemas de informação.

Procedimentos Metodológicos:

O processo de ensino e aprendizagem é conduzido por meio da aplicação do conceito de Aula Invertida, que integra diferentes momentos didáticos, promovendo a revisão dos conteúdos, o diagnóstico do aproveitamento e o aprofundamento da compreensão dos conceitos trabalhados, por meio de proposições via conteúdo web, livro didático, fóruns de discussão, objetos de aprendizagem, textos ou outros recursos que o professor julgar relevantes. Um destes momentos é a Aula mediada, em que são desenvolvidas atividades relacionadas com situações-problema do cotidiano profissional, permitindo e estimulando trocas de experiências e conhecimentos. Nessa jornada acadêmica o aluno é desafiado à realização de atividades que o auxiliam a fixar, correlacionar e sistematizar os conteúdos da disciplina por meio de avaliações virtuais. A metodologia adotada, em consonância com o modelo acadêmico, viabiliza ações para favorecer

o processo de ensino e aprendizagem de modo a desenvolver as competências e habilidades necessárias para a formação profissional de seus alunos.

Sistema de Avaliação:

O sistema de avaliação adotado nos cursos de graduação, ofertados na modalidade EaD, visa avaliar o desempenho e desenvolvimento das competências necessárias, sendo composto por:

I. Prova por disciplina, aplicada presencialmente, com valor de 5000 pontos na média final da disciplina. As Provas presenciais são realizadas individualmente.

II. Avaliações Virtuais – Avaliações realizadas no decorrer do semestre, no Ambiente Virtual de Aprendizagem – AVA – COLABORAR, correspondendo a 1500 pontos na média final da disciplina.

III. Produção Textual Interdisciplinar – Atividade realizada ao longo do semestre. A elaboração da Produção Textual corresponde a 2000 pontos na média final da disciplina.

IV – Fórum de Discussões – Atividade que se destina a interação dos estudantes, sendo desenvolvida no Ambiente Virtual de Aprendizagem – AVA – COLABORAR, correspondendo a 1000 pontos na média final da disciplina.

V - Desafio Nota Máxima (DNM) - plataforma de ensino adaptativo disponibilizado aos estudantes em todos os semestres dos cursos, correspondente a 2000 pontos na média final da disciplina.

VI – Engajamento – Corresponde a pontuação atribuída para realização de atividades no Ambiente Virtual de Aprendizagem – AVA – COLABORAR, sendo elas: Pré aula; Assistir/Rever Tele aula; Pós aula; Estudo do Conteúdo Web; Avaliações Virtuais e; Fórum de Discussões, que corresponde a 3000 pontos na média final da disciplina.

VII - Frequência mínima de 50% em teleaulas e aulas-atividades.

VIII - Frequência mínima de 75% em aulas práticas (quando se aplicar).

IX – Avaliação de Proficiência, aplicada presencialmente, com valor de 1000 pontos na média final da disciplina. A avaliação de proficiência presenciais são realizadas individualmente.

O detalhamento do Sistema de Avaliação deve ser acompanhado no Manual de Avaliação Continuada disponibilizado no AVA.

Bibliografia Básica

STALLINGS, Willian.Criptografia e Segurança de Redes: princípios e práticas - 4ª edição São Paulo: Editora Pearson Prentice Hall,2008. https://plataforma.bvirtual.com.br/Acervo/Publicacao/396

HINZBERGEN, Jule. Tradução Alan de Sá. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.São Paulo: Brasport,2018. https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044

KOLBE JUNIOR, Armando.Sistemas de segurança da informação na era do conhecimento. Curitiba:Intersaberes,2017. https://plataforma.bvirtual.com.br/Acervo/Publicacao/52012

International Journal of Communication Networks and Information Security ISSN: 2076-0930, 2073-607X. Computer & Data Security, Telecommunications. [ProQuest]

International Journal of Information and Network Security (IJINS) ISSN: 2089-3299. Computer & Data Security.[ProQuest]

Security and Communication Networks ISSN: 1939-0114, 1939-0122. Computer Science.[ProQuest]

Bibliografia Complementar

COACHMAN, Erica. Segurança da Informação. São Paulo: Pearson Education do Brasil,2010. https://plataforma.bvirtual.com.br/Acervo/Publicacao/1642

ALMEIDA, Carlos André Barbosa de. Tecnologias aplicadas à segurança: um guia prático. Curitiba : Intersaberes, 2018. https://plataforma.bvirtual.com.br/Acervo/Publicacao/179908

GALVÃO, Michele da Costa (org.)Fundamentos em Segurança da Informação. São Paulo:Pearson Education do Brasil, 2015. https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525

Information Security ISSN: 1096-8903. Computer & Data Security.[ProQuest]

IET Information Security ISSN: 1747-0722. Computer & Data Security. [ProQuest]

Security and Communication Networks ISSN: 1939-0114, 1939-0122. Computer Science.[ProQuest]
The Art of Error Correcting Coding By: Morelos-Zaragoza, Robert H. John Wiley & Sons Incorporated. ISBN: 978-0-471-49581-9, 978-0-470-84782-4, 978-0-470-85247-7, 978-1-280-55560-2. Computer Science. .[ProQuest]
Advanced Computing: An International Journal ISSN: 2229-726X, 2229-6727. Computer Programming.[.[ProQuest]
Anale. Seria Informatica / Annals. Computer Science Series ISSN: 1583-7165, 2065-7471. Computer Science.[ProQuest]
APC - Australian Personal Computer ISSN: 0725-4415. Computer Science. .[ProQuest]
Applied Computing and Informatics ISSN: 2210-8327. Computer Programming. .[ProQuest]