Pós-graduação em "Segurança de Informação, Cibersegurança e Privacidade"

OBJETIVOS GERAIS E ENQUADRAMENTO:

A realidade atual e a sensibilidade para a importância da segurança de informação nas organizações nunca foi tão alta. Uma simples comparação do número de notícias relacionadas com o tema há 5 anos e hoje é elucidativo da relevância do tema e da tendência que está a seguir.

Com a introdução em maio de 2018 do Regulamento Geral de Proteção de Dados (RGPD), a privacidade dos dados ganhou uma importância considerável. O RGPD foi um catalisador e acelerador da procura de profissionais da área da segurança de informação/cibersegurança.

As empresas, em especial as de maior dimensão, já começaram a dar mais importância ao tema, sendo um dos exemplos empresas do sector automóvel, que agora começam a impor aos seus fornecedores regras relacionadas com a segurança de informação, algo que há poucos anos não era um requisito.

Esta necessidade de mais segurança e privacidade vai provocar que as organizações demonstrem competências e garantam a segurança de informação. Para tal, o cumprimento de normas relacionadas com a segurança de informação, como as da família ISO 27000 (a mais conhecida é a ISO 27001) são essenciais para atingir esse objetivo. Para tal necessitam de novas soluções, que permitam obter os objetivos de um modo mais rápido e coerente.

Com o surgimento do RGPD urge fazer uma integração entre ISO 27xxx e RGPD de modo a articular as soluções existentes e criar/adaptar o que ainda falta.

O aumento da utilização da IOT, de soluções móveis, da cloud, levanta a questão: Como é que se irão conseguir soluções arquiteturais com suporte à segurança de informação? A solução passa por utilizar as melhores práticas de desenvolvimento de software que permitam uma verdadeira transformação digital, que será obtida através da integração de sistemas, processos de negócio, gestão de identidades e acessos num contexto de segurança de informação.

É importante relembrar que estão em curso duas novas realidades: "Sociedade 5.0" e "Indústria 4.0", patentes por toda a sociedade, que encontram na segurança e privacidade, pilares fundamentais do desenvolvimento civilizacional estável e sustentado.

De modo a dar suporte à transformação digital que está a acontecer, é necessário que existam profissionais habilitados para aplicar as boas práticas e utilização de devops/secops, engenharia de software e inteligência artificial na criação de soluções arquiteturais seguras e respetiva integração dessas soluções.

Esta especialização pretende fornecer conhecimentos que abranjam todas as vertentes relacionadas com a segurança de informação. Para tal os alunos irão adquirir competências em:

- **Gestão de identidades e acessos (Ex: IAM, BYOI);**
- **Desenvolvimento de software seguro (OWASP / SANS TOP 25, Segurança no desenvolvimento de APIs);**

- **Segurança no desenvolvimento de aplicações para sistemas móveis - Android e IOS;**
- **Testes de Segurança e deteção de vulnerabilidades no Ciclo de Vida do Desenvolvimento de Software;**
- **Normas e boas práticas no desenvolvimento de software seguro (ISO 27034, IEEE 1012-2012);**
- **Sistemas de Gestão de Segurança de Informação num contexto de transformação digital (Automatização/digitalização dos processos de negócio associados à gestão de segurança de informação);**
- **Normas e Frameworks de Segurança de Informação: ISO 270xx(27001,27002... 27050), NIST);**
- **Integração de COBIT ou ITIL, ISO27001 e NIST, para potenciar a obtenção de soluções mais produtivas e seguras;**
- **Hacking Ético e Cibersegurança - Cibersegurança na Cloud, IOT, Normas e frameworks para a Cibersegurança (ISO/IEC 27032, 27017,27039, 27040, NIST, CIS Controls, Gestão de configurações para a gestão de testes de intrusão;**
- **Aplicação de inteligência artificial no suporte à cibersegurança;**
- **Gestão de Incidentes e Análise Forense Digital (Norma ISO 31000, Norma ISO 22301, Threat Intelligence);**
- **Gestão de Incidentes e Análise Forense Digital num contexto de aplicação de Inteligência Artificial;**
- **Segurança e Privacidade dos Dados (RGPD, Entidades, Normas e Frameworks: ENISA, CNCS - Centro Nacional de Cibersegurança, CNPD, PSD2, HIPAA, ISO 27799, ISO 29100, PCI DSS, Mapeamento entre ISO 27001 e RGPD).**

Os alunos vão adquirir nesta especialização conhecimentos sólidos, teóricos e práticos, para exercer uma atividade que já tem uma falta considerável de profissionais, sendo por isso muito valorizada e remunerada no mercado nacional e internacional.

Coordenador da pós-graduação: Orlando Sousa (oms@isep.ipp.pt)

Esta pós-graduação tem o seguinte planeamento para o ano letivo 2023-2024:

Ucs	PRCSE	SGSIN	SEPDD	HETCS	GIAFD	ADDSS	INACS	ASINF	SEPRJ
Total de Horas	30	30	30	30	30	30	30	30	60
07/11/2023	2	2							
09/11/2023	2	2							
10/11/2023	2	2							
14/11/2023	2	2							
16/11/2023	2	2							
17/11/2023	2	2							
21/11/2023	2	2							
23/11/2023	2	2							
24/11/2023									
28/11/2023	2	2							
30/11/2023	2	2							
01/12/2023									
05/12/2023	2	2							
07/12/2023	2	2							
08/12/2023									
12/12/2023	2	2							
14/12/2023	2	2							
15/12/2023									
19/12/2023	2								
21/12/2023		2							
22/12/2023									
26/12/2023									
28/12/2023									
29/12/2023									
02/01/2024									
04/01/2024			2	2					
05/01/2024			2	2					
09/01/2024			2	2					
11/01/2024			2	2					
12/01/2024			2	2					
16/01/2024			2	2					
18/01/2024			2	2					
19/01/2024			2	2					
23/01/2024			2	2					
25/01/2024			2	2					
26/01/2024									
30/01/2024			2	2					
01/02/2024			2	2					
02/02/2024									
06/02/2024			2	2					
08/02/2024			2	2					
09/02/2024									
13/02/2024									
15/02/2024			2						
16/02/2024				2					
20/02/2024					2	2			

22/02/2024					2	2			
23/02/2024					2	2			
27/02/2024					2	2			
29/02/2024					2	2			
01/03/2024					2	2			
05/03/2024					2	2			
07/03/2024					2	2			
08/03/2024									
12/03/2024					2	2			
14/03/2024					2	2			
15/03/2024									
19/03/2024					2	2			
21/03/2024					2	2			
22/03/2024									
26/03/2024									
28/03/2024									
29/03/2024									
02/04/2024					2	2			
04/04/2024					2	2			
05/04/2024									
09/04/2024					2				
11/04/2024						2			
12/04/2024									
16/04/2024							2	2	
18/04/2024							2	2	
19/04/2024									2
23/04/2024							2	2	0
25/04/2024									
26/04/2024							2	2	2
30/04/2024							2	2	0
02/05/2024							2	2	0
03/05/2024									2
07/05/2024									
09/05/2024									
10/05/2024									
14/05/2024							2	2	0
16/05/2024							2	2	0
17/05/2024									2
21/05/2024							2	2	2
23/05/2024							2	2	2
24/05/2024									2
28/05/2024							2	2	2
30/05/2024							2	2	2
31/05/2024									2
04/06/2024							2	2	
06/06/2024							2	2	
07/06/2024									4
11/06/2024								2	4
13/06/2024							2		4
14/06/2024									4
18/06/2024									4

20/06/2024									4
21/06/2024									4
25/06/2024									4
27/06/2024									4
28/06/2024									4

UNIDADE CURRICULAR : Arquitetura, Desenho e Desenvolvimento de Software Seguro - PGSICP-ADDSS

ENQUADRAMENTO: Informação e dados sob todas as formas são bens, e as pessoas são obrigadas a proteger os seus bens. A maioria destes bens são geridos por software e, por causa deles, o software está sujeito a numerosas formas de ataque para os roubar, danificar ou revelar. Esta UC aborda as questões de segurança do software e fornece métodos de programação para o desenvolvimento de software seguro.

CONHECIMENTOS PRÉVIOS ASSUMIDAMENTE ADQUIRIDOS: Assume-se que o aluno possui conhecimentos básicos de disciplinas de ciência e engenharia, como matemática e estatística e também competência geral em algoritmia, programação, sistemas operativos e redes de comunicação.

PROPÓSITOS E OBJETIVOS: Este curso aborda os fundamentos e técnicas para conceber e implementar sistemas de software seguros. Também cobre a avaliação de vulnerabilidades de segurança de software, exploração de vulnerabilidades de software, e métodos para proteger software vulnerável. No final da UC, o aluno deverá ter adquirido competências para:

C01. Classificar a segurança em sistemas de software vulneráveis.

CO2. Avaliar as ameaças, riscos e ataques à segurança dos sistemas de software .

CO3. Criar métodos para proteger software vulnerável.

CO4. Desenvolver software seguro.

PROGRAMA

P1- Fundamentos e princípios de segurança em software (~15%)

P2-Modelação e mitigação de ameaças (~15%)

P3-Padõres para desenvolvimento de software seguro (~15%)

P4-Práticas de programação de software seguro (~15%)

P5-Desenho de software seguro (~20%)

P6-Ciclo de vida do processo de desenvolvimento de software seguro (~20%)

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE:

Apresentações e leituras recomendadas (essencialmente artigos de investigação) disponibilizados no website da UC.

Livros:

- "Designing Secure Software: A Guide for Developers",Loren Kohnfelder, No Starch Press, 2021

- "Building Secure & Reliable Systems, Best Practices for Designing, Implementing and Maintaining Systems", Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea, and Adam Stubblefield, O?Reilly Media, Inc., 2020.

- "Secure by Design",Daniel Deogun, Dan Bergh Johnsson, Daniel Sawano, Manning Publications, 2019

- "Segurança no Software (2ª Edição Atualizada e Aumentada)", Miguel Pupo Correia, Paulo Jorge Sousa FCA, 2017.

Ferramentas:

- IntelliJ

- Bitbucket

MATERIAL DE ENSINO COMPLEMENTAR: https://owasp.org/

METODOLOGIA ENSINO-APRENDIZAGEM: As aulas expõem os alunos aos diversos conceitos. Técnicas de aprendizagem ativa e centradas no aluno serão empregues por forma a motivar os alunos em debates, discussão de casos de estudo e revisão crítica de sistemas/arquiteturas/mecanismos. Parte das aulas serão para a realização e apresentação dos trabalhos.

UNIDADE CURRICULAR: Auditoria da Segurança de Informação - PGSICP-ASINF

ENQUADRAMENTO: De modo que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais relacionadas com a auditoria da segurança de informação. Esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. É crucial entender a relevância das auditorias da segurança de informação num contexto de gestão de risco de modo a elaborar relatórios de auditoria.

CONHECIMENTOS PRÉVIOS ASSUMIDAMENTE ADQUIRIDOS: Proficiência no uso de computadores e tecnologias atuais (Internet, web, etc.) assim como de sistemas de gestão de segurança de informação

PROPÓSITOS E OBJETIVOS:

P1. Entender as principais etapas na elaboração de um plano de auditorias de segurança de informação

P2. Compreender e avaliar o risco de segurança de ativos

P3. Perceber e avaliar as necessidades relativas a testes de intrusão, perante auditorias de segurança

P4. Reconhecer a importância da utilização de ferramentas de deteção de vulnerabilidades

P5. Implementar soluções que permitam a automatização dos processos relacionados com a auditoria da segurança de informação

P6. Elaborar relatórios de segurança de informação, como consequência das auditorias efetuadas.

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar os principais passos na criação de um plano de auditorias de segurança de informação

C02 Avaliar, testar e verificar a viabilidade das soluções escolhidas para efetuar a auditorias de segurança de informação

C03 Implementar sistemas e soluções que permitam a automatização dos processos e reutilização dos dados de auditoria

C04 Desenvolver e aplicar soluções de auditoria da segurança de informação com a capacidade de gerar relatórios para apresentação a responsáveis da gestão da organização.

PROGRAMA

- A importância da auditoria da segurança de informação numa organização

- Auditoria da gestão da segurança de informação

- O ciclo do Programa de auditorias

- Tecnologias de suporte às auditorias da segurança de informação

- Gestão de risco nas organizações

o Avaliação de risco de ativos

o Priorização

o Definição de âmbito

o Planeamento e execução de auditorias

o Identificação da necessidade de auditorias perante o plano definido

o Automatização de descoberta de vulnerabilidades

o Como comunicar findings

o Relatório de auditoria

o Gestão de vulnerabilidades e ferramentas adequadas

o NIST Guide for Conducting Risks Assessments

- Eventos de Segurança

- Gestão de vulnerabilidades no contexto de uma auditoria

- Deteção de vulnerabilidades na Web

- Deteção de vulnerabilidades em aplicações moveis

- Auditoria aos controlos de segurança ISO 27001

- Red Team no contexto de uma auditoria

- Auditoria de segurança na implementação de soluções de segurança

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle)

MATERIAL DE ENSINO COMPLEMENTAR

NIST.CSWP - Framework for Improving Critical Infrastructure Cybersecurity, 2018, https://doi.org/10.6028/NIST.CSWP.04162018

J. Vest, J. Tubberville, Red Development and Operations: A Practical Guide, 2020

A. Kohnke, D. Shoemaker, K.Sigler , The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit), 2022

C. Davis, M. Schiller, K. Wheeler, IT Auditing Using Controls to Protect Information Assets, Third Edition, 2019, ISBN: 1260453227

Angel R. Otero , Information Technology Control and Audit, Fifth Edition, 2019, ISBN: 9780367657154

M. Weiss, M. Solomon, Auditing IT Infrastructures for Compliance 2nd Edition, 2017, ISBN: 9781284143447

UNIDADE CURRICULAR: Gestão de Incidentes e Análise Forense Digital - PGSICP-GIAFD

ENQUADRAMENTO: De modo que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais relacionadas com a gestão de incidentes e análise forense digital. Esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. É crucial entender a relevância da análise forense digital num processo de gestão de incidentes e dominar a importância dos sistemas de monitorização numa infraestrutura.

PROPÓSITOS E OBJETIVOS:

P1. Entender e compreender o que é um incidente, o processo de estão de incidentes e os papéis e responsabilidades envolvidos na gestão de incidentes

P2. Compreender a relevância da Análise Forense Digital num processo de gestão de incidentes

P3. Perceber a importâncias dos sistemas de monitorização numa infraestrutura

P4. Reconhecer a importância da preparação da infraestrutura para permitir a deteção de incidentes e a reconstrução dos eventos associados a um incidente.

P5. Entender as principais metodologias utilizadas por grupos atacantes

P6. Compreender e saber aplicar o processo de gestão de incidentes em cenários de incidente realistas.

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar o que é um incidente, o processo de gestão de incidentes e os papéis e responsabilidades envolvidos na gestão de incidentes

C02 Avaliar, testar e verificar a viabilidade das soluções escolhidas para efetuar a Análise Forense Digital

C03 Implementar sistemas de monitorização na infraestrutura e prepará-la de modo que permita a deteção de incidentes e a reconstrução dos eventos associados a um incidente.

C04 Desenvolver e aplicar o processo de gestão de incidentes em cenários de incidente realistas.

PROGRAMA:

- Incidente - Definição e caracterização

o Exemplos de incidentes:

- Taxonomia Comum da Rede Nacional de CSIRT

- Como gerir eficazmente um incidente de cibersegurança numa organização

- Gestão de Incidentes de segurança de informação

- Triagem em dispositivos com Microsoft Windows

- Fase 1 da gestão de um incidente - Preparação

- CNCS - Roadmap para a criação de capacidades mínimas

- CNCS - Notificação de incidentes

- Fase 2 da gestão de um incidente - Identificação

- Fase 3 da gestão de um incidente - Contenção

- Fase 4 da gestão de um incidente - Erradicação

- Triagem de malware

o Utilização de ambientes de sandbox, segregados, sem acesso à Internet

o Ferramentas de análise estática e dinâmica

- Fase 5 da gestão de um incidente - Recuperação

- Fase 6 da gestão de um incidente - Lições Aprendidas

- SIEM - Security Information and Event Management

Casos de uso mais habituais

- Processos envolvidos na análise forense digital

- Guia da integração de técnicas forenses na resposta a incidentes

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE:

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle

MATERIAL DE ENSINO COMPLEMENTAR

Don Murdoch (2019), Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter

Jason T. Luttgens (2014), Incident Response & Computer Forensics, Third Edition (NETWORKING & COMM - OMG), McGraw-Hill Education, ISBN-13 : 978-0071798686

Scott J. Roberts (2017), Intelligence-Driven Incident Response: Outwitting the Adversary, O'Reilly Media, ISBN-13 : 978-1491934944

Gerard Johansen (2020), Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition, Packt Publishing,

Richard Bejtlich (2013), The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, ISBN-13 : 978-1593275099

NIST SP 800-61r2 ? Computer Security Incident Handling Guide - https://doi.org/10.6028/NIST.SP.800-61r2

ANSON (2020), Steve, Applied Incident Response, 1st Edition, Wiley, ISBN-13: 978-1119560265

CARVEY (2018), Harlan, Investigating Windows Systems, 1st Edition, Academic Press, ISBN-13: 978-0128114155

LIGH, Michael, CASE, Andrew (2014), The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 1st Edition, Wiley, ISBN-13: 978-1118825099

Greg Gogolin, Digital Forensics Explained, CRC Press, ISBN-13: 978-0367502812

Bruce Nikkel (2021), Practical Linux Forensics: A Guide for Digital Investigators, No Starch Press, ISBN-13: 978-1718501966

UNIDADE CURRICULAR: Hacking Ético e Cibersegurança - PGSICP-HETCS

ENQUADRAMENTO: De modo que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais relacionadas com o hacking ético num contexto de cibersegurança. Esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. Para tal, é necessário perceber as várias estratégias e ferramentas de hacking assim como a sua utilização num contexto de deteção de falhas de segurança num sistema.

PROPÓSITOS E OBJETIVOS

P1. Entender e compreender a importância do Hacking Ético nas organizações.

P2. Compreender as metodologias de ataque num contexto de cibersegurança.

P3. Perceber os conceitos da framework OSINT

P4. Conhecer o ciclo de vida do hacking ético

P5. Entender a deteção de vulnerabilidades em vários tipos de sistemas

P6. Compreender e saber aplicar a deteção de anomalias

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar os pontos chave relacionados com o hacking ético nas organizações

C02 Avaliar, testar e verificar a viabilidade das soluções escolhidas

C03 Criar métodos para melhorar a implementação e automatização da deteção de vulnerabilidades

C04 Desenvolver e implementar soluções de deteção de vulnerabilidades numa organização

PROGRAMA

- Motivação para a utilização de Hacking Ético nas organizações.
- A lei portuguesa do cibercrime
- Tipos de compromisso em equipas de ataque
- Metodologias de ataque
- Tipos de ataque habituais
- O ciclo de vida do Hacking Ético
- A framework OSINT.
- Ferramentas de deteção de Vulnerabilidades
- Automatização da deteção de vulnerabilidades
- Segurança na Cloud

- Segurança nos dispositivos IoT

- Técnicas de ataque a hardware

- Hacking de sistemas operativos

- Ataques a canais cifrados

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle)

MATERIAL DE ENSINO COMPLEMENTAR

MS. Harris, A. Harper, C. Eagle, J. Ness (2018), Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition, Daniel Regalado, McGraw Hill, ISBN-13 : 978-1260108415

P. Wylie, K. Crawley; (2020), The Pentester BluePrint: Starting a Career as an Ethical Hacker, Wiley, ISBN-13 : 978-1119684305

Christopher Hadnagy (2018), Social Engineering: The Science of Human Hacking, 2nd Edition, John Wiley & Sons, ISBN-13 : 978-1119433385

Daniel W Dieterle (2018), Basic Security Testing With Kali Linux, Third Edition,CreateSpace Independent Publishing Platform, ISBN-13 : 978-1725031982

Wil Allsopp (2017), Advanced Penetration Testing: Hacking the World's Most Secure Networks, Wiley, ISBN-13: 978-1119367680

D. Teixeira, A. Singh, M. Agarwal; (2018), Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition, Packt Publishing, ISBN-13 : 978-1788623179

Peter Kim; (2018), The Hacker Playbook 3: Practical Guide To Penetration Testing, Independently published, ISBN-13: 978-1980901754

Andrew Bunnie Huang (2019), The Hardware Hacker: Adventures in Making and Breaking Hardware, No Starch Press, ISBN-13 : 978-1593279783

R. A. Grimes, Hacking the Hacker (2017): Learn From the Experts Who Take Down Hackers, Wiley, ISBN-13 : 978-1119396215.

UNIDADE CURRICULAR: Inteligência Artificial e Cibersegurança - PGSICP-INACS

ENQUADRAMENTO: De modo que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais na aplicação da inteligência artificial em soluções de cibersegurança. Esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. Para tal, é necessário perceber os vários métodos e abordagens existentes na inteligência artificial que se adequem à implementação de soluções que proporcionem uma melhoria na segurança de informação, cibersegurança e privacidade. Também é crucial entender e solucionar os problemas de segurança na IA.

PROPÓSITOS E OBJETIVOS

P1. Entender e compreender a importância da aplicação da inteligência artificial nas organizações.

P2. Compreender o funcionamento do Machine Learning assim como o seu ciclo de vida.

P3. Perceber os conceitos associados aos algoritmos de classificação

P4. Conhecer e compreender a aplicação da inteligência artificial em soluções de suporte à cibersegurança.

P5. Entender os problemas de segurança e privacidade associados à utilização de inteligência artificial

P6. Compreender e saber aplicar soluções que mitiguem os problemas de privacidade e segurança das soluções baseadas em inteligência artificial

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar os pontos chave de um sistema baseado em inteligência artificial

C02 Avaliar, testar e verificar a viabilidade das soluções escolhidas

C03 Criar métodos para melhorar a implementação inteligência artificial em soluções para o suporte à cibersegurança

C04 Desenvolver e implementar soluções com recurso à inteligência artificial e cibersegurança.

PROGRAMA

- Introdução à inteligência artificial (IA)

o O que é a IA?

o IA vs Machine Learning (ML) vs Deep Learning

o Paradigmas de Machine Learning (Supervisionado, Não supervisionado, Aprendizagem por reforço)

- Ciclo de vida do ML

o Como construir uma solução de ML ponta a ponta

o O processo CRISP-DM - Cross Industry Standard Process for Data Mining

- Algoritmos supervisionados de ML para classificação

o K-vizinhos mais próximos

o Árvores de decisão

o Conjuntos de árvores

o Fundamentos de Redes Neurais Artificiais

- Inteligência Artificial e Cibersegurança

o Phishing; Malware; Intrusão (Rede e Host); Fraude

o Reconhecimento Facial; Análise de emoções

o Robustez; Explicabilidade;

o Imparcialidade e Preconceito; Transparência.

- Riscos de privacidade na utilização da IA

- Segurança no desenvolvimento de soluções baseadas em inteligência artificial

- Gestão de risco em inteligência arficial

o A framework de gestão de risco em inteligência artificial do NIST

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle

MATERIAL DE ENSINO COMPLEMENTAR

1. T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, Machine Learning Approaches in Cyber Security Analytics, 1st ed. Springer Publishing Company, Incorporated, 2019.

2. E. Tsukerman, Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python. Packt Publishing, 2019.

3. S. Halder and S. Ozdemir, Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Packt Publishing, 2018.

4. A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O?Reilly Media, 2019.

5. M. Stamp, Introduction to Machine Learning with Applications in Information Security, 1st ed. Chapman & Hall/CRC, 2017.

6. T. C. D. S. T. Staff, Introduction to Artificial Intelligence for Security Professionals. Cylance Press, 2017.

7. A. Parisi, Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies. Packt Publishing, 2019.

B. Gupta, M. Sheng, and Q. Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. Taylor & Francis Group, 2021.

9. P. Ganapathi and D. Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security. IGI Global, 2019.

10. L. F. Sikos, AI in Cybersecurity. Springer International Publishing, 2018

UNIDADE CURRICULAR: Princípios de Computação Segura - PGSICP-PRCSE

ENQUADRAMENTO: De modo a que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais de tecnologias de suporte à segurança e privacidade, esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. Para tal, é necessário perceber o que são os princípios básicos de cibersegurança e como os implementar (Confidencialidade, Integridade, Disponibilidade, Autenticação, Autorização, Criptografia, Redes de Computadores, Sistemas Operativos).

PROPÓSITOS E OBJETIVOS:

P1. Entender e compreender os conceitos de segurança e de privacidade

P2. Compreender a importância da utilização de computação segura

P3. Perceber os conceitos chave da segurança computacional

P4. Conhecer boas práticas para implementar computação segura

P5. Usar tecnologias computacionais de forma segura

P6. Saber aplicar princípios, métodos e técnicas de segurança

P7. Compreender e usar a criptografia simétrica e assimétrica

P8. Entender a importância das linguagens de programação na computação segura.

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar as tecnologias para computação segura

C02 Avaliar, testar e verificar a viabilidade das soluções escolhidas

C03 Criar métodos para melhorar a computação segura

C04 Desenvolver e implementar computação segura.

PROGRAMA

- Princípios de Cibersegurança

o Confidencialidade, Integridade a Disponibilidade

o Estados dos dados

o Safeguards

- Autenticação, Autorização e registo

o Mecanismos de controlo de acesso lógico

o Mecanismos de controlo de acesso físico

- Criptografia, Hashing e Estenografia

o Criptografia simétrica

o Criptografia assimétrica

o Assinaturas digitais

o Certificados de Chave Pública

- Conceitos fundamentais de Sistemas Operativos

- Linguagens de programação no contexto da cibersegurança

- Conceitos fundamentais de Redes de Computadores

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle)

MATERIAL DE ENSINO COMPLEMENTAR

McCumber, C.J.R. (1991) Information Systems Security: A Comprehensive Model. The 14th National Computer Security Conference, Washington DC, 1-4 October 1991, 328-337.

Q. Kiser, Cybersecurity: A Simple Beginner?s Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering. Primasta, 2020.

R. Blum and C. Bresnahan, Linux Command Line and Shell Scripting Bible, 3rd ed. Wiley, 2015.

B. Lubanovic, Introducing Python, 2nd ed. O'Reilly Media, 2019.

J. F. Kurose en K. W. Ross, Computer Networking: A Top-Down Approach, 7th ed. Boston, MA: Pearson, 2016.

D. Wong, Real-World Cryptography. Manning, 2021

UNIDADE CURRICULAR: Segurança e Privacidade dos Dados - PGSICP-SEPDD

ENQUADRAMENTO: Pretendendo-se que os diplomados deste curso obtenham ou consolidem noções de segurança e privacidade, esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender e enquadrar esses mesmos conceitos. Para tal, é necessário perceber o que é segurança e conceitos a ela associados (ameaça, acaso, erro, falha, dano, risco, salvaguarda, etc.) e o que é privacidade de modo a ter permanentemente uma postura construtiva.

PROPÓSITOS E OBJETIVOS

1. Entender e compreender o conceito de segurança e de privacidade

2. Compreender a importância da segurança

a) Dominar os conceitos chave da segurança computacional

b) Conhecer boas práticas no desenvolvimento de aplicações seguras

c) Usar tecnologias computacionais de forma segura

3. Adquirir uma postura de "desconfiança construtiva"

a) Saber aplicar princípios, métodos e técnicas de segurança

b) Compreender e usar a criptografia

c) Aplicar ferramentas de teste da segurança computacional

4. Discutir e elaborar planos de privacidade

5. Discutir e utilizar padrões de cibersegurança

PROGRAMA

Segurança e privacidade

Política de cibersegurança

Cifragem e autenticação de mensagens

Tokens de segurança

Regulamento Geral sobre Proteção de Dados (RGPD)

Cifragem simétrica e assimétrica

PKI

Redundância e diversidade

Análise de casos práticos

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle)

MATERIAL DE ENSINO COMPLEMENTAR

Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, ISBN 13: 9780471389224, Wiley (http://www.cl.cam.ac.uk/~rja14/book.html)

André Zúquete, Segurança em Redes Informáticas, 6a Edição Atualizada e Aumentada. 2021 FCA, Editora de Informática. ISBN: 9789727229239

Normas ISO

Framework NIST

UNIDADE CURRICULAR: Seminário e Projeto - PGSICP-SEPRJ

ENQUADRAMENTO: Esta unidade curricular (UC) pretende ser o culminar do ciclo de estudos, devendo ser, num contexto normal, a última unidade curricular em que o estudante obtém aprovação. Nessa medida, todos os conhecimentos e competências adquiridos deverão estar em condições de ser aplicados durante a resolução do problema associado ao projeto e, eventualmente, em ambiente de estágio. A UC foi desenhada para a aplicação e verificação dos conhecimentos, capacidades e competências que o estudante desta pós-graduação deve possuir.

PROPÓSITOS E OBJETIVOS

Esta UC tem por objetivo o desenvolvimento de um Projeto promovendo a recolha de informação pertinente, a seleção fundamentada dos métodos de abordagens, o desenho e implementação duma solução para o problema proposto, bem como, uma posterior a análise crítica dos resultados.

No final desta unidade curricular o aluno deve ser capaz de:

CO1. Interpretar o problema em estudo, aplicando os conhecimentos adquiridos e adotando boas práticas de engenharia informática num contexto de segurança de informação e privacidade.

CO2. Sintetizar o conhecimento existente no âmbito do problema em estudo

CO3. Identificar, analisar e avaliar diferentes abordagens para a resolução do problema. Reconhecer a importância das restrições não técnicas - sociais, de saúde e segurança, ambientais, económicas e industriais.

CO4. Desenhar uma solução para o problema, adotando boas práticas de engenharia informática num contexto de segurança de informação e privacidade.

CO5. Construir a solução para o problema aplicando boas práticas de engenharia informática num contexto de segurança de informação e privacidade.

CO6. Avaliar a solução desenhada/implementada aplicando boas práticas de engenharia informática num contexto de segurança de informação e privacidade.

CO7. Descrever e apresentar de forma rigorosa os processos e resultados dos pontos anteriores.

PROGRAMA I- Seminários na área da Segurança de Informação, Cibersegurança e Privacidade

II - Desenvolvimento do projeto

UNIDADE CURRICULAR: Sistemas de Gestão de Segurança de Informação - PGSICP-SGSIN

ENQUADRAMENTO: De modo que os diplomados deste curso obtenham ou consolidem noções estruturais e fundamentais relacionadas com as estratégias e métodos para a gestão de segurança de informação. Esta unidade justifica-se na medida em que vai fornecer o contexto que prepara as pessoas para entender, enquadrar e aplicar esses mesmos conceitos. Para tal, é necessário perceber as várias normas e frameworks de segurança de informação e como os implementar num contexto de automatização e ou digitalização dos processos de negócio.

PROPÓSITOS E OBJETIVOS

P1. Entender e compreender a importância de um Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.

P2. Compreender a norma ISO/IEC 27001 como base para definição dos requisitos para a implementação Sistemas de Gestão de Segurança da Informação.

P3. Compreender a norma ISO/IEC 27005 como base para definição de uma Metodologia de Gestão de Risco.

P4. Compreender a norma ISO/IEC 27002 e a sua utilização para definição dos controlos de segurança.

P5. Compreender a norma ISO/IEC 27701 e como pode ser usada como extensão da ISO/IEC 27001 na componente de privacidade de dados.

P6. Perceber os princípios de Auditoria de um Sistema de Gestão de Segurança de Informação.

P7. Perceber os conceitos de outras framework de cibersegurança (ex. NIST, QNRCS, CIS, etc.) e como podem ser enquadradas num um Sistema de Gestão de Segurança de Informação.

No final da UC, o aluno deverá ter adquirido competências para:

C01 Identificar os pontos chave de um Sistema de Gestão de Segurança de Informação;

C02 Desenvolver e Implementar um Sistema de Gestão de Segurança de Informação;

C03 Criar métodos para avaliar e melhorar a implementação do Sistema de Gestão de Segurança de Informação;

C04 Utilizar os normativos apresentados de forma adequada.

PROGRAMA

- Motivação para um Sistema de Gestão de Segurança da Informação nas organizações.

- A norma ISO 27001 para Sistemas de Gestão de Segurança da Informação.

- A norma ISO/IEC 27005 como base para definição de uma Metodologia de

Gestão de Risco.

- A norma ISO/IEC 27002 e a sua utilização para definição dos controlos de segurança.

- A norma ISO/IEC 27701 e como pode ser usada como extensão da ISO/IEC 27001 na componente de privacidade de dados.

- Princípios de Auditoria de um Sistema de Gestão de Segurança de Informação.

- Frameworks de cibersegurança (ex. NIST, QNRCS, CIS, etc.) e como podem ser enquadradas num um Sistema de Gestão de Segurança de Informação.

- Apresentação de Trabalhos Práticos

MATERIAL E FERRAMENTAS DE ENSINO MAIS IMPORTANTE

Apresentações e material adicional (Moodle)

Guias práticos / de laboratório (Moodle)

Outro material de apoio fornecido por professores durante a frequência (Moodle)

MATERIAL DE ENSINO COMPLEMENTAR

Alan Calder, Steve Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002; Kogan Page, Seventh Edition, 2019, ISBN: 978-0749496951.

Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online], https://www.nist.gov/cyberframework

ISO/IEC 27005:2018, Third Edition: Information technology - Security techniques - Information security risk management

QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA ? QNCRS, https://www.cncs.gov.pt/pt/quadro-nacional/

David Kim, Michael G. Solomon, Fundamentals Of Information Systems Security, 2016, Jones and Bartlett Publishers

Mark Stamp, Information Security: Principles and Practice, 2021, Wiley Axelos. (2019). ITIL® Foundation, ITIL 4 Edition. TSO (The Stationery Office).

ISACA. (2018). Cobit 2019 Framework Governance and Management Objectives. In COBIT® 2019 Framework. ISACA. https://www.isaca.org/resources/cobit

ISACA. (2018). Cobit 2019 Framework Introduction and Methodology. In COBIT® 2019