MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ

SETOR DE CIÊNCIAS SOCIAIS APLICADAS

Departamento de Ciência e Gestão da Informação

Ficha 2 (variável)

Disciplina: **Segurança da Informação - Turma A**	Código: **SIN188**
Professor Responsável: **Luiz Rogério Lopes Silva**	Período de oferta: **20/03 a 07/07/23**

Natureza: (**X**) Obrigatória ( ) Optativa	(**X**) Semestral ( ) Anual ( ) Modular Vagas: **45**

Pré-requisito: **Não há**	Co-requisito: **Não há**	Modalidade: (X) Totalmente Presencial ( ) Totalmente EAD ( ) Parcialmente EAD: _____ *CH

CH Total: **45** CH Semanal: **3** Prática como Componente Curricular (PCC): Atividade Curricular de Extensão (ACE):	Padrão (PD): **45**	Laboratório (LB):	Campo (CP): **0**	Estágio (ES): **0**	Orientada (OR):**0**	Prática Específica (PE): **0**	Estágio de Formação Pedagógica (EFP): **0**

Aulas às quintas-feiras das 09:30 às 12h30.

Período do exame final: de 03 a 08/07/2023

Feriados e outras datas previstas (conforme PORTARIA ME No 11.090, DE 27 DE DEZEMBRO DE 2022): 7 de abril, Paixão de Cristo (feriado nacional); 21 de abril, Tiradentes (feriado nacional); 1o de maio, Dia Mundial do Trabalho (feriado nacional); 8 de junho, Corpus Christi (ponto facultativo);

EMENTA

Segurança em ambiente de redes: vulnerabilidade da informação e dos recursos tecnológicos; princípios de criptografia e biometria sob a ótica das normas técnicas e padrões de segurança nacionais; planos de segurança, contingência e continuidade de negócios.

PROGRAMA

Módulo I:

- Introdução à Segurança da Informação

- Políticas, diretrizes e procedimentos em Segurança da Informação

Módulo II:

- Segurança de Infraestrutura;

- Segurança de TI;

Módulo III:

- Segurança Cibernética;

- Planos de Segurança

OBJETIVO GERAL

Compreender os riscos e vulnerabilidades das informações e recursos tecnológicos em ambientes de rede, sob a ótica das normas técnicas e padrões de segurança nacionais. Além disso, estimular o desenvolvimento de planos de segurança, contingência e continuidade de negócios eficazes, capazes de proteger os ativos de informação, mitigar riscos, garantir a conformidade legal e preservar a reputação e a continuidade das organizações em caso de incidentes de segurança.

OBJETIVO ESPECÍFICO

1. Identificar as vulnerabilidades de informações e recursos tecnológicos em ambientes de rede, utilizando as normas técnicas e padrões de segurança nacionais como referência.

2. Analisar e avaliar as ameaças e riscos à segurança da informação em redes de computadores, utilizando as melhores práticas e metodologias de análise de riscos.

3. Propor soluções e implementar medidas de segurança adequadas para proteger informações sensíveis em ambientes de rede, considerando as normas e padrões nacionais e internacionais de segurança da informação.

4. Compreender e aplicar os conceitos de segurança digital e operacional, por meio do desenvolvimento de habilidades para proteger os sistemas de informação contra ameaças cibernéticas e incidentes operacionais, bem como para identificar e tratar vulnerabilidades em processos, infraestrutura e recursos tecnológicos das organizações.

4. Promover a conscientização sobre segurança da informação em ambientes de rede, por meio da difusão de informações sobre as melhores práticas e medidas de proteção para usuários e gestores de sistemas de informação.

PROCEDIMENTOS DIDÁTICOS

1. **Modalidade e organização da disciplina:** A disciplina é ministrada na modalidade presencial e é dividida em módulos, de acordo com o Programa. As estratégias didáticas utilizadas incluem aulas expositivas, revisão bibliográfica, discussões em grupo, atividades de pesquisa, preparação de documentos e trabalhos individuais e coletivos em sala de aula.
2. **Ambiente Virtual de Aprendizagem (AVA):** No AVA Moodle, os alunos têm acesso a conteúdos sugeridos, como leitura de textos e visualizações de vídeos, e a atividades, como pesquisas de avaliação, questionários, glossários, tarefas, fóruns e outras. As instruções e o período ideal para a realização das atividades são disponibilizados na plataforma.
3. **Acompanhamento contínuo das atividades:** Durante o período de realização da disciplina, o professor acompanha continuamente as atividades dos alunos, orientando a correta execução das tarefas e oferecendo feedback sobre as ações desenvolvidas pelos estudantes no AVA.
4. **Estratégia de comunicação:** Todas as dúvidas devem ser postadas nos respectivos fóruns do AVA, para que o professor possa compartilhar as respostas com toda a turma. Em caso de questões individuais, será utilizado o sistema de comunicação de usuário do Moodle.
5. **Exemplos práticos e casos reais:** A disciplina utiliza exemplos práticos e casos reais para ilustrar situações em que as medidas de segurança da informação são necessárias, como fraudes eletrônicas, phishing, malware, entre outros. Isso ajuda os alunos a compreenderem melhor a importância e a aplicabilidade dos conceitos aprendidos em sala de aula.
6. **Exercícios práticos:** A aplicação de exercícios práticos tem como objetivo fixar os conceitos de segurança da informação, incluindo a criação de políticas de segurança, simulação de ataques, o desenvolvimento de planos de contingência, entre outros.
7. **Discussão de casos reais:** A discussão de casos reais de segurança da informação estimula a participação dos alunos e aprofunda o entendimento sobre os temas.
8. **Utilização de recursos audiovisuais:** A utilização de recursos audiovisuais, como vídeos e imagens, pode ajudar a tornar as aulas mais dinâmicas e atraentes, além de facilitar a compreensão dos conceitos abordados.
9. **Metodologia Ágora:** A metodologia Ágora é uma abordagem de ensino que se baseia na colaboração, na troca de experiências e na discussão de ideias entre os participantes. O objetivo é estimular a participação ativa dos alunos no processo de aprendizagem e incentivar a construção coletiva do conhecimento. O professor atua como facilitador do processo, proporcionando um ambiente propício para o debate e a reflexão, e os alunos assumem um papel ativo na construção do conhecimento, compartilhando suas experiências e conhecimentos prévios.
10. **Palestras e Feira de Gestão da Informação:** A disciplina prevê palestras sobre segurança da informação e a organização de uma Feira de Gestão da Informação, com abordagem também voltada para Segurança da Informação. O objetivo é compartilhar com a comunidade interna e externa as ameaças e vulnerabilidades.

FORMAS DE AVALIAÇÃO

A aprovação na disciplina ocorrerá conforme a Resolução n° 37/97-CEPE. Ela dependerá do resultado das avaliações realizadas ao longo do período letivo (atividades), segundo o plano de ensino e cronograma divulgado no início do semestre, sendo o resultado global expresso de zero a cem. Será aprovado por média a e o discente que alcançar, no total do período letivo, frequência mínima de 75% da carga horária inerente à disciplina e obtiver, no mínimo, grau numérico 70 de média aritmética no conjunto de provas e outras tarefas propostas. Discente que não obtiver a média prevista deverá prestar exame final, desde que alcance a frequência mínima exigida e média não inferior a 40. No exame final a aprovação na disciplina dependerá da obtenção de grau numérico igual ou superior a 50 na média aritmética entre o grau do exame final e a média do conjunto das avaliações realizadas.

O processo avaliativo consiste em quatro atividades. Cada atividade tem um peso específico e uma descrição detalhada é fornecida abaixo:

1. **Cursos online (20%):** Esta atividade envolve a conclusão de cursos online relacionados ao tema da disciplina. Os cursos serão selecionados pelo professor e o aluno deve apresentar o certificado de conclusão com nota igual ou superior a 7 (sete);

2. **Resenha de filme (10%):** Para esta atividade, os alunos serão solicitados a assistir a um filme relacionado ao tema da disciplina e escrever uma resenha crítica do filme. A resenha deve conter uma breve sinopse do filme, análise crítica e reflexões pessoais sobre o tema abordado. A pontuação será baseada na qualidade da resenha apresentada.

3. **Documentário sobre Engenharia Social (30%):** Esta atividade envolve a produção de um documentário curto sobre o tema de Engenharia Social. Os alunos trabalharão em grupos, e devem abordar questões relevantes relacionadas ao assunto, como o impacto na sociedade, conhecimento/desconhecimento da população e exemplos de casos famosos. A pontuação será baseada na qualidade do trabalho produzido, incluindo a criatividade, originalidade e relevância do conteúdo.

4. **Organização e participação na Feira de Gestão da Informação (40%):** A última atividade é uma participação ativa na Feira de Gestão da Informação. Os alunos devem trabalhar em equipe e organizar uma apresentação sobre um tema relacionado à disciplina. A apresentação pode ser em formato de pôster, apresentação oral ou outro formato aprovado pelo professor. A pontuação será baseada na qualidade da apresentação e na participação ativa na organização da feira.

Em resumo, o processo avaliativo descrito envolve uma variedade de atividades que testam a compreensão dos alunos sobre o tema da disciplina e sua capacidade de aplicar esse conhecimento em contextos práticos. Cada atividade é avaliada de forma diferente, com base em critérios específicos, para garantir uma avaliação justa e precisa do desempenho dos alunos.

Para mais detalhes sobre as datas previstas para as avaliações favor consultar o cronograma dentro do Guia Didático. Eventuais necessidades de ajustes nas datas, atividades e afins serão combinadas em acordo com a turma.

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

PINHEIRO, Patricia P. Segurança Digital - Proteção de Dados nas Empresas. [Digite o Local da Editora]: Grupo GEN, 2020. E-book. ISBN 9788597026405. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 23 fev. 2023.

BARRETO, Jeanine dos S.; ZANIN, Aline; MORAIS, Izabelly Soares de; VETTORAZZO, Adriana de S. Fundamentos de segurança da informação. [Digite o Local da Editora]: Grupo A, 2018. E-book. ISBN 9788595025875. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 23 fev. 2023.

AGRA, Andressa D.; BARBOZA, Fabrício Felipe M. Segurança de sistemas da informação. [Digite o Local da Editora]: Grupo A, 2019. E-book. ISBN 9788595027084. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595027084/. Acesso em: 23 fev. 2023.

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

KIM, David; SOLOMON, Michael G. Fundamentos de Segurança de Sistemas de Informação. [Digite o Local da Editora]: Grupo GEN, 2014. E-book. ISBN 9788521635284. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788521635284/. Acesso em: 23 fev. 2023.

BRANQUINHO, Thiago; Marcelo. Segurança Cibernética Industrial. [Digite o Local da Editora]: Editora Alta Books, 2021. E-book. ISBN 9786555204117. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555204117/. Acesso em: 23 fev. 2023.

MACHADO, Felipe Nery R. Segurança da informação - princípios e controle de ameaças - 1ª edição - 2014. [Digite o Local da Editora]: Editora Saraiva, 2014. E-book. ISBN 9788536531212. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536531212/. Acesso em: 23 fev. 2023.

ALENCAR, Gliner Dias et al. GOVERNANÇA, GESTÃO E MATURIDADE DA SEGURANÇA DA INFORMAÇÃO: UM MAPEAMENTO SISTEMÁTICO DO CENÁRIO NACIONAL. Revista de Sistemas e Computação-RSC, v. 8, n. 1, 2018.

KI-ARIES, Duncan; FAILY, Shamal. Persona-centred information security awareness. computers & security, v. 70, p. 663-674, 2017.