



MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ

SETOR DE CIÊNCIAS SOCIAIS APLICADAS

Coordenação do Curso de ou Departamento de Gestão da informação

Ficha 2 (variável)

Disciplina: Segurança da informação		Código: SIN-188					
Natureza: (X) Obrigatória () Optativa		(X) Semestral () Anual () Modular					
Pré-requisito: não tem		Co-requisito: não tem		Modalidade: () Presencial () Totalmente EAD (X) CH em EAD: 100%			
CH Total: 45							
CH Semanal: 8	Padrão (PD):	Laboratório (LB):	Campo (CP):	Estágio (ES):	Orientada (OR):	Prática Específica (PE):	Estágio de Formação Pedagógica (EFP):

JUSTIFICATIVA

Esta disciplina está sendo ofertada em modalidade 100%EAD, em regime especial, para que os alunos possam evoluir em sua formação devido às Resoluções de Trabalho Remoto e de Suspensão do Calendário.

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.

VAGAS

Para esta oferta serão oferecidas 70 vagas.

PROFESSORES RESPONSÁVEIS

Prof. José Simão de Paula Pinto

Pro. Newton Correia de Castilho Júnior

PROGRAMA

1. Pressupostos da segurança da informação.
2. Redes de computadores, internet e segurança.
3. Vulnerabilidades e ameaças.
4. Princípios de criptografia.
5. Biometria e privacidade.
6. Normas e padrões nacionais e internacionais.
7. Administração de segurança e governança.
8. Planos de segurança e contingência.
9. Negócios digitais e continuidade de negócios.

Datas dos encontros síncronos: 04/02/2021 e 17/03/2021. Horário: 13:30-15:30.

Início da disciplina: 04/02/2021

Término da disciplina: 24/03/2021

Prova final: 24/03/2021

Todas as atividades listadas a seguir são para entrega assíncrona. A média das notas das atividades de 1 a 4 correspondem à primeira nota da disciplina. As datas limite para entrega são:

1. Responder as questões do AVA relativas a conceitos de segurança, redes e criptografia - até dia 12/02/2021.
2. Responder as questões do AVA relativas a falhas e vulnerabilidades - até dia 19/02/2021
3. Responder as questões do AVA relativas às NBR de segurança da informação - até dia 26/02/2021
4. Postar vídeo no AVA relativo à cartilha de segurança da informação - até dia 12/03/2021.
5. Entregar o plano de segurança e continuidade de negócios - esta atividade corresponde à segunda nota da disciplina e deve ser postada até dia 17/03/2021.

OBJETIVO GERAL

Compreender a importância da gestão da segurança da informação nas organizações.

OBJETIVOS ESPECÍFICOS

Reconhecer os quesitos de segurança da informação.

Compreender aspectos de redes de computadores e suas vulnerabilidades.

Avaliar o impacto de falhas de segurança da informação em negócios digitais.

Planejar processos de melhoria da segurança da informação e continuidade de negócios.

PROCEDIMENTOS DIDÁTICOS

Estudo em ambiente virtual voltados a questões teóricas da governança de TI.

Pesquisas e/ ou resumos críticos postados no ambiente virtual de aprendizagem.

Sistema de comunicação: mensagens e fórum permanente da disciplina disponível no AVA (ufprvirtual).

Tutoria: por meio de mensagens no AVA. O próprio professor atua como tutor, em horários dentro do período previsto de atividades e assincronamente;

Material didático: bibliografia indicada na disciplina e sugerida para cada atividade, além do material de aulas (cópias de transparências, exercícios, links para sites eletrônicos e artigos) disponibilizados no AVA;

Infraestrutura: AVA da UFPR;

Ambientação: o curso de Gestão da Informação prevê a ambientação de seus estudantes no AVA durante o 1º ano, 1º período, na semana do calouro. Para a visão inicial da educação a distância existe o curso Ambientação: <https://ufprvirtual.ufpr.br/course/view.php?id=9724>. Caso persistam dúvidas sobre a utilização da plataforma, recomenda-se visualizar 'Conheça a UFPR Virtual': <http://www.cipead.ufpr.br/portal1/index.php/cipead/saberesonline/ufpr-virtual/> Os tutoriais podem ser acessados em: <https://ufprvirtual.ufpr.br/course/view.php?id=8737>.

Controle de frequência: a frequência será avaliada pela entrega das atividades propostas até a data limite planejada.

Suporte técnico: Suporte técnico ao AVA UFPR Virtual é oferecido pela Coordenação de Integração de Políticas de Educação a Distância (CIPEAD/PROGRAD). Eventuais problemas no Moodle deverão ser comunicados sempre que verificados ao professor da disciplina, mais informações para contato em: <https://ufprvirtual.ufpr.br/course/view.php?id=8742>.

FORMAS DE AVALIAÇÃO

Frequência obrigatória em 75% das atividades propostas - entrega. A presença será computada a partir da entrega das atividades propostas no período previsto para cada uma delas. Não entregar a atividade até a data limite corresponderá à aplicação de faltas nas aulas correspondentes àquela semana letiva.

NOTA 1 - média aritmética das atividades realizadas ao longo da disciplina.

NOTA 2 – vídeo entregue no AVA relativo ao conteúdo da disciplina.

MÉDIA DA DISCIPLINA: média aritmética das duas notas [(Nota 1 + Nota 2) / 2].

Observação: somente as atividades assíncronas serão avaliadas! Constatado plágio não será considerada nota e/ ou frequência para a atividade. Questões no moodle terão autocorreção. Opiniões dos alunos serão consideradas desde que postadas no prazo e coerentes à questão proposta. Questões objetivas serão avaliadas automaticamente pelo sistema. As questões objetivas serão avaliadas segundo os seguintes critérios: 1- a resposta atende ao questionado, 20 pontos; 2 - o aluno expressou sua opinião, 80 pontos.

Os capítulos necessários ao acompanhamento estarão no AVA, assim como links para conteúdos e vídeos. Livros da Escola Superior de Redes estão disponíveis em: [https://pt.scribd.com/user/30482015/Escola-Superior-de-Redes?tab=collections](https://pt.scribd.com/user/30482015/Escola-Superior-de-Redes?tab=collections*)

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

BARROS, Fábio Gomes. **Elaboração de PDTI**. Rio de Janeiro : Escola Superior de Redes, 2014.

COELHO, Flávia Estéla Silva; ARAÚJO, Luiz Geraldo Segadas de. **Gestão da segurança da informação**. NBR 27001 e 27002. Rio de Janeiro : Escola Superior de Redes, 2013.

RNP. Escola Superior de Redes. **Introdução a infraestrutura de chaves públicas e aplicações**. Rio de Janeiro : Escola Superior de Redes, 2010.

ISACA. **Modelo corporativo para governança e gestão de TI da organização**. COBIT 5.0. Rolling Meadows : ISACA, 2012. Disponível em: <http://www.cefet-rj.br/attachments/article/2870/Cobit_5_pt-br.pdf>. Acessado em: 06/10/2020.

Maximiano, Antonio Cesar Amaru. **Introdução à administração**. 5. ed. rev. e ampl. São Paulo : Atlas, 2000. Disponível em: <https://docente.ifrn.edu.br/paulogomes/disciplinas/conteudos-1-bimestre/introducao-a-administracao-antonio-cesar-amaru-maximiano-5-edicao/at_download/file>. Acessado em: 06/10/2020.

RHEE, Man Young. **Internet security. Cryptographic principles, algorithmis and protocols**. John Willey & Sons : West Sussex, England, 2003.

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética**. À luz do marco civil da internet. São Paulo: Brasport, 2016.

BEZERRA, Edson Kowask. **Gestão de riscos de TI**. NBR 27005. Rio de Janeiro : Escola Superior de Redes, 2013.

CERT.br. **Cartilha de Segurança para Internet**. Versão 4.0. Comitê Gestor da Internet no Brasil : São Paulo, 2012. Disponível em: <<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>>. Acessado em: 06/10/2020.

CESTARI FILHO, Felício. **ITIL. Information Technology Infrastructure Library**. Rio de Janeiro : Escola Superior de Redes, 2012.

FONTE, Edison Luiz Gonçalves. **Políticas de segurança da informação**. Rio de Janeiro : Escola Superior de Redes, 2015.

STALLINGS, Willian. **Criptografia e segurança de redes**. Princípios e práticas. 6.ed. São Paulo: Pearson, 2015.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5.ed. São Paulo : Pearson, 2011.

VENERE, Guilherme. **Engenharia reversa de código malicioso**. Rio de Janeiro : Escola Superior de Redes, 2013. Disponível em: <<http://documents.scribd.com/s3.amazonaws.com/docs/7861nr4ry82pyp3l.pdf>>. Acessado em: 06/10/2020.

**OBS: ao assinalar a opção CH em EAD, indicar a carga horária que será à distância.*



Documento assinado eletronicamente por **JOSE SIMAO DE PAULA PINTO, PROFESSOR DO MAGISTERIO SUPERIOR**, em 14/10/2020, às 15:10, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **NEWTON CORREA DE CASTILHO JUNIOR, PROFESSOR DO MAGISTERIO SUPERIOR**, em 15/10/2020, às 15:52, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **JOSE MARCELO ALMEIDA PRADO CESTARI, CHEFE DO DEPARTAMENTO DE CIENCIA E GESTAO DA INFORMACAO - SA**, em 15/10/2020, às 16:07, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **DENISE FUKUMI TSUNODA, PROFESSOR DO MAGISTERIO SUPERIOR**, em 16/10/2020, às 15:47, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida [aqui](#) informando o código verificador **2995388** e o código CRC **6184931A**.

Criado por [simao](#), versão 22 por [simao](#) em 14/10/2020 15:09:57.