Pós-graduação

em

Ciber-Segurança / Cyber-Security

(CiberSeg)

ESTRUTURA CURRICULAR

(2016-06-06)

Diploma de Formação
Avançada
Instituto Superior
Técnico
3º Ciclo de
Bolonha

1ª Edição
2016/2017

http://ciberseg.tecnico.ulisboa.pt/

Este documento foi desenvolvido para a Pós-graduação em Ciber-Segurança.

Versão 1

Instituto Superior Técnico, Lisboa, Portugal

Julho de 2016

Table of Contents

1 Enquadramento

A área da segurança informática é, actualmente, umas das que apresenta maiores desafios aos profissionais na área em causa que, tendo feito a sua formação alguns anos atrás, se apercebem que a tecnologia tem evoluído a grande ritmo.

Assim, este documento apresenta o diploma proposto pelo Instituto Superior Técnico (IST) para o programa de pós-graduação em Ciber-Segurança; o desenho deste diploma levou em consideração os seguintes requisitos:

1. O universo de candidatos está entre os profissionais formados com um grau de mestrado (ou equivalente) nos campos da Engenharia Informática (MEIC), Engenharia Eletrotécnica e de Computação (MEEC), ou Engenharia de Telecomunicações e Informática (METI), ou similar;

2. O programa deve assegurar aos alunos um conhecimento básico, teórico e prático, em todos os domínios fundamentais da Ciber-Segurança, cobrindo as vertentes de **segurança em computadores e segurança em redes**;

3. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas em Ciber-Segurança cobrindo a **segurança no software, em redes, dispositivos móveis, na web, na cloud, e em bases de dados**;

4. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas em Ciber-Segurança cobrindo os **testes de segurança e os processos de desnvolvimento de software seguro**;

5. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas, em Ciber-Segurança cobrindo a **componente organizacional da segurança, e normas e aspectos legais relacionados**.

O requisito #1 exclui deste programa as matérias que são ensinadas nos mestrado dos cursos acima mencionados.

As unidades curriculares **Fundamentals of Computer Security**, **Fundamentals of Network Security**, foram incluídas no programa especificamente para satisfazer o requisito #2.

As unidades curriculares **Application Software Security**, **Network Software Security**, **Mobile Application Security**, e **Web, Cloud and Database Security**, foram incluídas para satisfazer o requisito #3.

As unidades curriculares **Software Security Testing**, e **Secure Software Development Processes**, foram incluídas para satisfazer o requisito #4.

As unidades curriculares **Organizational Security**, e **Compliance and Legal Aspects**, foram incluídas para satisfazer o requisito #5.

É de notar que é fundamental que os alunos deste curso apresentem um conjunto de conhecimentos base que seja uniforme e que abranja as áreas fundamentais de sistemas operativos, sistemas distribuídos, computação móvel, computação na nuvem, e bases de dados, na vertente da segurança informática. Assim, são oferecidas duas disciplinas base (i.e. propedêuticas) que cobrem estes temas: **Fundamentals of Distributed Operating Systems**, e **Fundamentals of Mobile and Cloud Computing**.

O IST está empenhado em oferecer um serviço de educação de alta qualidade, não só em termos de operações, mas especialmente em termos do "produto final" entregue: os graduados deste programa e seu desempenho profissional.

O IST propõe um programa maduro de pós-graduação, incluindo unidades curriculares, docentes e modelos de ensino, que proporcionarão ensino competente e de qualidade que poderá escalar internacionalmente, para não falar do impacto nacional em termos de inovação e competitidade.

O curso de Ciber-Segurança confere um Diploma de Formação Avançada do IST ao abrigo do 3º Ciclo do Processo de Bolonha, com 39 créditos ECTS.

Os Proponentes do Curso de Ciber-Segurança

Prof. Doutor José Manuel Tribolet
Prof. Doutor Paulo Ferreira
Prof. Doutor Miguel Correia
Prof. Doutor Carlos Ribeiro
Prof. Doutor Pedro Adão
Engº Nelson Escravana

2 Objectivos

O curso de Pós-Graduação em Ciber-Segurança apresenta-se como uma nova plataforma de conhecimentos imprescindíveis para a adaptação das empresas às novas e crescentes exigências do mercado do século XXI, na vertente da segurança informática, através de uma preparação sólida e séria e competitiva nos respectivos domínios.

Os requisitos que serviram de pressuposto ao desenho do programa incluem:

1. O universo de candidatos está entre os profissionais formados com um grau de mestrado (ou equivalente) nos campos da Engenharia Informática (MEIC), Engenharia Eletrotécnica e de Computação (MEEC), ou Engenharia de Telecomunicações e Informática (METI), ou similar;

2. O programa deve assegurar aos alunos um conhecimento básico, teórico e prático, em todos os domínios fundamentais da Ciber-Segurança, cobrindo as vertentes de **segurança em computadores e segurança em redes**;

3. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas em Ciber-Segurança cobrindo a **segurança no software, em redes, dispositivos móveis, na web, na cloud, e em bases de dados**;

4. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas em Ciber-Segurança cobrindo os **testes de segurança e os processos de desnvolvimento de software seguro**;

5. O programa deve fornecer profundas capacidades conceituais e profissionais, teóricas e práticas, em Ciber-Segurança cobrindo a **componente organizacional da segurança, e normas e aspectos legais relacionados**.

O requisito #1 exclui deste programa a maior parte das matérias que são ensinadas nos mestrado dos cursos acima mencionados. Tendo em conta este este mesmo requisito #1, é oferecido o módulo designado **Módulo Propedêutico**. O objectivo deste módulo é proporcionar aos alunos um conhecimento uniforme e básico nos domínios fundamentais dos sistemas operativos, sistemas distribuídos, computação móvel, computação na nuvem, e base de dados, com ênfase nos tópicos mais relevantes para a segurança. Note-se que não se pretende, através destas duas unidades curriculares, apresentar os conceitos subjacentes aos sistemas operativos, sistemas distribuídos, ambientes móveis ou bases de dados; com efeito, o que estas duas disciplinas abordam são as vertentes de segurança associadas aso conceitos fundamentais, que se asssumem serem já conhecidos dado o perfil dos alunos. Assim, este módulo permite garantir que todos os alunos têm um conjunto de conhecimentos uniforme que é necessário para poder abordar as matérias lecionadas nos módulos posteriores. As duas unidades curriculares são **Fundamentals of Distributed Operating Systems,** e **Fundamentals of Mobile and Cloud Computing.**

O módulo designado **Módulo Fundamentos**, em resposta ao requisito #2, desenvolve as competências fundamentais da segurança informática. Este módulo inclui duas unidades curriculares: **Fundamentals of Computer Security**, **Fundamentals of Network Security**.

O módulo designado **Módulo Avançado**, em resposta ao requisito #3, desenvolve as competências avançadas da segurança informática no que concerne a segurança do software e em redes, assim como a segurança nos ambientes de computação actuais (dispositivos móveis, nuvem, bases de dados). Este módulo inclui quatro unidades curriculares: **Application Software Security**, **Network Software Security**, **Mobile Application Security**, e **Web, Cloud and Database Security**.

O módulo designado **Módulo Desenvolvimento e Teste**, em resposta ao requisito #4, desenvolve as competências avançadas da segurança informática no que concerne os testes e desenvolvimento de software seguro. Este módulo inclui duas unidades curriculares: **Software Security Testing**, e **Secure Software Development Processes**.

O módulo designado **Módulo Organizacional**, em resposta ao requisito #5, desenvolve as competências avançadas da segurança informática no que concerne as componentes organizacional e legal da segurança, assim como em normas relacionadas. Este módulo inclui duas unidades curriculares: **Organizational Security**, e **Compliance and Legal Aspects**.

Como complemento, o curso prevê um conjunto de seminários (**Módulo de Seminários**) que se destinam a acrescentar (ou a complementar) conhecimentos em áreas importantes da segurança informática directamente relacionadas com os sistemas de informação nas organizações.

As unidades curriculares são organizadas de tal forma que os alunos são capazes de desenvolver os seus projectos num ambiente que vai evoluindo ao longo do curso resultando numa aplicação de software completa, com todas as vertentes de segurança entretanto abordadas nas várias disciplinas. Assim, durante o programa, os alunos vão progressivamente incorporando e integrando as capacidades aprendidas nas diferentes unidades curriculares.

Com esta formação, os alunos adquirirão novas capacidades e fluência intelectual e profissional nas seguintes vertentes:

- Conhecer as vulnerabilidades de segurança em sistemas de informação;
- Mecanismos, algoritmos, tecnologias que permitem detectar e resolver as vulnerabilidades de segurança mais comuns em ambientes computacionais locais, distribuídos, móveis, e na nuvem, assim como em bases de dados;
- Conhecimento das componentes organizacional, regulamentar, e legal da segurança informática nas organizações;
- Experiência prática de detecção de vulnerabilidades de segurança e soluções respectivas no ambito do desenvolvimento de sistemas em rede contemplando ambientes móveis, na nuvem e bases de dados.

3 Diploma e Créditos ECTS

O curso de Ciber-Segurança confere um Diploma de Formação Avançada do IST ao abrigo do 3º Ciclo do Processo de Bolonha com 39 créditos ECTS (European Credit Transfer System).

4 Destinatários

O curso destina-se a profissionais cujas atividades e responsabilidades envolvem diretamente a gestão dos sistemas de informação e desenvolvimento de software com foco na segurança informática.

Assim, os alunos em causa necessitam de adquirir uma formação técnica sólida, séria e atualizada nas várias vertentes da segurança informática e a forma como estas se relacionam com a organização e os negócios.

Este curso de Ciber-Segurança é formalmente um curso de pós-graduação do 3º ciclo de Bolonha do IST. O percurso de continuidade para obtenção de um diploma de 3º ciclo está normalmente associado a detentores de diplomas académicos de estudos superiores e universitários.

Este curso de Ciber-Segurança admite preferencialmente (mas não exclusivamente) engenheiros já com alguns anos de experiência na área da segurança informática, preferencialmente com um grau de mestrado em cursos de Engenharia Informática (MEIC), Engenharia Eletrotécnica e de Computação (MEEC), ou Engenharia de Telecomunicações e Informática (METI) ou similar ou possuidores de um currículo profissional que dê garantias do domínio científico e técnico dos conteúdos equivalentes a estas qualificações académicas

Assim, são requisitos fundamentais para a frequência deste curso de Ciber-Segurança a experiência, maturidade e capacidade profissional do candidato, que tem em conta quer a formação de base, nomeadamente de nível superior e universitária, quer pelas competências adquiridas pelo seu exercício profissional ao longo da vida.

5 Regimes de funcionamento

Este curso poderá ser oferecido segundo dois regimes de funcionamento alternativos, visando populações discentes distintas.

5.1 Regime presencial contínuo e intensivo

Neste regime puramente presencial a tempo inteiro, a decorrer nas instalações académicas do curso, as disciplinas são oferecidas de forma intensiva, num contínuo de duas U.C.s por mês, ao longo de seis meses. Este regime é adequado aos profissionais cujas empresas pretendam qualificar os seus quadros no mais curto espaço de tempo, libertando-os de qualquer outra responsabilidade que não a de frequentarem o curso.

5.2 Regime misto, presencial/ à distância, a tempo parcial

Neste regime, mais adequado para os profissionais que estão ativamente ao serviço das suas organizações em vários pontos do globo, alternam períodos de ensino/aprendizagem em part-time das UC à distância, recorrendo a sessões síncronas e assíncronas, com períodos presenciais intensivos a decorrer nas instalações académicas do IST, para realização de trabalhos, projetos e "exercícos de campo" individuais e em grupo, com durações típicas de uma a duas semanas. A duração total prevista para a frequência do curso neste regime não excederá dois anos.

A oferta em regime misto poderá seguir padrões de implentação segundo vetores temáticos de formação PGG do regime CEPEI do IST, potenciando novos graus de liberdade dos alunos na escolha do regime de frequência mais adequado às suas circunstâncias. A definição dos vetores CEPEI relevantes para este diploma de PGD em Ciber-segurança será feita a partir das UCs deste curso, a seguir discriminadas. Mais detalhes na secção 13.2.

6 Candidaturas

Os candidatos terão ainda que ter um bom domínio da língua Inglesa, dado que muitas aulas e a bibliografia primária do curso serão nesta língua. O processo completo de candidatura deverá conter:

- Documentação comprovativa do grau académico obtido e da respetiva classificação ou do curriculo professional a ser avaliado em termos de qualificação de entrada
- Certificado de Habilitações;
- Curriculum vitae académico e profissional;
- Duas cartas de referência preferencialmente provindas de pessoas que tenham contato com o candidato no seu meio profissional;
- Carta de motivação, com um limite máximo de 700 palavras, expondo as razões que levam o candidato a querer frequentar o curso em causa e os objetivos que pretende atingir;
- Uma fotografia tipo passe;
- Cópia do BI ou do Cartão de Cidadão;
- Cópia do Cartão de Contribuinte ou Cartão de Cidadão.

7 Critérios de Selecção

O processo de admissão resulta da combinação dos seguintes critérios de seleção:

- Ter experiência e maturidade profissional;
- Ter conhecimentos de língua inglesa (idealmente nível B2 ou superior);
- Ter vontade interior para aprender, persistir e progredir;
- Ter disponibilidade para frequenter o curso no regime a que se candidate, seja o presencial seja o misto.
- Ter boa capacidade de relacionamento e de trabalho em equipa.

Para além da apresentação do processo completo, os candidatos poderão ser sujeitos a uma ou mais entrevistas de seleção.

8 Estrutura do Curso

O curso de Ciber-Segurança é composto por:

- um módulo de preparação, i.e. um módulo propedêutico, com duas unidades curriculares;
- quatro módulos curriculares, e
- um módulo de seminários.

Módulos Curriculares	Módulo Propedêutico	Aspectos básicos de ciber-segurança em sistemas operativos, sistemas distribuídos, ambientes móveis, sistemas na nuvem, e bases de dados.	Avaliação
	Módulo Fundamentos	Fundamentos de ciber-segurança em computadores assim como em redes de computadores.	
	Módulo Avançado	Conhecimentos de ciber-segurança em software aplicacional em computadores, em redes, em dispositivos móveis, na web, na numevm, e em bases de dados.	
	Módulo Desenvolvimento e Teste	Conhecimentos de ciber-segurança nas áreas de desenvolvimento de software seguro e teste.	
	Módulo Organizacional	Conhecimentos de ciber-segurança na área das organizações e aspectis legais relacionados.	
	Módulo Seminários	Conhecimentos de ciber-segurança em casos reais de organizações existentes apresentados por especialistas.	

Em cada unidade curricular existe um período de avaliação. Na secção seguinte são resumidos os principais conteúdos programáticos inerentes a cada módulo.

9 Unidades Curriculares do Curso de Ciber-Segurança

As unidades curriculares do curso de Ciber-Segurança estão distribuídas temporalmente da seguinte forma.

	Mês 1	Mês 2	Mês 3	Mês 4	Mês 5	Mês 6
Módulo Propedêutico	Fundamentals of Distributed Operating Systems					
	Fundamentals of Mobile and Cloud Computing					
Módulo Fundamentos		Fundamentals of Computer Security				
		Fundamentals of Network Security				
Módulo Avançado			Application Software Security	Mobile Application Security		
			Network Software Security	Web, Cloud and Database Security		
Módulo Desenvolvimento e Teste					Software Security Testing	Secure Software Development Processes
Módulo Organizacional					Organizational Security	Compliance and Legal Aspects
Módulo de Seminários	Seminários	Seminários	Seminários	Seminários	Seminários	Seminários

As unidades curriculares têm os ECTS que se indicam de seguida.

Ucs	ECTS	Ucs	ECTS
Fundamentals of Distributed Operating Systems	3		
Fundamentals of Mobile and Cloud Computing	3		
Fundamentals of Computer Security Architecture	3		
Fundamentals of Network Security	3		
Application Software Security	3	Mobile Application Security	3
Network Software Security	3	Web, Cloud and Database Security	3
Software Security Testing	3	Secure Software Development Processes	3
Organizational Security	3	Compliance and Legal Aspects	3
Seminários	3		
Total			39

10 Avaliação

A avaliação de cada unidade curricular é constituída por uma combinação dos seguintes elementos:

- Exame, onde são demonstrados, individualmente, os conhecimentos teóricos e práticos apreendidos numa dada unidade curricular.
- Trabalho teórico, onde se apresenta através de um trabalho escrito, desenvolvido individualmente ou em grupo, o resultado da análise ou investigação sobre determinado problema.
- Trabalho prático, onde se produz um ou mais artefactos com o objetivo de resolver determinado problema prático.

Todas as unidades curriculares têm um trabalho prático na sua avaliação. Este trabalho apresenta uma continuidade ao longo das várias unidades curriculares e utiliza uma infra-estrutura com a flexibilidade adequada aos vários passos de desenvolvimento e de configuração da rede subjacente, recorrendo para tal a ambiente distrbuído com várias máquinas virtuais configuradas de forma a suportarem os vários elementos constituintes de um ambiente real (*desktops, laptops, smartphones, cloud, data-bases, routers*, *servers*, etc.)

Aplicam-se as seguintes regras gerais de avaliação a todas as unidades curriculares do curso:

- As notas finais de cada unidade curricular são dadas na escala de 0 a 20 valores por combinação ponderada dos seus elementos de avaliação. Os elementos de avaliação e a ponderação específica são definidos no contexto de cada unidade curricular.
- Um aluno obtém aproveitamento positivo a uma unidade curricular se obtiver uma nota mínima de dez valores na avaliação da unidade curricular.
- Em caso de reprovação, o aluno poderá reinscrever-se à unidade curricular (ou unidade curricular equivalente de substituição) nos dois (2) anos seguintes. A reinscrição obriga ao pagamento da propina da unidade curricular. Situações de exceção, devidamente justificadas e resultantes de motivos de força maior, serão analisadas caso a caso pela Coordenação.

11 Módulos

Esta secção apresenta os módulos constituintes do curso de Ciber-Segurança, indicando quais as unidades curriculares respectivas e seus objectivos, competências, requisitos, programas, método, métodos de avaliação e bibliografia.

11.1 Módulo Propedêutico

O objetivo das unidades curriculares do Módulo Propedêutico é proporcionar aos alunos um conhecimento uniforme e básico nos domínios fundamentais dos sistemas operativos, sistemas distribuídos, computação móvel, computação na nuvem, e base de dados, com ênfase nos mecanismos e algoritmos subjacentes à segurança informática nos ambientes em causa.

As unidades curriculares e respetivos objetivos que compõem este módulo são as seguintes:

Unidade Curricular	Objetivo
Fundamentos de Sistemas Operativos Distribuídos / *Fundamentals of Distributed Operating Systems*	Apresentar uma visão geral dos sistemas computacionais, desde conceitos de baixo nível (gestão de memória, processamento) a camadas superiores, como os sistemas operativos e os sistemas distribuídos, focando os aspectos mais directamente relacionados com a ciber-segurança.
Fundamentos de Computação Móvel e na Nuvem / *Fundamentals of Mobile and Cloud Computing*	Apresentar uma visão geral dos sistemas móveis e na cloud, incluindo conceitos como consistência, virtualização, e bases de dados, focando os aspectos mais directamente relacionados com a ciber-segurança.

11.1.1 Fundamentals of Distributed Operating Systems

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Fundamentos de Sistemas Operativos Distribuídos
Name: Fundamentals of Distributed Operating Systems
Acrónimo: FSOD
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Propedêutico
Período: 1º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar uma visão geral dos sistemas computacionais, desde conceitos de baixo nível (gestão de memória, processamento) a camadas superiores, como os sistemas operativos e os sistemas distribuídos, focando os aspectos mais directamente relacionados com a ciber-segurança.

GOALS
Present a global view of computing systems, from low-level concepts (e.g. memory management, processing) to upper layers, such as operating systems and distributed systems, with a focus on the issues most related to ciber-security.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender as várias camadas de abstração de um sistema computacional mais relevantes para efeitos de ciber-segurança.
- Compreender o papel e os princípios básicos do sistema operativo com ênfase nos mecanismos de autenticação e controle de acesso.
- Compreender os mecanismos básicos para a construção de sistemas distribuídos focando os mecanismos mais relevantes do ponto de vista da ciber-segurança.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Understand the abstraction layers of a computing system with a focus on those most relevant for ciber-security purposes.
- Understand the role and the basic principles of an operating system with an emphasis on the authentication and acess control mechanisms.
- Understand the basic mechanisms for developing distributed systems with a focus on ciber-security.

REQUISITOS
Programação em C e em Java.

REQUIREMENTS
C and Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Sistemas operativos.
- Hierarquia e gestão de memória.
- Sistema de ficheiros.
- Sistemas distribuídos.

PROGRAM
The unit covers the following topics:

- Operating systems.
- Memory hierarchy and memory management.
- File systems.
- Distributed systems.

MÉTODO

- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD

- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Distributed Systems - Concepts and Design, Fifth Edition	George Coulouris, Jean Dollimore, Tim Kindberg and Gordon Blair	2011	Pearson ISBN-10: 0132143011 ISBN-13: 978-0132143011	Principal

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.1.2 Fundamentals of Mobile and Cloud Computing

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Fundamentos de Computação Móvel e na Nuvem
Name: Fundamentals of Mobile and Cloud Computing
Acrónimo: FCMN
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Propedêutico
Período: 1º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar uma visão geral dos sistemas móveis e na nuvem, incluindo conceitos como permissões, controle de acesso, consistência, virtualização, e bases de dados, focando os aspectos mais directamente relacionados com a ciber-segurança.

GOALS
Present a global view of both mobile and cloud computing systems, including concepts such as permissions, access control, consistency, virtualization, and persistence (e.g. databases) with a focus on the issues most related to ciber-security.

COMPETÊNCIAS
Após o completamento da UC os alunos terão competências para:

- Compreender os mecanismos e algoritmos existentes nos dispositivos móveis (*smartphones, tablets, laptops*), com impacto na ciber-segurança, ao nível dos sistemas operativos, bibliotecas e aplicações.
- Compreender os mecanismos e algoritmos existentes nos sistemas e aplicações na nuvem com impacto na ciber-segurança.
- Compreender os mecanismos e algoritmos existentes nas bases de dados, incluindo as interacções das aplicações com essas, com impacto na ciber-segurança.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Understand the existing mechanisms and algorirthms in mobile devices (e.g. smartphones, tablets, laptops), at the level of the operating system, libraries, and applications, which are most relevant for ciber-security purposes.
- Understand the existing mechanisms and algorirthms in cloud systems and applications, which are most relevant for ciber-security purposes.
- Understand the existing mechanisms and algorirthms in persistent systems (e.g. databases), including their interactions with applications, with impact on ciber-security.

REQUISITOS
Programação em C e em Java.

REQUIREMENTS
C and Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Noções fundamentais de computação móvel e ubíqua
- Tecnologias de localização
- Sistema Android
- Máquinas virtuais e virtualização
- Suporte hardware para virtualização (e.g, VMWare, QEMU/KVM, Xen)
- Componentes principais da JVM
- Gestão na nuvem e APIs
- Bases de dados SQL e no-SQL

PROGRAM
The unit covers the following topics:
- mobile and ubiquituous computing (fundamental notions),
- location technologies,
- Android framework,
- virtual machines,
- CPU virtualization,
- hardware support for virtualization (examples, VMWare, QEMU/KVM, Xen),
- Java VM main components,
- cloud management APIs,
- databases (SQL and no-SQL).

MÉTODO
- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD
- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Mobile Platform Security	N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, Ahmad-Reza Sadeghi	2013	Morgan and Claypool ISBN-10: 1627050973 ISBN-13: 978-1627050975	Principal
Building the Infrastructure for Cloud Security: A Solutions View (Expert's Voice in Internet Security)	Raghuram Yeluri, Enrique Castro-Leon	2014	Apress ISBN-10: 1430261455 ISBN-13: 978-1430261452	Principal
Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) 1st Edition	Tim Mather, Subra Kumaraswamy, Shahed Latif	2009	O'Reilly Media ISBN-10: 0596802765 ISBN-13: 978-0596802769	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION

Máquina virtual configurável em rede. Android studio.

11.2 Módulo Fundamentos

O objetivo das unidades curriculares do Módulo Fundamentos é proporcionar aos alunos um conhecimento básico, teórico e prático, em todos os domínios fundamentais da segurança informática, cobrindo as vertentes da segurança em computadores e segurança em redes.

As unidades curriculares e respetivos objetivos que compõem este módulo são as seguintes:

Unidade Curricular	Objetivo
Fundamentos de Segurança de Computado / *Fundamentals of Computer Security*	Apresentar os conceitos fundamentais subjacentes à ciber-segurança em computadores; compreender os modelos de ciber-segurança mais relevantes, modelo de ataques, mecanimos e algoritmos fundamentais de identificação, autenticação, criptografia e chaves, controle de acesso, monitores de referência, acesso a bases de dados e segurança do software.
Fundamentos de Segurança em Redes / *Fundamentals of Network Security*	Apresentar os conceitos fundamentais subjacentes à ciber-segurança em sistemas distribuídos, i.e. em redes de computadores; compreender os mecanimos e algoritmos fundamentais subjacentes à comunicação em rede, código mal-intencionado, cifras, criptografia simétrica e assimétrica, assinaturas digitais, certificados, segurança nível transporte.

11.2.1 Fundamentals of Computer Security

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Fundamentos de Segurança de Computadores
Name: Fundamentals of Computer Security
Acrónimo: FSC
Nível: : Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Fundamentos
Período: 2º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar os conceitos fundamentais subjacentes à ciber-segurança em computadores; compreender os modelos de segurança mais relevantes, modelo de ataques, mecanismos e algoritmos fundamentais de identificação, autenticação, criptografia e chaves, controle de acesso, monitores de referência, acesso a bases de dados e segurança do software.

GOALS
Present the fundamental concepts underlying computer ciber-security; understand the most relevant security and attack models, fundamental mechanisms and algorithms for identification and authentication, basic aspects of key management and cryptography, access control, reference monitors, access to databases, and software security.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender os conceitos fundamentais de ciber-segurança em computadores;

- Conhecer os problemas fundamentais na área da segurança informática e modelo de ataques;
- Dominar os mecanismos e algoritmos mais usuais para identificação e autenticação, controle de acesso, monitores de referência e acesso a bases de dados;
- Relacionar as soluções estudadas com as que se encontram nos sistemas de informação baseados em Unix.

COMPETENCIES
Upon unit completion, students will have the competencies to:
- Unserstand the fundamental concepts of computer security;
- Understand the fundamental problems in the area of computer security and attack model;
- Knowledge of the most common mechanisms and algorithms used for identification and athetication purposes, access control, monitors and access to databases.
- Relate the solutions presented with those found in Unix based information systems.

REQUISITOS
Programação em C em Java.

REQUIREMENTS
C and Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:
- História da segurança em computadores;
- Gestão da segurança (ataques, riscos e análise de ameaças);
- Camadas de segurança;
- Identificação e autenticação;
- Monitores de segurança;
- Segurança em sistemas operativos (e.g. Unix);
- Segurança em bases de dados;
- Segirança do software;
- Modelos de segurança (Bell-LaPadula, Chinese Wall etc.)

PROGRAM
The unit covers the following topics:
- History of computing security,
- Managing security (attacks, risk and threat analysis),
- Foundations (layers),
- Identification and authentication,
- Access control,
- Reference monitors,
- Operating system security,
- Database security,
- Sotware security,
- Security models (Bell-LaPadula, Chinese Wall etc.)

MÉTODO
- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD
- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Computer Security, 3rd Edition.	Dieter Gollmann	2011	Wiley ISBN-10: 0470741155 ISBN-13: 978-0470741153	Principal

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.2.2 Fundamentals of Network Security

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Fundamentos de Segurança em Redes
Name: Fundamentals of Network Security
Acrónimo: FSR
Nível: : Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Fundamentos
Período: 2º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar os conceitos fundamentais subjacentes à ciber-segurança em redes de computadores; compreender as vulnerabilidades mais relevantes assim como as respetivas soluções compreendendo os mecanismos e algoritmos fundamentais subjacentes à comunicação em rede, código mal-intencionado, cifras, criptografia simétrica e assimétrica, assinaturas digitais, certificados, segurança nível transporte.

GOALS
Present the fundamental concepts regarding network security; understand the most important vulnerabilities and the corresponding solutions in computer networks with a with a focus on the fundamental mechanisms and algorithms for communication, malware, cryptography, digital signatures, certificates, transport-level security, wireless network security, electronic mail security, IP security, intrusion, firewalls.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender os conceitos fundamentais de ciber-segurança em redes de computadores;
- Conhecer as vulnerabilidades mais relevantes em ambiente distribuído;
- Dominar os mecanismos e algoritmos: para obter chaves para crifra e assinar digitalmente, subjacentes à segurança ao nível transporte, em redes sem fios, e ao nível IP;
- Relacionar as soluções estudadas com as que se encontram nos sistemas de informação distribuídos baseados em Unix.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Understand the main concepts regarding network ciber-security;
- Knowledge of the most important vulnerabilities in computer networks;
- Mastering the mechanisms and algorithms used for key management (to encrypt/decryt, sign), for transport-level security, wireless and IP security;
- Relate the solutions studied with those used in Unix based information systems.

REQUISITOS
Programação em C e em Java.

REQUIREMENTS
C and Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Arquitectura de segurança OSI
- Conceitos básicos de criptografia
- Gestão de chaves
- Segurança nível transporte e nível IP
- Segurança em redes sem fios
- Segurança do email
- Intrusão
- Anteparas de segurança
- Segurança web.

PROGRAM
The unit covers the following topics:

- OSI Security Architecture,
- cryptography (basic concepts, symetric, assymetric),
- key establishment,
- digital signatures,
- transport-level security,
- wireless network security,
- electronic mail security,
- IP security,
- intrusion,
- firewalls,
- web security.

MÉTODO

- Aulas teóricas e aulas de laboratório;
- Projeto em grupo.

METHOD

- Theoretical and lab classes;
- Group projects.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components:

- Project (50%);
- Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Network Security Essentials Applications and Standards (5th Edition)	William Stallings	2013	Pearson ISBN-10: 0133370437 ISBN-13: 978-0133370430	Principal

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.3 Módulo Avançado

O objetivo das unidades curriculares do Módulo Avançado é fornecer profundas capacidades conceituais e profissionais, teóricas e práticas, em segurança informática cobrindo a segurança no software, dispositivos móveis, na web, na cloud, e em bases de dados.

As duas primeiras cadeiras apresentam os aspectos fundamentais de segurança na vertente do software; as restantes duas focam a segurança em dispositivos móveis (Android), na web, e em bases de dados.

As unidades curriculares e respetivos objetivos que compõem este módulo são as seguintes:

Unidade Curricular	Objetivo
Segurança de Software Aplicacional / *Application Software Security*	Compreender as vulnerabilidades de segurança em software mais comuns assim como as suas causas fundamentais. Conhecer as soluções (mecanismos, algoritmos) para a sua prevenção e/ou detecção.
Segurança em Redes de Computadores / *Network Software Security*	Compreender as vulnerabilidades de segurança mais comuns em redes de computadores e quais as respectivas soluções.
Segurança em Sistemas Móveis / *Mobile Application Security*	Compreender as vulnerabilidades de segurança que ocorrem em ambientes móveis, assim como as suas causas fundamentais (com ênfase no ambiente Android). Conhecer as soluções (mecanismos, algoritmos) para a sua prevenção e/ou detecção.
Segurança na Nuvem, na Web e em Bases de Dados / *Web, Cloud, and Database Security*	Compreender as vulnerabilidades de segurança que ocorrem em sistemas na web, nuvem e em bases de dados, assim como as suas causas fundamentais. Conhecer as soluções (mecanismos, algoritmos) para a sua prevenção e/ou detecção.

11.3.1 Application Software Security

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Segurança de Software Aplicacional
Name: Application Software Security
Acrónimo: SSA
Nível: : Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Avançado
Período: 3º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar os conceitos fundamentais subjacentes à segurança de aplicações de software; compreender as vulnerabilidades mais relevantes assim como as respetivas soluções para os casos das aplicações web e aplicações de código nativo.

GOALS
To present the basic concepts underlying the security of software applications; to understand the most relevant vulnerabilities as well as the respective solutions for the cases of web applications and native code applications.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender os conceitos fundamentais de segurança de software aplicacional;
- Conhecer as vulnerabilidades mais relevantes em aplicações Web e de código nativo;
- Dominar os principais mecanismos para evitar essas vulnerabilidades.

COMPETENCIES
After completing the course, students will have skills to:

- Understand the basic concepts of application software security;
- Know the most important vulnerabilities in Web applications and native code;
- Master the main mechanisms to prevent these vulnerabilities.

REQUISITOS
Programação em C e em Java.

REQUIREMENTS
C and Java programming.

PROGRAMA
A unidade curricular cobre os seguintes temas:

- Vulnerabilidades em aplicações Web (injecção de SQL, cross-site scripting, injeção de ficheiros, etc.);
- Vulnerabilidades em aplicações código nativo (buffer overflows, return oriented programming, injeção de comandos, corridas, etc.);
- Principais protecções.

PROGRAM
The unit covers the following topics:

- Vulnerabilities in web applications (SQL injection, cross-site scripting, file injection, etc.);
- Vulnerabilities in native code applications (buffer overflows, return oriented programming, command injection, races, etc.);
- Main protections.

MÉTODO

- Aulas teóricas e aulas de laboratório;
- Projeto em grupo.

METHOD

- Theoretical and lab classes;
- Group projects.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS

TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Segurança no Software	Miguel Pupo Correia e Paulo Jorge Sousa	2010	FCA ISBN 9789727226627	Principal
24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	Michael Howard, David LeBlanc and John Viega	2009	McGraw Hill ISBN-10: 0071626751 ISBN-13: 978-0071626750	Principal

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.3.2 Network Software Security

Área Científica: Arquitetura de Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Segurança em Redes de Computadores
Name: Network Software Security
Acrónimo: SRC
Nível: : Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Avançado
Período: 3º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Compreender as vulnerabilidades de segurança mais comuns em redes de computadores e quais as respectivas soluções. Nomeadamente, conhecer os principais erros na utilização e implementação de mecanismos de autenticação, na utilização de APIs criptográficas e as principais vulnerabilidades dos protocolos da família IP. Entender os conceitos essenciais para gestão de identidades, autenticação e autorização na internet.

GOALS
Understanding common security vulnerabilities and solutions in computer networks. Specifically understand the most common errors in authentication mechanisms, and in the usage of cryptographic APIs. Understanding federated identity management in the web (SAML 2.0, OAuth 2.0, WS-*).

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender as vulnerabilidades de segurança mais comuns em redes de computadores;
- No âmbito do desenvolvimento de soluções em rede, conceber e implementar as medidas apropriadas à mitigação das principais vulnerabilidades de segurança;
- Analisar de forma critica as interfaces com outros sistemas, precavendo-se de futuras vulnerabilidades;
- Conhecer os principais erros na utilização e implementação de mecanismos de autenticação, na utilização de APIs criptográficas e as principais vulnerabilidades dos protocolos da família IP;
- Desenhar e implementar sistemas de autenticação e autorização na internet.

COMPETENCIES
After completing the course, students will have skills to:

- Understand the most common security vulnerabilities in computer networks;
- Design and implement appropriate measures to mitigate the main security vulnerabilities;
- Analyze critically interfaces with other systems, being precautious - future vulnerabilities;
- Undestand how to securely use cryptographic APIs;
- Design and implement authentication and authorization systems on the internet.

REQUISITOS
Conhecimento básico de redes IP. Programação C e Java.

REQUIREMENTS
Basic understanding of IP networks. C and Java Programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Utilização incorreta de cifras (senhas fracas , números aleatórios fraco , utilização incorrecta),
- Erros protocolares nas diferentes camadas do modelo OSI
- Protocolos de autenticação
- Gestão de Identidades (SAML 2.0 , WS- * , O- Auth)
- Usar APIs de criptografia.

PROGRAM
The unit covers the following topics:

- criptography software errors (weak passwords, weak random numbers, incorrect use),
- network errors (protecting traffic, PKI and SLL errors, name resolution trust),
- identity management (SAML 2.0 , WS- * , O- Auth),
- using cryptographic APIs.

MÉTODO

- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD

- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
24 Deadly sins of software security programming flaws and how to fix them	M. Howard, D. LeBlanc, and J. Viega	2010	McGraw-Hill ISBN-10: 0071626751 ISBN-13: 978-0071626750	Principal
Identity Management Concepts, Technologies, and Systems	Elisa Bertino, Kenji Takahashi	2010	Artech House ISBN-13: 978-1-60807-039-8	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.3.3 Mobile Application Security

Área Científica: Arquitetura de Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Segurança em Sistemas Móveis
Name: Mobile Application Security
Acrónimo: SSM
Nível: : Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Avançado
Período: 4º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Compreender as vulnerabilidades de segurança que ocorrem em ambientes móveis, assim como as suas causas fundamentais (com ênfase no ambiente Android). Conhecer as soluções (mecanismos, algoritmos) para a sua prevenção e/ou detecção.

GOALS
Understand the security vulnerabilities in mobile devices (Android) along with the corresponding causes. Master the solutions for its prevention and detection.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender as várias camadas de abstração e módulos do sistema Android mais relevantes para efeitos de segurança
- Comprender o modelo de segurança do Android com ênfase no mecanimos de controle de permissões, gestão de software e configurações
- Compreender a gestão de chaves e de certificados assim como o serviço de armazenamento
- Compreender a segurança associada ao uso de NFC assim como o mecanimos de actualizações do sistema e acesso “root”.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Understand the main abstraction layers and modules of Android which most relevant for security purposes;
- Understand the Android security module with a focus on the mechanism to enforce permissions, software management anf configurations;
- Understand the management of keys and cetificates and their storage;
- Understand the NFC security;
- Understand the software update mechanism and root access.

REQUISITOS
Programação em Java.

REQUIREMENTS
Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Modelo de segurança do Android

- Gestão e verificação de permissões
- Gestão de software
- Criptografia , certificados e seu armazenamento
- Segurança do NFC
- Actualizações de software e acessos previligiados

PROGRAM
The unit covers the following topics:
- Android security model and attack surface,
- permissions,
- package and user management,
- criptographic providers,
- network security PKI,
- credentials and storage,
- online account management,
- NFC security,
- system updates and root access.

MÉTODO
- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD
- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Android Security Internals. An In-Depth Guide to Android's Security Architecture (1st Edition)	Nikolay Elenkov	2014	No Starch Press ISBN-10: 1593275811 ISBN-13: 978-1593275815	Principal
Android Hacker's Handbook (1st Edition)	Joshua J. Drake , Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski	2014	Wiley ISBN-10: 111860864X ISBN-13: 978-1118608647	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede. Android studio.

11.3.4 Web, Cloud and Database Security

Área Científica: Arquitetura e Sistemas Operativos
Grupo: Aplicações e Serviços em Rede
Nome: Segurança na Nuvem, na Web e em Bases de Dados
Name: Web, Cloud and Database Security
Acrónimo: SNWBD
Nível: : Formação (F)

Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Avançado
Período: 4º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Apresentar os conceitos fundamentais subjacentes à segurança de aplicações web na nuvem com bases de dados SQL e NoSQL, as ameaças mais relevantes e soluções. Apresentar os temas da detecção de intrusões e da segurança da cadeia de fornecimento.

GOALS
To present the basic concepts underlying the security of web applications in the cloud with SQL/NoSQL databases, the most relevant threats and solutions. To present the topics of intrusion detection and supply chain security.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Compreender os conceitos fundamentais de segurança de aplicações web na nuvem com bases de dados SQL e NoSQL;
- Dominar os mecanismos de sanitização, validação e codificação de entradas;
- Dominar a noção de mecanismos de protecção dinâmica;
- Dominar o conceito de detecção de intrusões;
- Dominar o conceito e as mitigações de ataques via cadeia de fornecimento.

COMPETENCIES
After completing the course, students will have skills to:

- Understand the basic concepts of web application security in the cloud with SQL and NoSQL databases;
- Mastering input sanitization, validation and encoding mechanisms;
- Mastering the notion of dynamic protection mechanisms;
- Mastering the concept of intrusion detection;
- Mastering the concept and mitigations against supply chain attacks.

REQUISITOS
Programação em Java.

REQUIREMENTS
Java programming.

PROGRAMA
A unidade curricular cobre os seguintes temas:

- Segurança na configuração de servidores Web e bases de dados (SQL, NoSQL) na nuvem;
- Sanitização, validação e codificação de entradas;
- Mecanismos de protecção dinâmica (firewalls Web, protecções contra buffer overflows, etc.);
- Conceito de detecção de intrusões, principais técnicas e exemplos de sistemas;
- Segurança na cadeia de fornecimento e mitigações (o problema em geral e o caso dos plugins/extensões).

PROGRAM
The unit covers the following topics:

- Web server, database (SQL, NoSQL) and cloud configuration security;

- Input saniztization, validation, and encoding;
- Dynamic protection mechanisms (Web application firewalls, buffer overflow protections, etc.);
- Intrusion detection concept, main approaches, and example intrusion detection systems;
- Supply chain security and mitigations (the problem in general and the plugin/extension case).

MÉTODO
- Aulas teóricas e aulas de laboratório;
- Projeto em grupo.

METHOD
- Theoretical and lab classes;
- Group projects.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Security Guidance for Critical Areas of Focus in Cloud Computing V3.0	Cloud Security Alliance	2011	na	Principal
Segurança no Software	Miguel Pupo Correia e Paulo Jorge Sousa	2010	FCA ISBN 9789727226627	Principal
Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) 1st Edition	Tim Mather, Subra Kumaraswamy, Shahed Latif	2009	O'Reilly Media ISBN-10: 0596802765 ISBN-13: 978-0596802769	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.4 Módulo Desenvolvimento e Teste

O objetivo das unidades curriculares do Módulo Desenvolvimento e Teste é fornecer profundas capacidades conceituais e profissionais, teóricas e práticas, em segurança informática no que concerne os testes e desenvolvimento de software seguro.

As unidades curriculares e respetivos objetivos que compõem este módulo são as seguintes:

Unidade Curricular	Objetivo
Testes de Segurança / *Software Security Testing*	Identificar riscos de segurança associados aos sistemas, e apresentar os conceitos fundamentais subjacentes ao teste de software seguro, o seu desenvolvimento e aplicação.
Desenvolvimento de Software Seguro / *Secure Software Development Processes*	Apresentar os conceitos fundamentais subjacentes ao desenvolvimento de software seguro abordando as técnicas e ferramentas de análise de requisitos.

11.4.1 Software Security Testing

Área Científica: Metodologia e Tecnologia de Programação
Grupo: Engenharia de Software
Nome: Testes de Segurança
Name: Software Security Testing
Acrónimo: TS
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Desenvolvimento e Teste
Período: 5º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Identificar as vulnerabilidades e os riscos associados a um sistema. Aprendizagem das diversas técnicas de desenvolvimento de testes de sofware e sua aplicação no contexto de testes de segurança.

GOALS
To identify the vulnerabilities of a system and its associated risks. To learn the different techniques of software testing and their application in the context of security testing.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Analisar as vulnerabilidades de um sistema, e calcular o risco associado às mesmas;
- Desenvolver um plano de testes por forma a detectar as vulnerabilidades identificadas.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Analyse the vulnerabilities of a system, and compute the associated risk;
- Develop a test plan in order to detect the identified vulnerabilities.

REQUISITOS
Programação em Java.

REQUIREMENTS
Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Definição da superfície de ataques,
- Modelação de ameaças e desenvolvimento de testes,
- Testes baseados em modelos e Testes a propriedades de segurança,
- Testes de Caixa-Preta, Caixa-Branca, e Caixa-Cinzenta,
- Auditoria de código,
- Análise e gestão de risco, e impactos na actividade de teste de software.
- Testes de Intrusão.

PROGRAM
The unit covers the following topics:

- Defining the attack surface,
- prioritizing tests using threat modelling,

- testing security properties,
- model-based testing,
- black-box testing (fuzzing, etc.),
- white-box testing (static analysis),
- grey-box testing,
- manual code auditing,
- the role of penetration testing.

MÉTODO
- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD
- Lectures and labs.
- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Security Engineering: A Guide to Building Dependable Distributed Systems (2nd Edition)	R. Anderson	2008	Wiley ISBN-10: 0470068523 ISBN-13: 978-0470068526	Principal
Computer Security: Art and Science (1st Edition)	M. Bishop	2002	Addison-Wesley Professional ISBN-13: 078-5342440997 ISBN-10: 0201440997	Secundária
Security Risk Management: Building an Information Security Risk Management Program from the Ground Up	E. Wheeler	2011	Syngress ISBN-10: 1597496154 ISBN-13: 978-1597496155	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.4.2 Secure Software Development Processes

Área Científica: Metodologia e Tecnologia de Programação
Grupo: Engenharia de Software
Nome: Desenvolvimento de Software Seguro
Name: Secure Software Development Processes
Acrónimo: DSS
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Desenvolvimento e Teste
Período: 6º Mês

CARGA HORÁRIA

Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Conhecer os princípios de desenvolvimento de software seguro. Dominar as técnicas e as ferramentas de análise de requisitos e desenvolvimento de software seguro.

GOALS
To know the design principles of secure software. To master the techniques and tools for analysis and development of secure software.

COMPETÊNCIAS
Após completarem a disciplina, os alunos terão competências para:

- Conhecer os princípios básicos do desenvolvimento de sistemas seguros,
- Conhecer e utilizar diferentes técnicas, métodos e ferramentas nas diversas fases do ciclo de desenvolvimento de software por forma a melhorar a segurança dos sistemas resultantes.

COMPETENCIES
Upon unit completion, students will have the competencies to:

- Understand the basic principles for development of secure systems,
- To master and use different techniques, methods, and tools in the several phases of the software development process, in order to improve the security of the resulting systems.

REQUISITOS
Programação em Java.

REQUIREMENTS
Java programming.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Princípios de desenvolvimento de software seguro,
- Requisitos de segurança e sua análise,
- Vulnerabilidades de Segurança,
- Modelação de requisitos de segurança durante o processo de desenho e desenvolvimento do sistema (Microsfot SDL),
- Programas de desenvolvimento de software seguro (BSIMM),
- Boas práticas de desenvolvimento de Software Seguro para o sector financeiro (BITS Software Assurance Framework),
- Desenvolvimento de Software Seguro em ambientes ágeis (SDL-Agile, SAFEcode).

PROGRAM
The unit covers the following topics:

- Software security design principles,
- Security Requirements and Analysis,
- Software vulnerabilities,
- Introducing security requirements in the software development lifecycle (Microsoft SDL),
- Software security programs (BSIMM),
- BITS Software Assurance Framework for developing software for the finantial sector,
- Security in agile software development (SDL-Agile, SAFEcode).

MÉTODO

- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD

- Lectures and labs.

- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be decided)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Security Engineering: A Guide to Building Dependable Distributed Systems (2nd Edition)	R. Anderson	2008	Wiley ISBN-10: 0470068523 ISBN-13: 978-0470068526	Principal
Security Risk Management: Building an Information Security Risk Management Program from the Ground Up	E. Wheeler	2011	Syngress ISBN-10: 1597496154 ISBN-13: 978-1597496155	Secundária

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
Máquina virtual configurável em rede.

11.5 Módulo Organizacional

O objetivo das unidades curriculares do Módulo Organizacional é fornecer profundas capacidades conceituais e profissionais, teóricas e práticas, nos domínios da Ciber-segurança, cobrindo as componentes de governança, risco e conformidade legal e normativa.

As unidades curriculares e respetivos objetivos que compõem este módulo são as seguintes:

Unidade Curricular	Objetivo
Segurança Organizacioanal / *Organizational Security*	Conhecer e entender as principais ameaças, vulnerabilidades e riscos relacionados com a Ciber-segurança nas Organizações e entender como uma Organização pode desenvolver uma visão holística para suporte às actividades de governança, gestão e controlo da Ciber-segurança. Conhecer as principais ferramentas, boas práticas e fontes de informação relacionadas com a implementação de modelos e frameworks de segurança e políticas nos domínios organizacionais, processos, pessoas e tecnologias (ex. COBIT 5, NIST, SANS CIS Critical Security Controls, ISF, ISO/IEC 27002).
Conformidade e Aspectos Legais da Ciber-segurança / *Compliance and Legal Aspects*	Abordar os aspectos de conformidade legal e normativa relacionados com a Segurança e Ciber-segurança nas Organizações, nomeadamente: o cibercrime; enquadramento legal e normativo do digital no contexto nacional, europeu e global; os desafios de gestão da privacidade da informação; realização de auditorias (ex. forenses); e processo de certificação em normativos internacionais relacionados com o risco, Ciber-segurança e continuidade/resiliência (ex. EU's Data Protection Directive, ISO/IEC 27001:2013, PCI DSS, ISO 22301:2012).

11.5.1 Organizational Security

Área Científica: TBC
Grupo: TBC
Nome: Segurança Organizacioanal

Name: Organizational Security
Acrónimo: SOG
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Organizacional
Período: 5º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Conhecer as principais ameaças, vulnerabilidades e riscos relacionados com a Ciber-segurança nas Organizações e entender como uma Organização pode desenvolver uma visão holística para suporte às actividades de governança, gestão e controlo da Ciber-segurança. Conhecer as ferramentas, boas práticas e fontes de informação relacionadas com a implementação de modelos e frameworks de segurança nos domínios organizacionais, processos, pessoas e tecnologias (ex. COBIT 5, NIST, SANS CIS Critical Security Controls, ISF, ISO/IEC 27002).

GOALS
Know and understand the main threats, vulnerabilities and risks related to Information Security and Cyber Security in Organizations and understand how an Organization can adopt a holistic vision to support the governance, management and control of Information Security and Cyber Security. Knowing the most relevant tools, good practices and information sources related to the implementation of security models and frameworks in organizational, processes, people and technologies domains (eg. COBIT 5, NIST, SANS CIS Critical Security Controls, ISF, ISO/IEC 27002).

COMPETÊNCIAS
A unidade curricular desenvolve as seguintes competências:

- Avaliar riscos e controlos os controlos de segurança para garantir um nível de mitigação aceitável.
- Implementar e manter o programa de segurança em alinhamento com a estratégia de segurança.
- Garantir o alinhamento entre o programa de segurança e outras funções de negócio para apoiar a integração com os processos de negócio.
- Implementar e manter arquiteturas de segurança (pessoas, processos, tecnologia) para operacionalizar o programa de segurança da informação.
- Implementar e manter um programa de sensibilização e formação em segurança para promover um ambiente seguro e uma cultura de segurança eficaz.
- Integrar os requisitos de segurança nos processos da Organização ou atividades de terceiros para manter a *baseline* de segurança.
- Implementar e manter uma estratégia de segurança em alinhamento com os objetivos e metas organizacionais
- Implementar e manter uma framework de governança e gestão da segurança para garantir que as atividades de segurança suportam a estratégia.
- Integrar os requisitos de governança de segurança na governança corporativa para garantir que os objetivos e metas organizacionais são suportadas pelo programa de segurança da informação.
- Implementar e manter as políticas de segurança para comunicar as diretrizes de gestão e orientar o desenvolvimento de normas, procedimentos e guidelines.
- Desenvolver business cases para apoiar os investimentos em segurança da informação.
- Definir e comunicar as funções e responsabilidades de segurança em toda a Organização
- Implementar, monitorar, avaliar e reportar métricas para fornecer à gestão informação relevante relacionada com a eficácia da estratégia de segurança.

COMPETENCIES
The unit covers the following competencies:

- Evaluate security risks and controls to determine whether they are aligned with acceptable risk level.
- Establish and maintain the security program in alignment with the security strategy.
- Ensure alignment between the security program and other business functions to support integration with business processes.
- Establish and maintain security architectures (people, process, technology) to execute the information security program.
- Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
- Integrate information security requirements into organizational processes or activities of third parties to maintain the organization's security baseline.
- Establish and maintain an information security strategy in alignment with organizational goals and objectives.
- Establish and maintain an information security governance framework to guide activities that support the information security strategy.
- Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
- Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.
- Develop business cases to support investments in information security.
- Define and communicate the roles and responsibilities of information security throughout the organization.
- Establish, monitor, evaluate and report metrics to provide management with accurate information regarding the effectiveness of the information security strategy.

REQUISITOS
Nenhum.

REQUIREMENTS
None.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Introdução e visão geral da Ciber-segurança nas Organizações:
    - Ciberguerra, Cibercrime e Advanced Persistent Threats (APTs)
    - *Game changers* e impactos do Cibercrime e da Ciberguerra nas Organizações e na Sociedade
    - Impacto da Ciber-segurança na criação de valor das Organizações
    - Desafios da adopção de tecnologias emergentes
    - Enquadramento do tema da segurança no contexto geral do risco e controlo da Organização, e do sistema de informação em particular
- Ameaças, vulnerabilidades e riscos relacionados com a Ciber-segurança nas Organizações:
    - Vulnerabilidades e categorização de Ciber-ameaças
    - A importância de abordagens sistémicas à análise de Ciber-riscos
    - Visão geral dos Ciber-riscos: Riscos Organizacionais; Riscos Sociais; Riscos Técnicos.
- Visão geral e utilização de boas práticas de governança, gestão e controlo da Ciber-segurança nos domínios de: Princípios, políticas e frameworks; Processos; Estruturas Organizacionais; Cultura, ética e comportamentos; Artefactos de Informação; Serviços, Infra-estruturas e aplicações; e Pessoas e competências.
- Desenvolvimento de objetivos e métricas para a gestão da segurança e alinhamento com os objetivos relacionados com TI e objetivos globais da Organização
- Desafios das funções de gestão de risco e segurança na Organizações (ex. CIO, CISO, CSO)
- Casos práticos e cenários de implementação de estratégias, programas e frameworks de governança, gestão e controlo dos riscos e segurança nas organizações.

PROGRAM

The unit covers the following topics:

- Introduction and overview of Cyber Security in Organizations:
  - Cyberwar, Cybercrime and Advanced Persistent Threats (APTs)
  - Game changers and impacts of Cybercrime and Cyberwar in Organizations and Society
  - Cyber Security Impact on value creation of Organizations
  - Challenges of the adoption of emerging technologies
  - Integration of Security in the general context of Orgnaization's risk and control enviroment and alignement with the IT governance and management
- Threats, vulnerabilities and risks related to Cyber Security in Organizations:
  - Vulnerabilities and categorization of cyber-threats
  - The importance of the systemic approaches to the analysis of cyber-risks
  - Overview of cyber-risks: Organizational Risk; Social risks; Technical risks.
- Overview and use of governance management and control enablers related with of Cyber Security: principles, policies and frameworks; processes; Organizational structures; Culture, ethics and behavior; Information artefacts; Services, infrastructure and applications; and People and skills.
- Development and implementation of Security Goals and metrics for management and alignment with the IT related goals and enterprise goals
- Challenges related with risk and Security roles in Organizations (eg. CIO, CISO, CSO)
- Case studies and implementation scenarios for strategies, programs and frameworks for the governance, management, risk and control.

MÉTODO

- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD

- Lectures and labs.
- Project in a team.

AVALIAÇÃO

A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION

The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS

TBD (to be defined)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
COBIT 5 Framework	ISACA	2012	www.isaca.org	Book
COBIT 5 for Information Security	ISACA	2012	www.isaca.org	Book
Implementing Cybersecurity Guidance for Small and Medium-Sized Enterprises	ISACA	2015	www.isaca.org	Book
Cybersecurity Guidance for Small and Medium-Sized Enterprises	ISACA	2015	www.isaca.org	Book
Transforming Cybersecurity using COBIT 5	ISACA	2014	www.isaca.org	Book
Advanced Persistent Threats: How to Manage the Risk to Your Business	ISACA	2013	www.isaca.org	Book
Responding to Targeted Cyber-attacks	ISACA	2013	www.isaca.org	Book
Cybersecurity: What the Board of Directors Needs to Ask	ISACA, IIA	2014	www.isaca.org	Whitepaper

European Cybersecurity Audit/Assurance Program	ISACA,	2014	www.isaca.org	Whitepaper
European Cybersecurity Implementation: Assurance	ISACA	2014	www.isaca.org	Whitepaper

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
NA

11.5.2 Compliance and Legal Aspects

Área Científica: TBC
Grupo: TBC
Nome: Conformidade e Aspectos Legais da Ciber-segurança
Name: Compliance and Legal Aspects
Acrónimo: CALC
Nível: Formação (F)
Estruturante: Não

CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Organizacional
Período: 6º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 15 horas
Aulas de Problemas (TP) ou Laboratório (PL): 15 horas
Trabalho autónomo: 54 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Abordar os aspectos de conformidade legal e normativa relacionados com a Ciber-segurança nas Organizações, nomeadamente: o cibercrime; enquadramento legal e normativo do digital no contexto nacional, europeu e global; os desafios de gestão da privacidade da informação; realização de auditorias (ex. forenses); e processo de certificação em normativos internacionais relacionados com o risco, ciber-segurança e continuidade (ex. EU's Data Protection Directive, ISO/IEC 27001:2013, PCI DSS, ISO 22301:2012).

GOALS
Address legal and regulatory compliance requirements related to the Security and Cyber Security in Organizations, particularly: Cybercrime, legal and regulatory frameworks of the digital context (national, European and global), information privacy management challenges, audits (e.g. Forensic Audits), and certification process in international standards related with risk, information security, cyber security and continuity/resilience (e.g. EU's Data Protection Directive, ISO / IEC 27001: 2013, PCI DSS, ISO 22301: 2012).

COMPETÊNCIAS
A unidade curricular desenvolve as seguintes competências:

- Identificar os requisitos legais, regulamentares, organizacionais e outros aplicáveis para gerir o risco de não conformidades.
- Avaliar as políticas, normas e procedimentos de segurança e privacidade e o alinhamento com as boas práticas de referência e requisitos legais e normativos.
- Avalias o desenho, implementação, manutenção e monitorização dos processos de classificação de dados e procedimentos para alinhamento com as políticas, normas e procedimentos da Organização e requisitos externos aplicáveis.
- Planeamento de auditorias específicas para determinar se os sistemas são protegidos, controlados e contribuem para a criação de valor na organização.
- Realizar auditorias de acordo com as normas de auditoria de sistemas de informação.

COMPETENCIES

The unit covers the following competecnies:

- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Evaluate security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.
- Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- Conduct audits in accordance with IS audit standards.

REQUISITOS
Nenhum.

REQUIREMENTS
None.

PROGRAMA
A unidade curricular cobre as seguintes temáticas:

- Introdução ao contexto legal e normativo (Portugal, Europa e Global):
    - Entidades reguladoras, supervisoras e outras instituições relevantes no contexto do risco e segurança
    - Enquadramento legal e normativo relacionado com o digital
    - Leis e normas de referência relacionadas com a segurança e privacidade da informação (ex. EU's Data Protection Directive)
- Processos de certificação em normas relacionadas com o risco, segurança e continuidade
    - Visão geral dos normativos internacionais relacionados com o risco, ciber-segurança e continuidade (ex. EU's Data Protection Directive, ISO/IEC 27001:2013, PCI DSS, ISO 22301:2012)
    - Implementação de um SGSI (Sistema de Gestão de Segurança da Informação) de acordo com a NP ISO/IEC 27001:2013 e *roadmap* para a certificação
- Realização de auditorias no contexto da segurança
    - Princípios gerais de auditoria e *standards* de referência
    - Realização de Auditorias forenses

PROGRAM
The unit covers the following topics:

- Introduction to the legal and regulatory context (Portugal, Europe and Global):
    - Regulatory and supervisory authorities and other relevant institutions in the context of risk and cybersecurity
    - Legal and regulatory context related to digital
    - Laws and industry standards related to security and privacy (eg. EU's Data Protection Regulation)
- Certitication processes related with risk, security and continuity standards
    - Overview of international standards related to risk, cyber security and continuity (eg EU's Data Protection Regulation, ISO / IEC 27001:. 2013, PCI DSS, ISO 22301: 2012)
    - Implementation of an ISMS (Information Security Management System) according to the NP ISO / IEC 27001: 2013, and roadmap for certification
- Conducting audits in the security context
    - General principles of auditing and reference standards
    - Forensic Audits

MÉTODO

- Aulas teóricas e aulas de laboratório.
- Projeto em grupo.

METHOD

- Lectures and labs.

- Project in a team.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Projeto (50%), e Exame final (50%).

EVALUATION
The evaluation results from the following combination of components: Project (50%), and Final exam (50%).

DOCENTES / TEACHERS
TBD (to be defined)

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
ITAF - Information Technology Assurance Framework	ISACA	2014	www.isaca.org	Standards, Guidelines, Tools and Techniques

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
NA

11.6 Módulo de Seminários

Como complemento, o curso prevê um conjunto de seminários que se destinam a acrescentar conhecimentos em áreas importantes da aplicação da segurança informática nos sistemas de informação nas organizações.

Estes seminários são ministrados em dois dias da semana e têm, normalmente, a duração de uma hora.

O ensino ministrado combina teoria e prática, e habilita os alunos a compreenderem em profundidade como se passa dos conceitos à ação.

11.6.1 Seminários

Área Científica: Sistemas de Informação
Grupo: Arquitetura e Gestão de Sistemas de Informação
Nome: Seminários
Name: Seminars
Acrónimo: SEM
Nível: Formação (F)
Estruturante: Não
CONTEXTO
Grupo: Ciber-Segurança > 3º Ciclo > Obrigatória
Módulo: Organizacional
Período: 1º - 6º Mês

CARGA HORÁRIA
Aulas Teóricas (T): 0 horas
Aulas de Problemas (TP) ou Laboratório (PL): 0 horas
Trabalho autónomo: 40 horas
Seminários (S): 48 horas
Créditos ECTS: 3 (84 horas)

OBJETIVOS
Convidar especialistas, académicos e/ou profissionais, para cobrir todos os temas relevantes na área do curso que, por várias razões, podem não estar abrangidos por nenhuma das outras unidades curriculares, ou que as complementam através de casos concretos em organizações existentes.

GOALS
Invite experts, academics and / or practioners, to cover all relevant issues in the area of the program that, for various reasons, may not be covered by any of the other courses, or may complement them by providing real-world examples.

COMPETÊNCIAS
Após a conclusão da UC os alunos terão competências para conhecer todos os temas relevantes, em particular os mais actuais, na área do curso.

COMPETENCIES
Upon unit completion, students will have the competencies to understanding all the relevant issues, in particular the most current in the area of the program.

REQUISITOS
Nenhum.

REQUIREMENTS
None.

PROGRAMA
Exemplos de temas que serão abordados nesta disciplina:

- Segurança na nuvem.
- Segurança nas bases de dados.
- Segurança forense.
- Detecção de ataques.
- Políticas de segurança multi-instituição.
- Segurança de sistemas industriais
- Segurança de Informação na perpsetiva operacional (material classificado, etc.)
- Gestão de incidentes/equipas CSIRT
- Criptografia na era da computação quântica
- Computação com dados cifrados (cifras homomórficas)
- Aspectos éticos, comportamentais e organizacionais da segurança informática

PROGRAM
The unit covers the following topics:

- Cloud security.
- Database security.
- Cyber-forensics.
- Attack detection.
- Multi-organization security policies.
- Secure criptography with quantum computing.
- Computing with encrypted data.
- Ethical, behavioral and organizational aspects of cyber-security.

MÉTODO

- Apresentações com discussão.
- Relatórios críticos sobre as apresentações.

METHOD

- Presentations with discussion.
- Critical reports on the presentations.

AVALIAÇÃO
A avaliação é composta pelo seguinte conjunto de componentes: Apresentações com discussão (20%), e Relatórios críticos sobre as apresentações (80%).

EVALUATION
The evaluation results from the following combination of components: Presentations with discussion (20%), and Critical reports on the presentations (80%).

DOCENTES / TEACHERS
Especialistas, académicos e/ou profissionais.
Experts, academics and / or practioners.

BIBLIOGRAFIA / BIBLIOGRAPHY

Título	Autor(es)	Ano	Referência	Tipo
Artigos vários	Vários autores.	na	(ACM, IEEE, Gartner, etc.)	Principal

SOFTWARE E CONFIGURAÇÂO / SOFTWARE CONFIGURATION
A definir.

12 Coordenação do Curso

O funcionamento deste curso decorre sob a responsabilidade científica e pedagógica dos órgãos competentes do IST, o Conselho Científico e o Conselho Pedagógico.

A gestão operacional do curso decorrerá sob a direção de uma Comissão Coordenadora, constituída por um dos Professores proponentes do DFA, designado pelo Departamento de Engenharia Informática, tendo em consideração as opiniões dos Departamentos de Engenharia Eletrotécnica e de Computadores e do Departamento de Matemática e pelo coordenador da PGP do DEI.

A comissão Coordenadora é apoiada, na tomada de decisões específicas, por uma Comissão Científico-Pedagógica, constituída por 2 Professores designados pelo Departamento de Engenharia Informática, 1 Professor designado pelo Departamento de Engenharia Eletrotécnica e de Computadores, 1 Professor designado pelo Departamento de Matemática, e 1 Professor escolhido de entre os Docentes do IST responsáveis pelas UCs do curso.

As propostas de evolução curricular, as proposta de admissão dos alunos bem como a apreciação da avaliação dos QUCs, apresentadas pela CC, são matérias sobre as quais a CCP do curso tem necessariamente que se pronunciar.

13 Regimes de Frequência

Como já foi referido anteriormente, este curso poderá ser oferecido segundo dois regimes de funcionamento alternativos, visando populações discentes distintas: i) regime presencial contínuo e intensivo, ou ii) regismo misto, presencial/á distância, a tempo parcial. Em qualquer dos regimes, os aspetos relacionados com procedimentos de organização interna estão resumidos no manual de procedimentos correspondente.

13.1 Regime Presencial

No regime presencial contínuo e intensivo, o curso de Ciber-Segurança está organizado em seis meses sequenciais, ocorrendo duas disciplinas por mês, tendo cada disciplina, aulas teóricas e práticas duas vezes por semana (ver detalhes sobre as disciplinas na secção própria). Assim, como exemplo, se as aulas começarem em Setembro de 2016, terminam em Fevereiro de 2017.

As sessões das unidades curriculares decorrem nas manhãs e tardes de segunda a sexta-feira de acordo com o esquema seguinte.

Horas	2ª feira	3ª feira	4ª feira	5ª feira	6ª feira
09:00 – 10:00	Estudo				
10:30 – 12:30	Aula Teórica				
13:00 – 13:30	Almoço				
14:00 – 14:30	Trabalho				
15:00 – 17:00	Aula Prática				
17:30 – 18:00	Revisão	Revisão	Seminário	Seminário	Revisão

13.2 Regime Misto

No regime misto, o calendário específico será organizado em moldes a determinar tendo em conta, obviamente, o cumprimento dos ECTS de cada unidade curricular, e experiências anteriores como é o

caso do regime CEPEI do IST (PCEPEI - Programa de Cursos de Especialização Profissional em Engenharia Informática do DEI, aprovado por unanimidade pelo CC do IST em 7 de Julho de 2015), potenciando assim novos graus de liberdade dos alunos na escolha do regime de frequência mais adequado às suas circunstâncias.[1]

Assim, por exemplo, será possível que os alunos frequentem grupos de unidades curriculares que se constituem como vectores de especialização (assim designados no PCEPEI). Cada vector de especialização (VE) é composto por, no mínimo, três UCs, com 3 créditos ECTS cada. A proposta de definição da composição e do conteúdo destes VE compete ao Conselho Coordenador da Pós-Graduação Profissional (CCPGP) do DEI que as submeterá para homologação ao Conselho Científico (CC) do IST. Portanto, os alunos poderão obter os ECTS correspondentes a um ou mais VEs, o que lhes permite posteriormente, completando os ECTS necessários, concluir com sucesso o curso de Ciber-Segurança. A conclusão com sucesso de um dado VE é reconhecida pela menção específica dos respetivos VEs no diploma de DFA do curso de Ciber-Segurança. Poderão existir VEs que requeiram um número mais elevado de UCs para a atribuição do respectivo subtítulo no DFA.

Como exemplo de VEs, podemos considerar os seguintes (sem prejuízo de outros poderem vir a ser propostos):

- Especialista em **Mobile Software Security**
    - Fundamentals of Computer Security
    - Application Software Security
    - Mobile Application Security

- Especialista em **Web, Cloud and Database Software Security**
    - Fundamentals of Network Security
    - Network Software Security
    - Web, Cloud and Database Security

- Especialista em **Test and Development of Secure Software for Organizations**
    - Software Security Testing
    - Secure Software Development Process
    - Organizational Security
    - Compliance and Legal Aspects

Os VEs acima indicados permitem que os alunos obtenham os respectivos diplomas de especialista; em acréscimo, estes mesmos VEs permitem obter os ECTS necessários para prossecução do curso de Ciber-Segurança. Como exemplo, podemos considerar o seguinte percurso de um aluno, em regime misto:
- dispensa de efectuar o Módulo Propedêutico por equivalência obtida às respectivas Ucs tendo em conta os conhecimentos do aluo em causa;
- frequência das Ucs do vector **Mobile Software Security** obtendo o respectivo título de especialista assim como os ECTS correspondentes de acordo com o curso DFA de Ciber-Segurança;
- frequência das Ucs do vector **Web, Cloud and Database Software Security** obtendo o respectivo título de especialista assim como os ECTS correspondentes de acordo com o curso DFA de Ciber-Segurança;
- frequência das Ucs do vector **Test and Development of Secure Software for Organizations** obtendo o respectivo título de especialista assim como os ECTS correspondentes de acordo com o curso DFA de Ciber-Segurança.

Portanto, através do percurso aqui exemplificado, um aluno pode obter o DFA em Ciber-Segurança de forma faseada, frequentando as Ucs dos vectores acima indicados em regime misto, obtendo os respectivos títulos de Especialista e ECTS. Este percurso aqui ilustrado, exemplifica a flexibilidade de funcionamento do regime misto sem comprometer a qualidade do curso oferecendo assim resposta às necessidades do mercado.

[1] Decisão CC-2015-07-07: Aprovado por unanimidade parecer favorável do Conselho Científico relativamente ao regime geral de enquadramento do DFA-EI - Programa de Formação Avançada em Engenharia Informática .

14 Docentes

Os docentes das UC integram o quadro do Instituto Superior Técnico, estando, na sua maioria, muito ligados à Investigação e Desenvolvimento mantendo, por isso, uma ligação às empresas.

Assim, as aulas são ministradas tendo em atenção dois aspetos, uma sólida componente teórica que se combina com a prática, habilitando a compreensão dos conceitos e a passagem destes para a acção.

Os docentes cujo CV se apresenta em seguida têm os conhecimentos e experiência adequada a leccionar o curso de Ciber-Segurança; existem outros no DEI que são igualmente adequados e que poderão juntar-se à equipa docente. Obviamente, a disponibilidade dos docentes aqui indicados está dependentente da efectiva realização deste curso em dias/horas a determinar posteriormente.

As secções seguintes apresentam o Currículo Vitae de cada docente.

14.1 Carlos Caleiro

Nome: Carlos Caleiro

Área Científica: Matemática, Lógica e Computação

Página Web: http://sqig.math.ist.utl.pt/carlos.caleiro

FORMAÇÃO ACADÉMICA

PhD in Mathematics, IST – Univ. Técnica de Lisboa, December 2000.

INTERESSES CIENTÍFICOS

Logic and applications; Security protocols; Temporal logic, concurrency and distribution; Abstract deductive systems.

UC ENSINADAS (ÚLTIMOS 5 ANOS)

Elementos de Programação (LMAC, MEBiom); Matemática Discreta (LEIC); Teoria da Computação (LEIC); Criptografia e Protocolos de Segurança (MMA, MEIC); Introdução à Computabilidade, Complexidade e Criptografia (MSIDC); Lógica Cleística (DMat); Lógica Funcional e Teoria da Demonstração (DMat, DSegInfo).

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)

C. Caleiro, J. Marcos, M. Volpe. Bivalent semantics, generalized compositionality and analytic classic-like tableaux for finite-valued logics. Theoretical Computer Science 603:84–110, 2015.

S. Marcelino, C. Caleiro, P. Baltazar. Deciding theoremhood in fibred logics without shared connectives. In A. Buchsbaum, A. Koslow, editors, The Road to Universal Logic – Volume 2, p. 387–406. Studies in Universal Logic, Springer, 2015.

A. Mordido, C. Caleiro. An equation-based classical logic. In V. de Paiva, R. de Queiroz, L. Moss, D. Leivant, A. de Oliveira, editors, Logic, Language, Information and Compu- tation (WoLLIC 2015), volume 9160 of Lecture Notes in Computer Science, p. 38–52. Springer Verlag, 2015.

C. Caleiro, R. Gonçalves. Abstract valuation semantics. Studia Logica 101(4):677–712, 2013.

C. Caleiro, L. Viganò, M. Volpe. On the mosaic method for many-dimensional modal logics: a case study combining tense and modal operators. Logica Universalis 7(1):33– 69, 2013.

B. Conchinha, D. Basin, C. Caleiro. Symbolic probabilistic analysis of off-line guessing. In J. Crampton, S. Jajodia, K. Mayes, editors, Computer Security - European Symp. on Research in Computer Security (ESORICS 2013), volume 8134 of Lecture Notes in Computer Science, p. 363–380. Springer Verlag, 2013.

C. Caleiro, J. Marcos. Many-valuedness meets bivalence: Using logical values in an effective way. Journal of Multiple-Valued Logic and Soft Computing 19(1–3):51–70, 2012.

M. Volpe, J. Marcos, C. Caleiro. Classic-like cut-based tableau systems for finite- valued logics. In L. Ong, R. de Queiroz, editors, Logic, Language, Information and Computation (WoLLIC 2012), volume 7456 of Lecture Notes in Computer Science, p. 321–335. Springer Verlag, 2012.

D. Basin, C. Caleiro, J. Ramos, L. Viganò. Distributed temporal logic for the analysis of security protocol models. Theoretical Computer Science 412(31):4007–4043, 2011.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)

GeTFun: Generalizing Truth-Functionality (2013–2016, ongoing) Project Marie Curie 318986 FP7-PEOPLE-2012-IRSES Research Executive Agency (REA), EU FP7.

14.2 Carlos Ribeiro

Nome: Carlos Ribeiro

Área Científica: Ciber Security

Página Web: www.gsd.inesc-id.pt/~cnr

FORMAÇÃO ACADÉMICA

PhD in Computer Engineering in July 2002, MSc in Electrical Engineering in July 1993, both by Instituto Superior Técnico, Universidade Técnica de Lisboa.

INTERESSES CIENTÍFICOS

He is currently Associate Professor in the Department of Electrical and Computer Engineering, and researcher at INESC-ID. His research has been focused on Network Security. More specifically in the design of security protocols for authentication, e-voting and e-payment, and on the design of solutions to detect attacks to critical infrastructures.

UC ENSINADAS (ÚLTIMOS 5 ANOS)

- Forensic Cyber Security in MSc METI and MSc CESIDB
- Computer and Network Security in MSc METI and MSc MEIC
- Security Protocols for Distributed Systems in PhD DEIC and PhD DEASegInf)
- Operating Systems in BSc LEIC
- Programming in MSc MEEC and MSc MEAer

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)

- D. Antunes, J. Lima, G. Pereira, N. Escravana, C. Ribeiro, NFC4Sure: Mobile ticketing system, 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), 26-27 Feb. 2016, Gainesville, FL, USA
- D. Oliveira and C. Ribeiro, An IDS for Browser Hijacking, The 9th SECURWARE 2015 - International Conference on Emerging Security Information, Systems and Technologies, Aug. 2015
- D Oliveira and C. Ribeiro, Local Password Validation Using Self-Organizing Maps, ESORICS'2014, Sep. 2014
- H. Rodrigues, R. José, A. Coelho, A. Melro, M. Ferreira, M. Monteiro and C. Ribeiro, MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC, Sensors, 14(8), pp. 13389-13415, Jul. 2014, MDPI.
- J. Lima and C. Ribeiro, BPIDS--Using business model specification in intrusion detection,17th International symposium on RAIDS, Gothenburg, Sweden, Sep 17-19,. 2014
- R. Joaquim, C. Ribeiro, An Efficient and Highly Sound Voter Verification Technique and its Implementation, E-Voting and Identity, Sep. 2012 , Springer

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)

Stork 2.0 – (2012-2015) was a project funded by the EC, with more than 50 partners from 19 MS.Its goal was to extend a Pan-European authentication platform to allow, among others, operations on behalf of a legal person, e.g., companies, organizations, associations.

SECUR-ED (2012-2015) was a project funded by the EC that intended to contribute to the security of European public transport systems relying on the performance of several pilots in the major European cities. The resulted intrusion detection tool has been national patented, and is pending for an international patent.

MobiPag – (2011-2013) was a project funded under the National Strategic Reference Framework (NSRF), run between 2011 and 2013 .The goal of the project was to build a platform for mobile payments that could be exploited by a number of companies in the industrial and financial fabric of the country. The platform conforms to the latest standards but has differentiating competitive factors, including security against attacks to mobile computing systems (phones, pDAs , etc.).

14.3 José Tribolet

Nome: José Manuel Nunes Salvador Tribolet
Área Científica: Sistemas de Informação
Página Web: https://sites.google.com/a/josetribolet.com/josetribolet/

FORMAÇÃO ACADÉMICA
Licenciou-se em Engenharia Electrotécnica, pelo Instituto Superior Técnico (IST), em 1971, com classificação final de 18 valores. A partir de 1972 frequentou o Massachussetts Institute of Technology (MIT), onde, em Janeiro de 1975 obteve o grau de "Master of Science in Electrical Engineering", e em Junho de 1977, obteve o grau de "Doctor of Science on Electrical Engineering and Computer Science. Obteve o grau de Agregado em Engenharia Elecrotécnica, no IST, em 1979. Frequentou, como Visiting Sloan Fellow, uma Pós-Graduação em Sistemas de Informação Empresariais, na Sloan School of Management, do MIT, de Setembro de 1997 a Junho de 1998.

INTERESSES CIENTÍFICOS
Engenharia, Arquitectura e Governação Empresarial, Arquitectura dos Sistemas de Informação, Engenharia dos Processos de Negócio, Estratégia e Sistemas de Informação e Engenharia do Conhecimento, Organização e Gestão da Função Informática, Transformação Organizacional e Gestão da Mudança.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Introdução à Engenharia Informática (1º Semestre, LEIC/IST)
Engenharia Organizacional (2º Semestre, DEIC/IST)
Seminário de Informação e Sistemas Empresariais (Ead) (1º Semestre, MISE, IST/UAb)
Arquitectura Organizacional de Sistemas de Informação (MEIC-A, MEIC-T, IST)
Projecto em Engenharia e Gestão Industrial (2011/2012, 2 Semestre, MEGI)
Arquitectura Empresarial (POSIE3, DEI/IST)

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
- Value-Oriented Specification of Service Systems: Modeling the Contribution Perspective of Enterprise Networks, João Pombinho and David Sardinha Andrade de Aveiro and José Manuel Nunes Salvador Tribolet, International Journal of Information Systems in the Service Sector (IJISSS), 7(1), pp. 60-81, Jan. 2015, IGI Global.

- Strategy essentials: organizational simulators, Carlos Páscoa , Nelson Ferreira , José Tribolet, The Learning Organization 2013 20:6 , 358-376, Emerald Publishers.

- The discipline of enterprise engineering, Jan LG Dietz and Jan AP Hoogervorst and Antonia Albani and David Aveiro and Eduard Babkin and Artur Caetano and Philip Huysmans and Junichi Iijima and Steven JH Van Kervel and Hans Mulder and Martin Op't Land and Henderik A Proper and Jorge Sanz and Linda Terlouw and José Manuel Nunes Salvador Tribolet and Jan Verelst and Robert Winter, International Journal of Organisational Design and Engineering, 3(1), pp. 86-114, Jan. 2013, Inderscience Publishers.

- Applying the principle of separation of concerns to business process design, Artur Caetano and António Rito Silva and José Manuel Nunes Salvador Tribolet, International Journal of Organisational Design and Engineering, Special Issue on Enterprise Engineering, 2(3), pp. 250-270, Nov. 2012, Inderscience.

- GOD-theory for organizational engineering: continuously modeling the continuous (re)Generation, Operation and Deletion of the enterprise, David Sardinha Andrade de Aveiro and António Rito Silva and José Manuel Nunes Salvador Tribolet, International Journal of Internet and Enterprise Management: Special Issue on Enterprise Systems Modeling and Simulation, 7(1), pp. 64-83, Jan. 2011.

- A "context aware" and agent-centric perspective for the alignment between individuals and organizations, Marielba Zacarias and H. Sofia Pinto and Rodrigo Magalhães and José Manuel Nunes

Salvador Tribolet, Information Systems Journal - Vocabularies, Ontologies and Rules for Enterprise and Business Process Modeling and Manag, 35(4), pp. 441-466, Jun. 2010, Elsevier Science Publisher.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)

Assessoria ao Programa de Arquitectura, Desenvolvimento e Operacionalização do novo Portal BASE das Compras Públicas online, para o INCI.

Assessoria ao Programa de Arquitetura, Desenvolvimento e Operacionalização do futuro Sistema das Compras Públicas on line, nacioal e europeu para o INCI/IMPIC e para a ESPAP.

Acompanhamento activo do PGETIC da AP Central, na qualidade de Conselheiro Científico.

Avaliação Preliminar da Situação dos Sistemas de Informação do Ministério da Justiça, para o IGFEJ.

14.4 Luis Veiga

Nome: Luís Antunes Veiga
Área Científica: Arquiteturas e Sistemas Operativos
Página Web: http://www.gsd.inesc-id.pt/~lveiga/

FORMAÇÃO ACADÉMICA
Doutoramento em Engenharia Informática e de Computadores, Instituto Superior Técnico, 2007
Mestrado em Engenharia Electrotécnica e de Computadores - Ramo Informática e Computadores (pré-Bolonha), Instituto Superior Técnico, 2001
Licenciatura em Engenharia Informática e de Computadores (pré-Bolonha), Instituto Superior Técnico, 1998

INTERESSES CIENTÍFICOS
Sistemas distribuídos, virtualização, computação grid e cloud, sistemas peer-to-peer, middleware

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Plataformas para Aplicações Distribuídas na Internet, MEIC-T/METI, 1.º ano
Ambientes Virtuais de Execução, MEIC-A, 1.º ano
Técnicas Avançadas de Virtualização, DEIC, 1.º ano

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
José Simão and Luís Veiga, Partial Utility-driven Scheduling for Flexible SLA and Pricing Arbitration in Cloud, article in IEEE Transactions on Cloud Computing, 2015, IEEE

Sérgio Esteves and João Nuno de Oliveira e Silva and Joao P. Carvalho and Luís Veiga, Incremental Dataflow Execution, Resource Efficiency and Probabilistic Guarantees with Fuzzy Boolean Nets, article in Journal of Parallel and Distributed Computing (JPDC), 2015, Elsevier

Luis Pina and Luís Veiga and Michael Hicks, Rubah: DSU for Java on a stock JVM, presented at ACM Conference on Object-Oriented Programming Languages, Systems, and Applications (OOPSLA 2014), Sep. 2014, ACM

Leila Sharifi and Navaneeth Rameshan and Felix Freitag and Luís Veiga, Energy Efficiency Dilemma: P2P-cloud vs. mega-datacenter (Best-Paper Candidate), presented at IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom 2014), 2014

José Simão and Luís Veiga, Flexible SLAs in the Cloud with Partial Utility-driven Scheduling (Best-Paper Award Runner-up), presented at IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom 2013), Dec. 2013, IEEE

João Pedro Marques Silva and José Simão and Luís Veiga, Ditto – Deterministic Execution Replayability-as-a-Service for Java VM on Multiprocessors, presented at ACM/IFIP/Usenix International Middleware Conference (Middleware 2013), Dec. 2013, Springer.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Projecto Europeu FP7 Timbus - membro da equipa INESC-ID Lisboa.

14.5 Miguel Correia

Nome: Miguel Pupo Correia
Área Científica: Cyber-Security and Dependability
Página Web: http://www.gsd.inesc-id.pt/~mpc/

FORMAÇÃO ACADÉMICA
PhD in Informatics, Universidade de Lisboa, Faculdade de Ciências (2003); MSc in Electrotechnical and Computing Engineering, Universidade Técnica de Lisboa, Instituto Superior Técnico (1995); Engineering degree in Electrotechnical and Computing Engineering, Universidade Técnica de Lisboa, Instituto Superior Técnico (1991)

INTERESSES CIENTÍFICOS
cyber-security, cloud computing, software security, big data analytics for security, critical infrastructure protection, distributed systems, machine learning for security, intrusion tolerance

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Software Security
Security and Network Management
Intrusion Tolerance, Detection and Response
Computer Networks

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
Ibéria Medeiros, Nuno F. Neves, Miguel Correia. Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining. IEEE Transactions on Reliability, 65(1):54–69, March 2016.

N. Bessani, M. Correia, B. Quaresma, F. André, P. Sousa, DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. ACM Transactions on Storage, vol. 9, n. 4, Nov. 2013.

Ibéria Medeiros, Nuno F. Neves, Miguel Correia. DEKANT: A Static Analysis Tool that Learns to Detect Web Application Vulnerabilities. In Proceedings of the IEEE International Symposium on Software Testing and Analysis (ISSTA), Jul. 2016.

Ibéria Medeiros, Nuno F. Neves, Miguel Correia. Equipping WAP with WEAPONS to Detect Vulnerabilities. In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Jun. 2016.

Ibéria Medeiros, Miguel Beatriz, Nuno Neves and Miguel Correia. Hacking the DBMS to Prevent Injection Attacks. In Proceedings of the 6th ACM Conference on Data and Application Security and Privacy, March 2016.

Dário Nascimento, Miguel Correia. Shuttle: Intrusion Recovery for PaaS. In Proceedings of the 35th International Conference on Distributed Computing Systems (ICDCS), Jun.-Jul. 2015.

Daniel Gonçalves, João Bota, Miguel Correia. Big Data Analytics for Detecting Host Misbehavior in Large Logs. In Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Aug. 2015.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Projecto Europeu H2020 Safe Cloud - Secure and Resilient Cloud Architecture - coordenador da equipa INESC-ID Lisboa.

14.6 Nelson Escravana

Nome: Nelson Escravana
Área Científica: Information critical infrastructure protection
Página Web: https://www.linkedin.com/in/escravana

FORMAÇÃO ACADÉMICA
Computer Science Engineering 5 year BSc from Instituto Superior Técnico, Technical University of Lisbon (2002). Management post-graduation from Instituto Superior de Economia e Gestão, Technical University of Lisbon (2011).

INTERESSES CIENTÍFICOS
Intrusion detection, information critical infrastrcuture protection, industrial control systems, offensive security.

ARTIGOS RELEVANTES (ÚLTIMOS 5 ANOS)
Diogo Antunes, João Lia, Gonçalo Pereira, Nelson Escravana, Carlos Ribeiro, NFC4Sure: Mobile ticketing system, 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), 26-27 Feb. 2016, Gainesville, FL, USA

T.Fall, J.Lima, N.Escravana, "SECUR-ED cybersecurity roadmap for Public Transport Operators", 2014.
Lima, Joao, Nelson Escravana, and Carlos Ribeiro. "BPIDS-Using Business Model Specification in Intrusion Detection." Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, Setembro 17-19, 2014, Proceedings. Vol. 8688. Springer, 2014.

João Lima, Nelson Escravana, "Sistema e método para produção automática de software vulnerável através da injeção de código vulnerável durante o processo de compilação ou interpretação". Pedido de patente nacional nº PT#106777, INPI, 2014.

João Lima, Nelson Escravana, "Effectively detection of intrusions using business process specifications", 2013 FIRST/TF-CSIRT Technical Colloquium, 2013, Lisbon.

João Lima, Nelson Escravana, Carlos Ribeiro, "Detecção de Intrusões aplicada à infraestrutura TI das Redes de Transportes", Revista Nação e Defesa do Instituto de Defesa Nacional, 2012.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Estudos:
"SG-195 – Cyberdefense information sharing", NATO/NIAG, Dezembro 2015;
"SG-179 – Industrial contribution to cyber defence action plan", NATO/NIAG, 2014;
Nelson Escravana, John Rodrigues, "Parecer sobre o Projeto de implantação de um Centro Nacional de Ciber-segurança realizado pela Comissão de Instalação do CNC", GPTIC-Presidência do Concelho de Ministros, 2012;
"SG-165 – Private Sector support to NATO cyber defence", (National Focal Poin) NATO/NIAG, 2012.

Projectos:
2015-2018, **DOGANA**, H2020-653618, directly addresses the complexity stemming from the human dimension of attacks and aims to deliver solutions to help enterprises manage the risks associated with social engineering
2015 – NFC4SURE – development of NFC ticketing solution for public transportation.
2014-2017, **ECOSSIAN** (European Control SystemSecurity Incident Analysis Network) FP7- SEC-607577. The mission of ECOSSIAN is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities.
2011-2014, **SECUR-ED** (Secured Urban Transportation – European Demonstration) FP7- SEC-261605. The SECUR-ED project was a demonstration project with an objective to provide a set of tools to improve urban transport security.

14.7 Nuno Santos

Nome: Nuno Miguel Carvalho Santos
Área Científica: Security and Trusted Computer Systems
Página Web: http://www.gsd.inesc-id.pt/~nsantos/index.html

FORMAÇÃO ACADÉMICA
PhD in Computer Science from the Saarland University / Max Planck Institute for Software Systems (MPI-SWS), since November 2013.

MSc (2006) and BSc (2001) are both from Instituto Superior Técnico (Technical University of Lisbon) in Electrotechnical Engineering.

INTERESSES CIENTÍFICOS
He is currently Assistant Professor in Instituto Superior Técnico at the Department of Computer Science and Engineering. His research interests focus on the area of security and trusted computer systems. In recent work, he has built several systems aimed at improving trust in cloud, enterprise, and mobile platforms. This was achieved by leveraging trusted computing hardware, namely Trusted Platform Module (TPM) and ARM TrustZone technology. At IST, he has been teaching several courses related with the scientific area of Architecture and Operating Systems.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Operating Systems (2nd year, LEIC)
Computer Organization (3 year, LEIC)
Mobile Computing (MEIC/METI)
Forensic Cibersecurity (MEIC/METI/MSIDC)

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
A Case for Enforcing App-Specific Constraints to Mobile Devices by Using Trust Leases
Nuno Santos, Nuno O. Duarte, Miguel B. Costa, Paulo Ferreira
Proceedings of HotOS, 2015

Using ARM TrustZone to Build a Trusted Language Runtime for Mobile Applications
Nuno Santos, Himanshu Raj, Stefan Saroiu, and Alec Wolman
Proceedings of ASPLOS, 2014

Enhancing the OS against Security Threats in System Administration
Nuno Santos, Rodrigo Rodrigues, and Bryan Ford
Proceedings of Middleware, 2012

Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services
Nuno Santos, Rodrigo Rodrigues, Krishna P. Gummadi, and Stefan Saroiu
Proceedings of USENIX Security, 2012

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Development of Termite, a distributed testbed for emulation of WiFi Direct networks of Android devices. Termite is in active development and used in lab classes at IST by the students of Mobile Computing course since 2013.

14.8 Paulo Mateus

Nome: Paulo Mateus
Área Científica: Matemática, Lógica e Computação
Página Web: http://sqig.math.ist.utl.pt/paulo.mateus

FORMAÇÃO ACADÉMICA
PhD in Mathematics IST – Univ. Técnica de Lisboa, 2001
Agregação (Habilitation) in Mahtematics - IST – Univ. Técnica de Lisboa, 2006

INTERESSES CIENTÍFICOS
Quantum cryptography and computation
Security protocols
Temporal and probabilistic logics

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Computação e Programação (MEBiol,, LEMat, MEQ, MEAmbi) (LEIC)
Algoritmos e Modelação Computacional (LAMC, MEBiom)
Criptografia e Protocolos de Segurança (MMA, MEIC)
Lógica e Verificação de Modelos (MEIC, MMA)
Computação, Informação e Lógica Quânticas (DMat, DSegInfo)
Teoria da Computabilidade, Complexidade e Informação (DFisica, DSegInfo)

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
M. Biscaia, D. Henriques, and P. Mateus. Decidability of approximate Skolem problem and applications to logical verification of dynamical properties of Markov chains. ACM Transactions on Computational Logic, 16(1):4, 2015.

D. Qiu, L. Li, P. Mateus, and A. Sernadas. Exponentially more concise quantum recognition of non-RMM regular languages. Journal of Computer and System Sciences, 81(2):359--375, 2015.

J. Ribeiro, A. Souto, and P. Mateus. Quantum blind signature with an offline repository. International Journal of Quantum Information, 13(2):1550016, 2015.

Souto, P. Mateus, P. Adão, and N. Paunkovic. Bit-string oblivious transfer based on quantum state computational indistinguishability. Physical Review A, 91(4):042306, 2015.

X. Zou, D. Qiu, S. Zhang, and P. Mateus. Semiquantum key distribution without invonking the classical party's measurement capability. Quantum Information Processing, 14(8):2981--2996, 2015.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
QBigD: Quantum Big Data – IT Internal Project (SQIG – PIA) 2016-2018

CVQuantum: Continuous Variable Cryptography – IT Internal Project (SQIG OT Aveiro) 2013-2016.

PQuantum: Practical Quantum Cryptography – IT Internal Project (SQIG OT Aveiro) 2013-2016.

Trebaruna – GNS project 2009-2012 – private funding.

14.9 Paulo Ferreira

Nome: Paulo Jorge Pires Ferreira
Área Científica: Distributed Operating Systems
Página Web: https://fenix.tecnico.ulisboa.pt/homepage/ist12958

FORMAÇÃO ACADÉMICA
"Agregação" since November 2009 from Instituto Superior Técnico (Technical University of Lisbon) in Electrotechnical Engineering.

PhD from the Université Pierre et Marie Curie (1996) in Systemes Informatiques with equivalence from the Technical University of Lisbon in Engenharia Informática e de Computadores (1997).

MSc (1992) and BSc (1988) are both from Instituto Superior Técnico (Technical University of Lisbon) in Electrotechnical Engineering.

INTERESSES CIENTÍFICOS
He is currently Associated Professor with "Agregação" in Instituto Superior Técnico at the Department of Computer Science and Engineering where he has been teaching courses within the scientific area of Architecture and Operating Systems, at both undergraduate and graduate levels, including Operating Systems, Mobile Computing, Middleware for Distributed Internet Applications, and Advanced Distributed Systems. His research interest are distributed systems, mobility, large-scale and security.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Operating Systems (2º year, LEIC)
Mobile Computing (1º year, MEIC)
Advanced Distributed Systems (PhD)
Applications and Services on the Internet (IST and ISUTC, Maputo) – Two-week intensive course taught in Maputo (equivalent to a full semester).
Middleware (DFA POSTIT)

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
Termite: Emulation Testbed for Encounter Networks. Rodrigo Bruno, Nuno Santos, Paulo Ferreira. 12th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS 2015), July 22–24, 2015 Coimbra, Portugal.

A Case for Enforcing App-Specific Constraints to Mobile Devices by Using Trust Leases. Nuno Santos, Nuno O. Duarte, Miguel B. Costa, Paulo Ferreira. 15th Workshop on Hot Topics in Operating Systems. (HotOS XV), May 18-20, 2015, Kartause Ittingen, Switzerland.

AnonyLikes: Anonymous quantitative feedback on social networks. Pedro Alves, Paulo Ferreira. ACM/IFIP/USENIX 14th International Middleware Conference 2013, Dec. 2013 , Beijing (China), ACM.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Design and development of a software tool for extracting dependencies in the Windows operating system (withing a EU project FP7/2007-2013 under grant agreement Nº. 269940).

Design and development of an automatic registration of students attendance to classes allowing the use of mobile devices by the students.

14.10 Pedro Adão

Nome: Pedro Adão
Área Científica: Segurança e Criptografia
Página Web: http://web.ist.utl.pt/pedro.adao/

FORMAÇÃO ACADÉMICA
PhD in Mathematics from Instituto Superior Técnico, Technical University of Lisbon (2006). BSc in Applied Mathematics and Computation, Major in Computer Science from Instituto Superior Técnico, Technical University of Lisbon (2002).

INTERESSES CIENTÍFICOS
Pedro Adão is an Assistant Professor at the Department of Computer Science and Engineering of Instituto Superior Técnico (IST) and a researcher from Instituto de Telecomunicações. He has also been visiting researcher at the Centre de Recherche Commun INRIA-Microsoft Research, Paris, France. His major research interests are Mathematical Foundations of Cryptography, Specification and Verification of Cryptographic Protocols, and ``Physical" and ``Day-life" Cryptography. Pedro Adão is a faculty member of the FCT-Doctoral Programme in the Physics and Mathematics of Information. He currently leads the Security Team@Tecnico initiative, a team of students that participates in security-related competitions. He is also member of the ICT COST Action IC1306, Cryptography for Secure Digital Interaction. He is the General Chair of IEEE Computer Security Foundations Symposium for the years of 2016 and 2017.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Foundations of Programming (1st year, LEIC)
Introduction to Algorithms and Data Structures (1st year, LEIC)
Software Quality (1st year, MEIC)
Software Specification (1st year, MEIC)
Computational Models in Security (PhD Program in Information Security)
Security Engineering (PhD Program in Information Security)

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
Pedro Adão, Riccardo Focardi, Joshua D. Guttman, and Flaminia L. Luccio. *Localizing Firewall Security Policies.* In Proceedings of CSF'16 Lisboa, Portugal, 2016. IEEE Computer Society Press.

André Souto, Paulo Mateus, and Pedro Adão and Nikola Paunkovic. *Bit-String Oblivious Transfer Based on Quantum State Computational Distinguishability.* Physical Review A, 91(4):042306, 2015.

Pedro Adão, Paulo Mateus, and Luca Viganò. *Protocol Insecurity with a Finite Number of Sessions and a Cost-Sensitive Guessing Intruder is NP-Complete*. Theoretical Computer Science, 538:2–15, 2014.

Pedro Adão, Claudio Bozzato, Gian-Luca Dei Rossi, Riccardo Focardi, and Flaminia L. Luccio. Mignis: *A Semantic Based Tool for Firewall Configuration*. In Proceedings of CSF'14, Vienna, Austria, 2014. IEEE Computer Society Press.

Pedro Adão, Riccardo Focardi, and Flaminia L. Luccio*. Type-Based Analysis of Generic Key Management APIs*. In Proceedings of CSF'13, New Orleans, LA, USA, 2013. IEEE Computer Society Press.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Pedro Adão has led the FCT-funded project ComFormCrypt on secure abstractions of cryptography, and currently he is the co-leader of the FCT-funded project Confident. He is also member of the ICT COST Action IC1306, Cryptography for Secure Digital Interaction.

14.11 Ricardo Chaves

Nome: Ricardo Jorge Fernandes Chaves
Área Científica: Distributed Operating Systems
Página Web: https://fenix.tecnico.ulisboa.pt/homepage/ist143817

FORMAÇÃO ACADÉMICA
PhD from the Technical University of Delft (TUDelft) and from the University of Lisbon (IST) in "Secure Computing on Reconfigurable Systems" (2007). MSc (2003) and BSc (2001) are both from Instituto Superior Técnico (Technical University of Lisbon) in Electronics and Computer Engineering.

INTERESSES CIENTÍFICOS
Ricardo Chaves is an assistant professor at the Computer Science Department at the University of Lisbon/IST and a researcher at the Signal Processing Group (SiPS) of INESC-ID. He is also a senior member of IEEE.

His research interests are focused on cryptography systems, reconfigurable hardware architectures, and on embedded and user oriented systems, in which he has published more than 50 papers in international journals and conferences, with more than 700 citations on Google Scholar, with an h-index of 14. Supervised more than 25 MSc student and one PhD student.

Professionally, he is the vice coordinator of the embedded lab of INESC-ID and the scientific coordinator of the Signal Processing Group. He is an active member of HiPEAC3 and is in the Management Committee of EU COST Actions TRUDEVICE and CRYPTARCUS (of which he is the vice-leader of WG3). Is a technical adviser for the Portuguese National Security Cabinet (since 2008). As also server in the program committee and track chair of several international conferences.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Computer Organization (3rd year, LEIC); Network and Computer Security (1st year, MEIC); Architectures for Embedded Computing (1st year, MEIC); Applications and Implementation of Security Systems (1st year, METI);
Applications and Implementations of Cryptographic Algorithms (1st year, MERC); Operating Systems (2º year, LEIC);
Network Security (IST and ISUTC, Maputo) – Two-week intensive course taught in Maputo (equivalent to a full semester).

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
Ricardo Chaves, Leonel Sousa, Nicolas Sklavos, Apostolos P. Fournaris, Georgina Kalogeridou, Paris Kitsos and Farhana Sheikh. Circuits and Systems for Security and Privacy, chapter Secure Hashing: SHA-1, SHA-2, and SHA-3, CRC Press, February 2016.

João Resende and Ricardo Chaves. Compact Dual Block AES core on FPGA for CCM Protocol, In International Conference on Field Programmable Logic and Applications, pp. 228-235, London, UK, September 2015.

Ricardo Chaves, et. al. Challenges in Designing Trustworthy Cryptographic Co-Processors, In International Symposium on Circuits and Systems, pp. 2009-2012, May 2015.

João Amaral, Francesco Regazzoni, Pedro Tomás and Ricardo Chaves. Accelerating Differential Power Analysis on Heterogeneous Systems, In 9th Workshop on Embedded Systems Security, New Delhi, India, October 2014.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
He is also involved in several ongoing project European projects, such as EMC2 (focused on critical computational systems) and Rethink (the future of peer-to-peer internet). As also participated in several other European and National project (FARNuSyC, Threads, Mobipag, HELIX, Sideworks, SCryBAM, CORTIVIS, Safira).

14.12 Rodrigo Rodrigues

Nome: Rodrigo Miragaia Rodrigues
Área Científica: Arquitetura e Sistemas Operativos
Página Web: https://fenix.tecnico.ulisboa.pt/homepage/ist14022

FORMAÇÃO ACADÉMICA
Licenciado em Engenharia e Informática e de Computadores pelo Instituto Superior Técnico (1998)
Doctor of Philosophy in Computer Science pelo Massachusetts Institute of Technology (2005)

INTERESSES CIENTÍFICOS
Sistemas concorrentes e distribuídos, fiabilidade dos sistemas computacionais.

UC ENSINADAS (ÚLTIMOS 5 ANOS)
Arquitetura de computadores (Mestrado Integrado em Engenharia Informática - Universidade Nova de Lisboa). 2012-2014
Algoritmos e Sistemas Distribuídos (Mestrado Integrado em Engenharia Informática - Universidade Nova de Lisboa). 2012-2015
Programa de Introdução à Investigação Científica em Engenharia Informática (Mestrado Integrado em Engenharia Informática - Universidade Nova de Lisboa). 2013-2015
Sistemas transacionais (Doutoramento em Informática - Universidade Nova de Lisboa). 2012-2014

ARTIGOS CIENTÍFICOS RELEVANTES (ÚLTIMOS 5 ANOS)
Valter Balegas, Sergio Duarte, Carla Ferreira, Rodrigo Rodrigues, Nuno Preguica, Mahsa Najafzadeh and Marc Shapiro. Putting Consistency back into Eventual Consistency. In Proceedings of the Tenth European Conference on Computer Systems (EuroSys 2015).

Anjo Vahldiek-Oberwagner, Eslam Elnikety, Aastha Mehta, Deepak Garg, Peter Druschel, Rodrigo Rodrigues, Johannes Gehrke and Ansley Post. Guardat: Enforcing data policies at the storage layer. In Proceedings of the Tenth European Conference on Computer Systems (EuroSys 2015).

Pedro Fonseca, Rodrigo Rodrigues, Bjoern Brandenburg. SKI: Exposing Kernel Concurrency Bugs through Systematic Schedule Exploration. In Proc. of the 11th Usenix Symposium on Operating Systems Design and Implementation (OSDI 2014).

Nuno Santos, Rodrigo Rodrigues, Bryan Ford. Enhancing the OS Against Security Threats in System Administration. In the 13th ACM/IFIP/USENIX International Middleware Conference (Middleware'12).
Cheng Li, Daniel Porto, Allen Clement, Johannes Gehrke, Nuno Preguica, and Rodrigo Rodrigues. Making Geo-Replicated Systems Fast as Possible, Consistent when Necessary. In the 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI '12).

Nuno Santos, Rodrigo Rodrigues, Krishna P. Gummadi, Stefan Saroiu. Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services. In the 21st USENIX Security Symposium (USENIX Security '12).

Rodrigo Rodrigues, Barbara Liskov, Kathryn Chen, Moses Liskov, and David Schultz. IEEE Transactions on Dependable and Secure Computing, vol.9, no.2, pp.145-158, March-April 2012.

PROJETOS DE ENGENHARIA (ÚLTIMOS 5 ANOS)
Alguns sistemas resultantes da investigação dos artigos acima citados foram disponibilizados e tiveram impacto prático. Por exemplo, o sistema SKI para teste de sistemas operativos foi usado por programadores do sistema operativo Linux.