CAMPO: GERAL	**ÁREA DE CONCENTRAÇÃO:** PODER AEROESPACIAL E PENSAMENTO POLÍTICO-ESTRATÉGICO CONTEMPORÂNEO		
DISCIPLINA ELETIVA: FUNDAMENTOS DE SEGURANÇA E DEFESA CIBERNÉTICA	**CH AULA**: 40h	**CH AVALIAÇÃO**: 5h	**CH TOTAL**: 45h/3 créditos

OBJETIVOS ESPECÍFICOS:

a) Compreender os conceitos e processos de segurança e defesa cibernética na área de Defesa, com ênfase no Poder Aeroespacial (Cp);
b) Identificar as necessidades e recursos envolvidos na segurança e defesa cibernética (Cn);
c) Conhecer as principais técnicas envolvidas nos ataques e explorações cibernéticas e as formas eficazes de defesa. (Cn).

EMENTA:

Parte I – Marco Conceitual e Background Teórico:
- conceitos básicos: vulnerabilidades, ameaças, riscos e gestão de segurança;
- marcos regulatórios; e
- segurança em ambientes operacionais tradicionais: redes de computadores (LAN, Internet, Wireless), aplicativos convencionais, aplicações Web, sistemas operacionais, controle de acesso físico e lógico convencionais, criptografia e certificação digital.

Parte II – Gestão de Risco:
- gestão de ameaças e vulnerabilidades: técnicas e ferramentas disponíveis;
- avaliação qualitativa e quantitativa do risco; e
- métodos e técnicas para a redução de impacto no negócio.

Parte III – Resposta a Incidentes de Segurança:
- métodos e técnicas de ataques a segurança de sistemas em uso;
- prevenção e detecção de intrusos;
- continuidade de sistemas; e
- técnicas forenses.

Parte IV – Normatização e Avaliação de Segurança em Sistemas:
- política de segurança e normas associadas;
- auditoria de segurança;
- testes de penetração; e
- adoção de certificações de segurança.

Parte V – Novas Tecnologias e Segurança:
- Big Data;
- IoT, IoC e TTP;
- Cidades Inteligentes;
- Machine Learning; e
- Artificial Intelligence.

REFERÊNCIAS (BÁSICAS):

DAYA, Bhavya. Network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering. Disponível em: <http://askcypert.org/sites/default/files/Network%20Security.pdf>. Acesso em: 2 out. 2018.

FELLOW, Anil K. Jain,et al. Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security, Vol. 1, Nº 2. Jun. 2006.

HOEPERS, Cristine. STEDING-JESSEN, Klaus. Fundamentos de Segurança da Informação. Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 12 set. 2018.

HU, V.C., KUHN, D. R. e FERRAIOLO, D. F. Attribute-Based Access Control. IEEE Computer Society. Fev. 2015.

JUNIOR A. Ferreira de Souza, STREIT Rosalvo Ermes. Segurança cibernética: política brasileira e a experiência internacional. Disponível em:< https://revista.enap.gov.br/index.php/RSP/article/view/864>. Acesso em: 2 out. 2018.

MONALI S. Gaigole et al. The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms. International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, Maio 2015, pg. 728-735.

SOMTOCHUKWU Nnabuife Godfrey. The Significance and Future of Network Security. Cranfield University, UK. IJCST Vol. 8, Issue 1, Jan - March 2017. Disponível em: <http://www.ijcst.com/vol8/2/10-nnabuife-godfrey-somtochukwu.pdf. Acesso em: 2 out. 2018.

SVENDSEN Heidi. Security Risk Assessment in Software Development Projects. Norwegian University of Science and Technology. Disponível em:< https://brage.bibsys.no/xmlui/handle/11250/2454373. Acesso em: 2 out. 2018.

WALKER, Matt. Certified Ethical Hacker All-in-One - Exam Guide. McGraw-Hill. 2012. Disponível em: < https://www.pdfdrive.com/ceh-certified-ethical-hacker-all-in-one-exam-guide-e27060168.html>. Acesso em: 24 out. 2018.