UNIVERSIDADE FEDERAL DE OURO PRETO
DEPARTAMENTO DE COMPUTAÇÃO

PLANO DE ENSINO

Nome do Componente Curricular em português: Criptografia e Segurança de Sistemas **Nome do Componente Curricular em inglês:** Cryptography and Security Systems		**Código:** BCC423
Nome e sigla do departamento: Departamento de Computação (DECOM)		**Unidade acadêmica:** ICEB
Nome do docente: Carlos Frederico M. C. Cavalcanti		
Carga horária semestral: 60 horas	**Carga horária semanal teórica:** 4 horas/aula	**Carga horária semanal prática:** 0 horas/aula
Data de aprovação na assembleia departamental: 20/08/2021		

Ementa:

Segurança de redes, de sistemas, da informação e segurança cibernética; criptografia; assinaturas digitais, certificados digitais e certificados de atributos; segurança de redes; mídias criptográficas; identificadores biométricos; cibersegurança; impactos na sociedade contemporânea.

Conteúdo Programático:

- Introdução à segurança: Segurança da informação, segurança de redes, de sistemas, da informação e segurança cibernética.
- Criptografia simétrica e assimétrica
- Algoritmos criptográficos
- Assinaturas digitais: Certificados Digitais e o padrão PKI (ICP).
- ICP-Brasil e ICP-Edu
- Segurança de redes: monitoramento e invasão de redes
- Princípios de hacking
- Mídias Criptográficas e identificadores biométricos
- ISO27000
- ITIL e COBIT, dentro do contexto da segurança da informação
- Certificações IISP e outros
- Cibersegurança e impactos na sociedade contemporânea

Objetivos:

Apresentar ao aluno diversos aspectos teóricos e práticos da segurança de redes, de sistemas, da informação dentro de uma visão contemporânea. O curso tem o objetivo de formar o aluno com os fundamentos em segurança cibernética dando-lhe condições de prosseguir sua formação em uma das áreas da segurança, tanto em nível profissional quanto acadêmico. Este curso não tem foco o estudo exaustivo de algoritmos criptográficos, que serão vistos no curso, mas tem como foco dar uma visão sistêmica.

Metodologia:

Aulas expositivas sobre o conteúdo programático, síncronas (webconferências usando Google Meet) e assíncronas na forma de aulas ou estudos dirigidos podendo valor de recursos didáticos analógos ao usados em aulas presenciais. Atividades desenvolvidas na disciplina serão na forma de trabalho e estudos dirigidos assíncronos relacionados ao conteúdo da disciplina. A frequência será computada mediante a entrega das atividades, acesso ao material das aulas e o comparecimento às provas. Será reprovado por frequência 1) quem não entregar, no mínimo, 75% dos TPs. 2)o discente que não acessar 25% do conteúdo do material das aulas disponíveis no Moodle no prazo de uma semana depois de disponibilizado na plataforma. 3) o discente que não fizer mais de 75% do numero de provas aplicadas. Provas online síncronas serão realizadas no horário regular da disciplina. Os alunos receberão uma prova com questões referentes aos conteúdos estudados e deverão enviar as respostas no formato solicitado dentro do horário regular da disciplina podendo, a critério do professor, estender o horário.

Atividades avaliativas:

Atividades avaliativas serão divididas em Provas (P) síncronas com peso de 33% da nota e Atividades Práticas (TPs) com peso de 66% da nota. Haverá 3 (três) provas síncronas de 10 (dez) pontos cada (respondendo por 33% da nota) e 7 (sete) TPs (Trabalho Prático) valendo 10 (dez) pontos (respondendo por 66% da nota). Todos os TPs terão tolerância de 24 horas no prazo de entrega e, TPs apresentados neste período de tolerância, terão redução de 50% nota. Qualquer problema na entrega por conta de acesso à plataforma Moodle ou outro por problemas de infraestrutura (internet..) ou outro , deverá ser imediatamente informado ao professor por e-mail do mesmo e mensagem no moodle. podendo fazer uso de colega para informar o fatou sando o mesmo canal (moodle e/ou e-mail). O professor poderá alterar o numero TPs no decorrer do semestre em favorecimento à execução da disciplina preservando sempre a proporção de 33% de Provas e 66% de Trabalhos Práticos na composição das notas. Exame Especial: os alunos que tiverem pelo menos 75% de frequência (mínimo para aprovação) conforme metodologia acima apresentada e média inferior a seis poderão fazer o Exame Especial. O Exame Especial será uma prova única, síncrona, oral e individual, contendo toda a matéria do conteúdo programático. Será agendado um horário para cada aluno podendo ser, alternativamente, ser aplicado especial em formato não síncrono, à critério do professor

Cronograma:

Data	Criptografia Segurança Redes	Modalidade / Assíncrona	Trabalho (TP) / Prova (P)
21/09/2021	Introdução	S	
23/09/2021	Cripto Simétrica	A	
28/09/2021	Cripto Simétrica	S	TP1
30/09/2021	Cripto Simétrica	A	
05/10/2021	Cripto Simétrica	S	
07/10/2021	Cripto Simétrica	A	TP2
12/10/2021	Cripto Assimétrica	A	
14/10/2021	Cripto Assimétrica	A	
19/10/2021	Prova 1	S	TP3
21/10/2021	Modernas Estruturas de Cripto	A	
26/10/2021	Modernas Estruturas de Cripto	S	
28/10/2021	Modernas Estruturas de Cripto	A	TP4
02/11/2021	Modernas Estruturas de Cripto	A	
04/11/2021	Assinaturas, ICP	A	

09/11/2021	Assinaturas, ICP	S	TP5
11/11/2021	Assinaturas, ICP	A	
16/11/2021	Hacking	S	
18/11/2021	Hacking	A	
23/11/2021	Prova 2	S	P2
25/11/2021	Hacking	A	
30/11/2021	Midia Cripto	S	
02/12/2021	Iso 27000	A	TP6
07/12/2021	Certificações	S	
09/12/2021	Segurança de Redes	A	
14/12/2021	Prova 3	S	P3
16/12/2021	Segurança de Redes	A	
04/01/2022	Segurança de Redes	A	TP7
06/01/2021	Segurança de Redes	A	
11/01/2021	(sem atividade)		
13/01/2021	EXAME ESPECIAL	S	ESPECIAL
17/01/2021	Ultimo dia lançamento nota		

Bibliografia Básica:

- STALLINGS,Willian, Criptografia e Segurança de Redes, 6ª edição, Editora Person, 2013, Disponível em https://plataforma.bvirtual.com.br/Acervo/Publicacao/22446, último acesso 03/12/2020.

- ROUTO, Terada, Segurança de Dados, Criptografia em redes de computares 2ª. edição, editora Blucher, 2008, Disponível em https://integrada.minhabiblioteca.com.br/#/books/9788521215400

- MENEZES, Alfred, van OORSCHOT, Paul e VANSTONE, Scott, Handbook of Applied Cryptography, 1ª edição, CRC Press, 1996, disponível em http://cacr.uwaterloo.ca/hac/ Último acesso 04/12/2020

- GOLDREICH, Oded, Foundations of cryptography, Cambridge: Cambridge University Press, 2009. Documentos preliminares da obra pode ser encontrados em http://www.wisdom.weizmann.ac.il/~oded/foc.html Último acesso 04/12/2020

Bibliografia Complementar:

- FRAGA, Bruno e BANGLLER, Thompson, Técnicas de Invação, 2017, cybersewer.com, disponível em https://tcxsproject.com.br/dev/Biblioteca%20Livros%20Hacker%20Gorpo%20Orko/Livro-Tecnicas-De-Invasao.pdf . Último acesso em 04-12-2020

- BOMFATI Cláudio e KOBE Jr., Armando, Crimes Cibernéticos, Editora Intersaberes, 1ª edição, 2020,disponível em https://plataforma.bvirtual.com.br/Acervo/Publicacao/179734 Último acesso em 04-12-2020

- NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, disponível em https://bitcoin.org/bitcoin.pdf, ultimo acesso 06-12-2020

- MARTINS, Dheneb, Investigação cibernética, editora Contentus, 2020, disponível em https://plataforma.bvirtual.com.br/Acervo/Publicacao/184415 . Último acesso 04/12/2020

- HJÁLMARSSON, Friðrik, Blockchain-Based E-Voting System, 2018, IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151. Disponível em https://ieeexplore.ieee.org/abstract/document/8457919 . Último acesso 04/12/2020
- CARLOMAGNO, Marcelo e outros. Introdução a Infraestrutura de Chaves Públicas e Aplicações, Escola Superior de Redes RNP, 2010.