

PLANO DE ENSINO

Disciplina: GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Carga Horária: 24h

Implantação 2020.1 - Versão 03/02/2020

EMENTA

A disciplina aborda a Gestão dos Riscos, a vulnerabilidades, medidas de proteção, métodos e processos de trabalho relativos à Segurança da Informação em Redes e Sistemas, apresentando a visão geral sobre as normas de segurança da informação, seus padrões atuais e prospecção de novos padrões. Nesse contexto, a disciplina proporciona conhecimento sobre as Normas de Segurança ISO 27001; ISO 27002 e suas aplicações, bem como a diferenciação entre as normas ISO 27001, ISO 17799 e ISO 27002.

COMPETÊNCIAS

- I. ANALISAR E RESOLVER PROBLEMAS.
- II. ADMINISTRAÇÃO E GERENCIAMENTO - Gerenciar recursos, tempo e processos visando a tomada de decisão e otimização dos resultados.
- III. GESTÃO DE CRISE - Elaborar e implementar Planos de Gestão de Crise e Recuperação de Desastres.

OBJETIVOS DE APRENDIZAGEM

- Capacitar o estudante para gerir recursos visando a segurança de fluxos de informações, melhorando a qualidade e produtividade no banco de dados.
- Proporcionar conhecimentos que permitam desenvolver competências e habilidades para desenvolver projetos e implementar programas internos e externos de sistemas de informações gerenciais seguras, além de diagnosticar disfunções nesses sistemas.

METODOLOGIA

A metodologia utilizada é o *Case-Based Learning* (CBL) ou Aprendizagem Baseada em Casos, que proporciona aos estudantes uma oportunidade de analisar um caso prático, usando o conteúdo disponível na disciplina. A CBL é uma metodologia ativa que põe o aluno como protagonista do processo de aprendizagem, sendo apoiada pela abordagem do desenvolvimento de competências e habilidades da Taxonomia de Bloom.

Nessa metodologia, os estudantes buscam a solução de um problema interdisciplinar enquanto promovem a comunicação e colaboração entre pares e docentes. No esforço para a construção da resolução do caso, os estudantes aplicam ferramentas analíticas, articulam questões e refletem sobre experiências relevantes de seu cotidiano para tirar conclusões que podem relacionar-se a novas situações, podendo ser aplicadas a cenários do mercado de trabalho.

Para cada disciplina de pós-graduação, a metodologia CBL utilizada conta com o apoio de recursos didáticos essenciais, que fornecem suporte para que o caso apresentado seja resolvido. Esses recursos estão disponíveis no Ambiente Virtual de Aprendizagem (AVA).

Alguns recursos utilizados são:

1. **Apresentação do caso com dicas do professor:** Exposição de um problema real ou fictício que requer uma análise do aluno, podendo ser uma decisão fundamentada, plano, projeto, análise ou produto. Semanalmente, são fornecidas dicas para resolução do problema, a fim de reforçar pontos importantes e destravar o desenvolvimento da solução. Ao final da disciplina, é revelado o Desfecho do caso, com comentários do professor.
2. **Material Referencial:** Contém todo conteúdo didático com fundamentos, teorias, boas práticas, ferramentas e métodos específicos para a resolução do problema apresentado no caso. O estudante deverá consumir este material a fim de buscar insights e respostas para composição da solução do problema exposto.
3. **Webconferência:** Realizada a discussão do caso com o objetivo de provocar e engajar os alunos a gerar insights sobre possíveis soluções. Também tem o objetivo de acompanhar e motivar as entregas das atividades e tirar dúvidas.
4. **Café, bate-papo e networking:** fórum assíncrono que tem por objetivo estimular que os estudantes discutam o caso e compartilhem situações parecidas em seu contexto de trabalho, de forma assíncrona. O professor tem um papel ativo neste fórum.

PLANO DE ENSINO

5. **Atividades avaliativas:** são apresentadas duas atividades para entrega do estudante, em que devem refletir sobre a utilização dos conteúdos e ferramentas adquiridas para solução do caso apresentado.

AValiação

A **Metodologia de Avaliação** prevista nesta disciplina está em convergência com a **Metodologia Ativa**, também contemplada no Processo Educativo.

O **Processo Avaliativo** estará, desse modo, organizado em **duas grandes etapas**:

N1: A **N1** é centrada na resolução da situação-problema apresentada na disciplina. De acordo com o estudo de caso, roteiro, dicas e outros materiais disponibilizados, será requisitado ao discente que apresente uma possível solução em formato de texto dissertativo ou relatório para compor a **Atividade Avaliativa da N1**, que corresponderá a **60% da Média Final**.

N2: A **N2** é composta por uma **avaliação em forma de teste objetivo com dez questões, baseada em todo o conteúdo da disciplina**.

A nota obtida nesta **Avaliação** corresponderá a **40% da Média Final**.

NOTA N1				NOTA N2
ESTUDO DE CASO	ROTEIRO	WEBCONFERÊNCIA	DICAS DO PROFESSOR	CONTEÚDO TOTAL DA DISCIPLINA
ATIVIDADE DISSERTATIVA N1				ATIVIDADE OBJETIVA N2

A média final da disciplina é calculado: **(N1 * 0,6) + (N2 * 0,4) = média final** (6,0 mínimo para aprovação).

BIBLIOGRAFIA

BÁSICA	BEAL, A. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações - 1. ed. - 2. reimpr. - São Paulo: Atlas, 2008. Disponível em Minha Biblioteca. JOÃO, B.[organizador] Sistemas computacionais . Biblioteca Universitária Pearson. - São Paulo: Pearson Education do Brasil, 2014. Disponível em Biblioteca Virtual Pearson. LAUDON, K. L.; AUDON, J. Sistemas de Informação Gerenciais - 9ª Ed.- São Paulo: Pearson Prentice Hall, 2010. Disponível em Biblioteca Virtual Pearson.
COMPLEMENTAR	LIMA, P. F. Crimes de computador e segurança computacional , 2ª edição. Atlas, 2011. MCCLURE, S., SCAMBRAY, J., KURTZ, G. Hackers Expostos: Segredos e Soluções para a Segurança de Redes , 7th edição. Bookman, 2014. SANTOS, V. O. dos. Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008 / Valdeci Otacílio dos Santos . --Campinas, SP: [s.n.], 2012.
	STALLINGS, W. Criptografia e segurança de redes: princípios e práticas . 6. edição - São Paulo: Pearson, 2015. WRIGHTSON, T. Segurança de Redes Sem Fio: Guia do Iniciante , 1st edição. Bookman, 2014.