Imprimir livro

Plano da Unidade Curricular

Sítio:	PlataformAbERTA	Impresso por:	Luís Pereira
Unidade curricular:	Segurança em Redes e Computadores 2025 (Espaço Central)	Data:	terça-feira, 7 outubro 2025, 20:49
Livro:	Plano da Unidade Curricular		

Descrição

Documento com o PUC desta unidade curricular.

Índice

PUC - Plano da Unidade Curricular

PUC

1. A Unidade Curricular

2. Competências

3. Roteiro

4. Metodologia

5. Recursos

6. Avaliação
6.1. Cartão de Aprendizagem
6.2. Calendário de avaliação contínua
6.3. Exame

7. Plano de Trabalho
7.1. Tópico 1
7.2. Tópico 2
7.3. Tópico 3

PUC - Plano da Unidade Curricular

UNIDADE CURRICULAR 21181

PUC
Plano de Unidade Curricular
UNIVERSIDADE AbERTA
www.uab.pt

Docente(s): José **Henrique S. Mamede**
Ano Letivo: 2025/2026

PUC

O que é o PUC?

O PUC constitui um documento que visa orientar o processo de aprendizagem do estudante ao longo da Unidade Curricular a que se refere. É por isso um guião que requer uma leitura atenta e que lhe será útil ao longo de todo o percurso de aprendizagem. Aqui encontrará informação sobre as temáticas a estudar, as competências a desenvolver, informações sobre como se organiza o processo de aprendizagem, como utilizar e tirar partido do espaço virtual relativo a esta Unidade Curricular, o que se espera de si, como é avaliado, entre outros aspetos fundamentais para realizar da melhor forma este percurso.

1. A Unidade Curricular

Apresentação da Unidade Curricular

Num mundo em rede, as questões associadas à segurança informática assumem um grau de importância extremo.

Interessa formar profissionais capazes de lidar com a problemática dos diversos aspectos da segurança informática, criando competências para o projecto e a implementação de mecanismos suficientes para lidar com as diferentes ameaças. Importa, assim, apresentar os conceitos centrais sobre segurança informática, com foco na segurança em redes e em computadores e propiciar os meios para o desenvolvimento académico da área.

2. Competências

Competências a desenvolver

Pretende-se que, no final desta Unidade Curricular, o estudante tenha adquirido as seguintes competências:

- Reconhecer a importância da segurança informática no contexto atual da sociedade de informação;
- Dominar os conceitos centrais relacionados com a transmissão segura de dados;
- Arquitetar e implementar mecanismos eficientes para lidar com as principais ameaças à segurança de redes de computadores.

3. Roteiro

Roteiro de conteúdos a trabalhar

Nesta Unidade Curricular serão trabalhadas as seguintes temáticas:

Tema 1	Introdução à Segurança Informática
Tema 2	Noções Básicas de Criptografia
Tema 3	Segurança em Redes

4. Metodologia

Como vamos trabalhar?

Indicações gerais sobre a metodologia de trabalho a adotar, tendo em conta os destinatários, e a especificidade da unidade curricular em causa, a exemplo de:

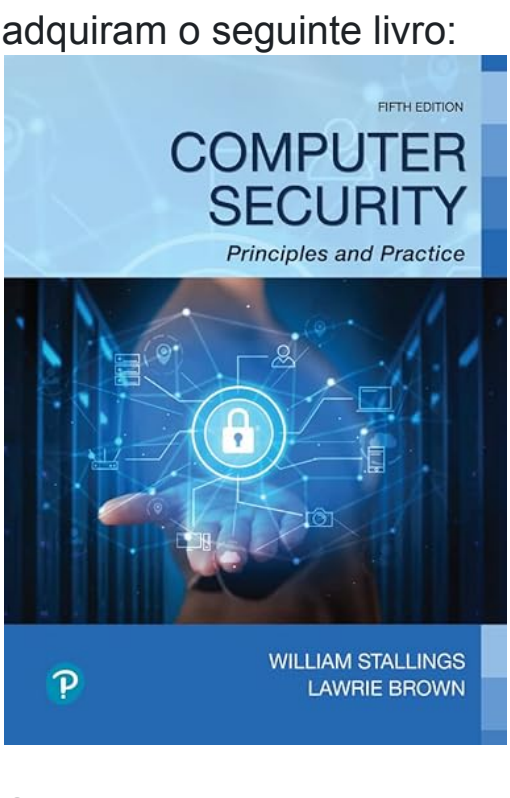
Esta UC é um pouco diferente das demais pelo simples facto de ter apenas 2 ECTS. Apesar disso, o modelo de trabalho colaborativo assíncrono é idêntico e baseado nos princípios estabelecidos pelo Modelo Pedagógico Virtual da Universidade Aberta (MPV). A bases de sustentação deste trabalho assíncrono são os fóruns de discussão, suportando as interações professor-estudante, bem como as estudante-estudante.
Em cada temática, o estudante começará pelas leituras dos recursos recomendados e, caso aplicável, pela instalação dos recursos de software que suportam a experimentação laboratorial das matérias. No decurso das leituras, à medida que surgem temas que considere de relevo ou que suscitem dúvidas, deve colocar as mesmas no fórum da temática, sendo que deve também apoiar os demais colegas nas suas intervenções nesse mesmo fórum, criando-se espaços de debate, moderados pelo professor.
Em cada temática existirão atividades formativas (AF) que permitirão ao estudante aferir os seus conhecimentos, obtidos das leituras, das discussões no fórum, bem como da experimentação laboratorial. Estas questões formativas devem ser amplamente debatidas, por todos, no fórum, sendo que o professor irá criar uma *thread* por cada AF.

Por fim, existem marcadas várias sessões síncronas que permitirão o esclarecimento de questões de uma forma mais célere. Se necessário, além das sessões previamente agendadas, poderão ser marcadas outras por conveniência dos trabalhos.

5. Recursos

Bibliografia e outros recursos

Bibliografia
Apesar de serem disponibilizados vários textos que cobrem a matéria da Unidade Curricular, recomenda-se que os alunos adquiram o seguinte livro:



Stallings, W., Brown, L. (2024). *Computer Security: Principles and Practice*. 5th Edition (Global Edition), Pearson.

Outros Recursos:

Disponibilizados pelo professor em cada módulo.

6. Avaliação

Como vai ser a avaliação?

A avaliação assume o regime de avaliação contínua. Os estudantes que não possam seguir esta modalidade de avaliação podem optar pela realização de um Exame Final.

A opção pelo regime de avaliação (contínua ou final) será feita pelo estudante até ao final da **3ª semana letiva**, não podendo ser alterada no decurso do semestre.

Os estudantes que optem pela avaliação contínua disporão de um **Cartão de Aprendizagem**, pessoal, onde será creditada a avaliação que forem efetuando ao longo do semestre. O Cartão de Aprendizagem é um instrumento personalizado e cada estudante tem acesso apenas ao seu cartão.

Os estudantes que optem pela realização de um Exame Final terão acesso a todas as orientações dadas na plataforma e/ou na WISEflow e às Atividades Formativas disponibilizadas ao longo do percurso de aprendizagem, mas não aos instrumentos de avaliação utilizados no regime de avaliação contínua - *E-fólios e e-fólio global*. Estes estarão disponíveis apenas para os estudantes que optem pela modalidade de
avaliação contínua.

A entrega do e-fólio global ou do exame é realizada na plataforma WISEflow em https://pt.wiseflow.net/aberta.
Os estudantes terão a oportunidade de selecionar, no início de cada semestre, se pretendem realizar a prova remotamente ou num centro de exames.
Informação atempada sobre os procedimentos de realização de provas na plataforma Wiseflow será remetida, diretamente para os estudantes, ao longo do semestre, pela Universidade Aberta.

6.1. Cartão de Aprendizagem

Avaliação Contínua

UNIVERSIDADE AbERTA
www.uab.pt
CARTÃO DE APRENDIZAGEM

Os estudantes que optarem pela avaliação contínua creditam no seu Cartão de Aprendizagem – CAP – as classificações que obtiveram com a realização de vários trabalhos ao longo do semestre e a classificação obtida no e-fólio global realizado no final do semestre.

Ao longo do semestre ser-lhes-á proposto que elaborem pequenos trabalhos, designados ***E-fólios***. A realização do conjunto dos e-fólios poderá levar à creditação do seu cartão (CAP) de um máximo de 8 valores.

À classificação obtida nos ***E-fólios*** juntam-se os valores obtidos na prova final, designada ***e-fólio global***, com duração de 90m com um período adicional de tolerância, que será submetida online na WISEflow. Esta terá a cotação global de 12 valores.

No sistema de avaliação contínua, a classificação final na unidade curricular corresponde ao somatório das classificações obtidas em cada *e-fólio* e no *e-fólio global*.

Um ***E-fólio*** é um pequeno documento digital elaborado de forma pessoal e incidindo sobre uma secção dos temas trabalhados.

O ***e-fólio global*** consiste num trabalho que complementa os e-fólios.

A entrega do e-fólio global é realizada na plataforma WISEflow em https://pt.wiseflow.net/aberta.
A aprovação na Unidade Curricular implica que o estudante obtenha um mínimo de 3.5 valores no conjunto dos ***E-fólios*** e um mínimo de 5.5 valores no ***e-fólio global***.

6.2. Calendário de avaliação contínua

Calendário de avaliação contínua

[O quadro seguinte deverá ser preenchido de acordo com o planeamento efetuado; ter em conta o número de *e-fólios* previstos e a valorização máxima de cada um ao preencher o quadro e as datas correspondentes ao semestre em questão.]

	Outubro	Novembro	Dezembro	Janeiro
E-fólio A [4 valores]				
Data da especificação do trabalho a realizar no *E-fólio A* e dos respetivos critérios de avaliação		Data: 03/11		
Envio do *E-fólio A* ao professor		Data: 17/11		
Indicação da classificação do *E-fólio A*			Data: 05/12	
E-fólio B [4 valores]				
Data da especificação do trabalho a realizar no *E-fólio B* e dos respetivos critérios de avaliação			Data: 09/12	
Envio do *E-fólio B* ao professor				Data: 22/12
Indicação da classificação do *E-fólio B*				Data: 09/01
e-fólio Global [12 valores]				
Realização				Data: [consultar datas oficiais das provas]

6.3. Exame

Opção pelo Exame

O **Exame Final** traduz-se numa única prova realizada na WISEflow e classificada numa escala de 0 (zero) a 20 (vinte) valores.

Esta prova tem um caráter somativo, reportando-se à totalidade dos conteúdos abordados na unidade curricular e é realizada no final do semestre letivo, tendo a duração de 120m com um período adicional de tolerância.

O estudante que optar pela modalidade de exame final, terá de obter nota igual ou superior a 9.5 valores.

A entrega do exame é realizada na plataforma WISEflow em https://pt.wiseflow.net/aberta.

7. Plano de Trabalho

Calendário e plano de trabalho

Este *Plano* apresenta a previsão da distribuição temporal das várias Temáticas de estudo, das atividades e respetivas orientações de trabalho, de modo a que possa planear, organizar e desenvolver o seu estudo. Esta informação é complementada por orientações que deverá consultar com regularidade nesta *Sala de Aula Virtual*.

7.1. Tópico 1

Mês 1

Semana da UC	O que se espera do estudante
1ª Semana	Comece por consultar as indicações dadas na sala de aula virtual relativamente ao Tópico 1. Ler as secções 1.1. (Computer Security Concepts) e 1.2. (Threats, Attacks and Assets) do manual de apoio. Discutir os conceitos com os colegas no fórum e tentar entender as perspetivas de cada um sobre o tema. Utilizar as questões formativas para responder e discutir com colegas e professor no fórum.
2ª Semana	Ler as secções 1.3. (Security Functional Requirements) e 1.4. (Fundamental Security Design Principles) do manual de apoio. Discutir os conceitos com os colegas no fórum. Utilizar as questões formativas para responder e discutir com colegas e professor no fórum.
3ª Semana	Indique ao professor até final desta 3ª semana a sua opção de avaliação: Avaliação Contínua ou Exame Final. Para isso, responda ao questionário "Decisão sobre a Avaliação", no espaço desta sala de aula virtual. Ler as secções 1.5. (Attack Surfaces and Attack Trees) e 1.6. (Computer Security Strategy) do manual de apoio. Discutir os conceitos com os colegas no fórum. Verificar se consegue responder a todas as questões formativas. Analise e reflita sobre todos os *posts* colocados no fórum.

7.2. Tópico 2

Mês 2

Semana da UC	O que se espera do estudante
4ª Semana	Inicie o estudo relativo à temática da criptografia e dos diferentes tipos de métodos criptográficos, essenciais para a transmissão segura de mensagens. Estude a secção 2.1. (Confidentiality with Symmetric Encryption). Coloque as suas questões no fórum e discuta com os colegas.
5ª Semana	Consulte as indicações no Fórum "Avaliação Contínua" relativas à elaboração do e-fólio A Prossiga no estudo dos métodos criptográficos. Estude a secção 2.2. (Message Authentication and Hash Functions). Utilizar as questões formativas para responder e discutir com colegas e professor no fórum.
6ª Semana	Prossiga no estudo dos métodos criptográficos. Estude a secção 2.3. (Public-Key Encryption). Discutir os conceitos com os colegas no fórum.
7ª Semana	Estudar a secção 2.4. (Digital Signatures and Key Management). Utilizar as questões formativas para responder e discutir com colegas e professor no fórum.
8ª Semana	Terminar o estudo dos métodos criptográficos. Aproveite para rever a matéria como um todo. Discutir os conceitos com os colegas no fórum. Consolidar o conhecimento sobre os métodos criptográficos estudados, analisando as questões formativas e as respostas dos colegas.

7.3. Tópico 3

Mês 3

Dezembro / Maio	O que se espera do estudante
9ª Semana	Inicie o estudo relativo à temática da segurança em redes de computadores. Consulte as indicações no Fórum "Avaliação Contínua" relativas à elaboração do e-fólio B. Leia todo o capítulo 6 (Malware) do livro de texto (da secção 6.1 à secção 6.10) Coloque as suas dúvidas no fórum e debata com os colegas e professor.
10ª Semana	Leia todo o capítulo 7 (Denial-of-Service Attacks) do livro de texto (da secção 7.1 à secção 7.7) Coloque as suas dúvidas no fórum e debata com os colegas e professor.
11ª Semana	Leia todo o capítulo 8 (Intrusion Detection) do livro de texto (da secção 8.1 à secção 8.5) Coloque as suas dúvidas no fórum e debata com os colegas e professor.
12ª Semana	Leia todo o capítulo 9 (Firewalls and Intrusion Prevention Systems) do livro de texto (da secção 9.1 à secção 9.6) Coloque as suas dúvidas no fórum e debata com os colegas e professor.
13ª Semana	Discutir os conceitos com os colegas no fórum e tentar entender as perspetivas de cada um sobre o tema. Consolidar os conhecimentos, utilizando as questões formativas. Fazer uma revisão total das matérias.