REFERENCIAL DE FORMAÇÃO

EM VIGOR

Nível de Qualificação: 5

Área de Educação e Formação	**481 . Ciências Informáticas**
Código e Designação do Referencial de Formação	**481344 - Técnico/a Especialista em Cibersegurança**
Modalidades de Educação e Formação	**Cursos de Especialização Tecnológica**
Total de pontos de crédito	**102,00** **(inclui 15 pontos de crédito da Formação Prática em Contexto de Trabalho)**
Publicação e atualizações	Publicado no Boletim do Trabalho e Emprego (BTE) nº 6 de 15 de fevereiro de 2016 com entrada em vigor a 15 de fevereiro de 2016.
Observações	

1. Organização do Referencial de Formação

Formação Geral e Científica		
Código	**UFCD**	**Horas**
5064	Matemática	50
0683	Ética e deontologia profissionais	25
3769	Probabilidades e estatística	50
5065	Empresa - estrutura e funções	25

Total de Pontos de Crédito da Formação Geral e Científica: 15

Formação Tecnológica				
Código [1]	**Nº**	**UFCD obrigatórias**	**Horas**	**Pontos de crédito**
5117	1	Primeiros conceitos de programação e algoritmia e estruturas de controlo num programa informático	25	2,25
9187	2	Legislação, segurança e privacidade	25	2,25
5745	3	Inglês técnico	50	4,50
5089	4	Programação - Algoritmos	25	2,25
5410	5	Bases de dados - conceitos	25	2,25
5113	6	Sistema operativo cliente (plataforma proprietária)	25	2,25
5114	7	Sistema operativo servidor (plataforma proprietária)	25	2,25
5101	8	Hardware e redes de computadores	25	2,25
5102	9	Redes de computadores (avançado)	25	2,25
5104	10	Instalação de redes locais	50	4,50
5106	11	Serviços de rede	25	2,25
5892	12	Modelos de gestão de redes e de suporte a clientes	25	2,25
9188	13	Fundamentos de cibersegurança	25	2,25
9189	14	Tecnologias de análise de evidências	50	4,50
9190	15	Introdução à programação aplicada à cibersegurança	25	2,25
9191	16	Introdução às técnicas de análise de evidências	50	4,50
9192	17	Análise de vulnerabilidades – iniciação	50	4,50
9193	18	Análise de vulnerabilidades - desenvolvimento	50	4,50
9194	19	Introdução à cibersegurança e à ciberdefesa	50	4,50
9195	20	Enquadramento operacional da cibersegurança	50	4,50

Formação Tecnológica				
Código [1]	**Nº**	**UFCD obrigatórias**	**Horas**	**Pontos de crédito**
9196	21	Cibersegurança ativa	50	4,50
9197	22	Wargamming	50	4,50
		Total da carga horária e de pontos de crédito:	**800**	**72,00**

Formação em Contexto de Trabalho	Horas	Pontos de crédito
A componente de formação em contexto de trabalho visa, aplicar conhecimentos e saberes adquiridos às atividades práticas do respetivo perfil profissional e executar atividades sob orientação, utilizando as técnicas, os equipamentos e os materiais que se integram nos processos de produção de bens ou de prestação de serviços. Esta formação desenvolve-se em parceria, estabelecida entre a instituição de formação e empresas, outras entidades empregadoras, associações empresariais ou socioprofissionais entre outras, e pode adotar diferentes modalidades, designadamente estágios.	560	15

[1] Os códigos assinalados a laranja correspondem a UFCD comuns a dois ou mais referenciais, ou seja, transferíveis entre referenciais de formação.

2. Desenvolvimento das Unidades de Formação de Curta Duração (UFCD)

2.1. Formação Geral e Científica

5064	**Matemática**	50 horas

Objetivos	**1.** Explicar os conceitos básicos da matemática e estatística. **2.** Realizar operações algébricas em diferentes bases. **3.** Efectuar conversões entre bases. **4.** Representar e realizar operações com conjuntos. **5.** Definir álgebra de boole e utilizar as suas propriedades. **6.** Utilizar tabelas de verdade para identificar o valor lógico de proposições. **7.** Realizar operações com matrizes. **8.** Utilizar grafos para modelar e interpretar problemas. **9.** Explicar como as ferramentas matemáticas introduzidas se aplicam à informática. **10.** Analisar e identificar situações e métodos de cálculo a adotar perante problemas concretos.

Conteúdos

1. Operações com bases

1.1. Noção de base de um sistema de representação

1.2. Representação de um número em diferentes bases

1.3. Conversão entre bases

1.4. Conversões rápidas entre as bases 2, 8 e 16

1.5. Limitação de representação

1.6. Operações aritméticas na base 2

1.7. Representação em complemento para 2

2. Teoria de conjuntos, lógica e álgebra de boole

2.1. Representação de conjuntos, relação de pertença e inclusão de conjuntos

2.2. Operações sobre conjuntos: reunião, interseção, diferença e complementação

2.3. Definição e valor lógico de uma proposição

2.4. Cálculo proposicional: negação, conjunção, disjunção de proposições

2.5. Tabelas de verdade

2.6. Definição de álgebra de boole e exemplos

2.7. Propriedades de uma álgebra de boole

3. Matrizes e operações com matrizes

3.1. Matriz de um sistema linear e dimensão de uma matriz

3.2. Matriz linha e matriz coluna, matriz quadrada, matriz diagonal, matriz identidade e matriz simétrica

3.3. Operações com matrizes: adição de matrizes, produto de um escalar por uma matriz, transposição de matrizes, multiplicação de matrizes

4. Teoria dos Grafos

4.1. Definição de grafo (não orientado) e sua representação

4.2. Conceitos fundamentais: lacete, grafo simples, multigrafo, grafo conexo, grafo completo e grau de um vértice Caminhos de um grafo: caminho simples, caminho elementar, circuito e ciclo

4.3. Matriz de adjacência de um grafo

4.4. Potências da matriz de adjacência e resultados relevantes

5. Noções elementares de estatística

5.1. De que trata a estatística: a estatística como metodologia da investigação científica. Estudos observacionais e experimentais. A recolha, limpeza, resumo e apresentação dos dados. Populações e amostras, unidades amostrais e variáveis. A escala de Stevens. Noções elementares sobre amostragem e planeamento de experiências

5.2. Análise inicial de dados: exploração de dados univariados. Características amostrais. Representações gráficas. Exploração de dados bivariados. Noções elementares sobre regressão

5.3. Probabilidade e probabilidade condicional: noções de probabilidade; a axiomática de Kolmogorov e suas consequências. Probabilidade condicional. Probabilidade de uma cadeia e regra da multiplicação. Independência. O Teorema da Probabilidade Total e o Teorema de Bayes

0683	**Ética e deontologia profissionais**	25 horas
Objetivos	**1.** Reconhecer as exigências ética associadas à sua atividade profissional. **2.** Identificar os fatores deontológicos associados à sua atividade profissional. **3.** Reconhecer as suas próprias competências e funções. **4.** Reconhecer as exigências éticas e deontológicas em relação aos seus colegas de trabalho, à própria organização e ao público externo.	

Conteúdos

1. Exigências éticas

1.1. Discrição

1.2. Consciência dos valores hierárquicos

1.3. Sentido de disciplina

1.4. Disponibilidade

1.5. Pontualidade

1.6. Assiduidade

2. Factores deontológicos

2.1. Capacidade de organização

2.2. Sentido de antecipação

2.3. Capacidade de realização profissional

2.4. Boa cultura geral

2.5. Facilidade de expressão oral e escrita

2.6. Criatividade

2.7. Polivalência

2.8. Facilidade nas relações interpessoais

2.9. Sigilo profissional

2.10. Vivência do sentido da solidariedade social

2.11. Sentido da obrigação da competência

3. Exigências em relação a si próprio/a e às suas funções

3.1. Competências

3.2. Aptidões

3.3. Responsabilidade na tomada de decisões e acções

3.4. Uso dos conhecimentos e experiências no sentido da produtividade

3.5. Objectividade (análise racional dos factos)

4. Exigências em relação aos colegas de trabalho

4.1. Respeito pela dignidade da pessoa humana

4.2. Valorização pessoal e profissional dos colegas

4.3. Consideração por sugestões, problemas e necessidades dos outros

4.4. Exercício da liberdade com responsabilidade no trabalho

5. Exigências em relação à organização

5.1. Participação nos objetivos da organização

5.2. Promoção do desenvolvimento da imagem da organização

5.3. Uso correto de materiais e equipamentos

5.4. Discernimento de julgamento em eventuais situações de conflito

5.5. Sigilo profissional

6. Exigências em relação ao público externo

6.1. Respeito e confiança

6.2. Principio da livre concorrência

6.3. Comunicação bilateral

3769	**Probabilidades e estatística**	50 horas
Objetivos	**1.** Identificar os fundamentos gerais de estatística e de probabilidades.	

Conteúdos

1. Obtenção, análise e classificação de amostras

2. Tratamento estatístico de amostras (parâmetros estatísticos)

3. Intervalos de confiança

4. Conceito de probabilidade

5065	**Empresa - estrutura e funções**	25 horas
Objetivos	**1.** Definir e distinguir os conceitos de empresa e os elementos que a compõem. **2.** Identificar e caracterizar as funções internas à empresa. **3.** Identificar e diferenciar os tipos de estrutura organizacional. **4.** Identificar os princípios da comunicação organizacional.	

Conteúdos

1. Organização

1.1. Conceito e tipos

1.2. Dimensão

1.3. Propriedade

1.4. Ramos de actividade

2. Empresa

- **2.1.** Conceito
- **2.2.** Objectivos e papel na sociedade
- **2.3.** Elementos constitutivos

3. Funções

- **3.1.** Produção
- **3.2.** Comercial
- **3.3.** Pessoal
- **3.4.** Financeira
- **3.5.** Planeamento estratégico

4. Estrutura organizacional

- **4.1.** Conceito e tipos
- **4.2.** Representação gráfica
- **4.3.** Análise

5. Comunicação organizacional

- **5.1.** Conceito e tipo e intervenientes
- **5.2.** Regras e efeitos da comunicação
- **5.3.** Assertividade

2.2. Formação Tecnológica

5117	**Primeiros conceitos de programação e algoritmia e estruturas de controlo num programa informático**	25 horas
Objetivos	**1.** Apreender conceitos sobre a lógica de programação. **2.** Aplicar instruções e sequências lógicas na resolução de problemas. **3.** Utilizar as regras e as diferentes fazes na elaboração de um algoritmo. **4.** Desenhar fluxogramas. **5.** Identificar os diferentes tipos de dados. **6.** Identificar variáveis e constantes. **7.** Enumerar e identificar os operadores aritméticos, relacionais e lógicos. **8.** Utilizar operadores e funções pré-definidas. **9.** Conhecer vários tipos de variáveis. **10.** Compreender a estrutura de um programa. **11.** Conhecer estruturas de seleção e repetição. **12.** Utilizar e identificar instruções compostas. **13.** Desenvolver programas que utilizem combinações entre estruturas de repetição e de seleção. **14.** Compreender e aplicar saltos incondicionais. **15.** Realizar testes e correção de erros (executar o Play Computer).	

Conteúdos

1. Introdução à lógica de programação
   - 1.1. Lógica
   - 1.2. Sequência lógica
   - 1.3. Instruções
   - 1.4. Algoritmos
2. Desenvolvimento de algoritmos
3. Pseudocódigo
   - 3.1. Regras e fases de construção de um algoritmo
   - 3.2. Fluxogramas
     - 3.2.1. Introdução ao fluxograma
     - 3.2.2. Simbologia
4. Constantes, variáveis e tipo de dados
   - 4.1. Constantes
   - 4.2. Variáveis
   - 4.3. Tipos de dados
5. Operadores e funções pré-definidas
   - 5.1. Operadores aritméticos
   - 5.2. Operadores relacionais
   - 5.3. Operadores lógicos
   - 5.4. Funções pré-definidas
6. Instruções compostas
7. Estruturas de decisão
   - 7.1. Selecção simples
   - 7.2. Selecção composta
   - 7.3. Escolha múltipla
   - 7.4. Selecção encadeada
8. Estruturas de repetição
   - 8.1. Condicionais
   - 8.2. Incondicionais
9. Salto incondicional
10. Testes e correção de erros

9187	**Legislação, segurança e privacidade**	25 horas
Objetivos	1. Identificar os conceitos fundamentais de direitos, liberdades e garantias, internacionais e nacionais. 2. Identificar legislação nacional e comunitária de proteção de dados (LPDP). 3. Interpretar a legislação nacional sobre manuseamento de informação classificada (SEGNAC). 4. Interpretar a legislação nacional sobre cibercriminalidade.	

Conteúdos

1. Princípios da Declaração Universal dos Direitos Humanos
2. Direito de imagem
3. Princípios da Carta dos Direitos Fundamentais da União Europeia aplicados à cibersegurança
4. Princípios constitucionais da Constituição da República Portuguesa (CRP) e os preceitos constitucionais respeitantes aos direitos, liberdades e garantias
5. Conceitos de privacidade, dados pessoais e dados sensíveis
6. Conceitos nacionais e comunitários em matéria de administração eletrónica e proteção de dados
   - **6.1.** Direito de informação
   - **6.2.** Direito de acesso
   - **6.3.** Direito de oposição
   - **6.4.** Direito de retificação e eliminação
   - **6.5.** Código de Procedimento Administrativo
7. Conceitos nacionais e comunitários em matéria informação classificada
   - **7.1.** Princípio da necessidade de conhecer
   - **7.2.** Manuseamento
   - **7.3.** Classificação da informação
8. Conceitos de cibercrime
9. Conceitos de competências de investigação criminal em cibercriminalidade
10. Conceitos de normas processuais na investigação de cibercrimes

5745	**Inglês técnico**	50 horas
Objetivos	**1.** Ler e traduzir orientações técnicas, desenhos, normas e outros documentos técnicos no âmbito do contexto socioprofissional. **2.** Utilizar a língua inglesa na produção de textos a nível oral e escrito, adequando-a ao contexto socioprofissional. **3.** Utilizar a língua inglesa no âmbito das TIC.	

Conteúdos

1. Língua inglesa no quotidiano socioprofissional
2. Terminologia técnica em língua inglesa no âmbito do contexto socioprofissional
   - **2.1.** Aspectos formais do sistema linguístico inglês
   - **2.2.** Tradução e terminologia: entidades normalizadoras e o papel da terminologia nas comunidades profissionais
   - **2.3.** Tipos de textos associados ao contexto socioprofissional (ex.: normas nacionais/internacionais; manuais de instruções; estudos científicos/técnicos)
3. Língua inglesa e as novas tecnologias
   - **3.1.** Terminologia associada a *software* utilizado no contexto socioprofissional (ferramentas linguísticas *on-line;* bases de dados; comunicação mista – videoconferências, *chatroom)*
   - **3.2.** Terminologia associada aos meios utilizados no contexto socioprofissional
4. Metodologias de um trabalho de projeto em inglês

5089	**Programação - Algoritmos**	25 horas
Objetivos	**1.** Elaborar algoritmos em pseudocódigo. **2.** Construir fluxogramas referentes a algoritmos. **3.** Identificar tipos de dados abstratos. **4.** Utilizar estruturas de controlo de forma eficiente.	

Conteúdos

1. Conceitos básicos

- **1.1.** Noção de Algoritmo
- **1.2.** Representação de Algoritmos
- **1.3.** Variáveis e tipos de dados
- **1.4.** Expressões lógicas e aritméticas
- **1.5.** Estruturas de programação e controlo

2. Algoritmos recursivos em contraponto com algoritmos iterativos

3. Estruturas de dados elementares

- **3.1.** Tabelas
- **3.2.** Vectores
- **3.3.** Matrizes
- **3.4.** Pilhas
- **3.5.** Filas

4. Algoritmos de inserção, pesquisa e ordenação

5. Escolha de estruturas de dados, sua definição e utilização

5410	**Bases de dados - conceitos**	25 horas
Objetivos	**1.** Definir os conceitos fundamentais sobre a gestão da informação. **2.** Reconhecer a importância de uma correta gestão da informação. **3.** Analisar e estruturar a informação que vai alimentar uma base de dados relacional. **4.** Implementar o modelo relacional. **5.** Normalizar dados não normalizados. **6.** Descrever as regras que contribuem para a integridade da informação.	

Conteúdos

1. Bases de dados

- **1.1.** Conceito de dados
- **1.2.** Conceito de modelo de dados
- **1.3.** Arquitectura de uma base de dados

1.4. Ficheiros e bases de dados

1.5. Bases de dados relacionais

1.6. Arquitectura de um sistema gestor de base de dados

2. Modelo relacional

2.1. Estrutura de dados relacional

2.2. Regras de integridade do modelo

2.3. Gestão de dados do modelo relacional

3. Tabelas, registos, campos e chaves

4. Normalização

4.1. Representação na forma não normalizada

4.2. Tipo de notação *DeMarco*

4.3. Tipo de notação *Gane* e *Sarson*

4.4. Fases da normalização segundo *Codd*

4.5. Integridade da informação

5113	**Sistema operativo cliente (plataforma proprietária)**	25 horas
Objetivos	**1.** Efectuar o levantamento das necessidades de utilização e selecionar o sistema operativo cliente mais adequado. **2.** Instalar e configurar sistemas operativos clientes. **3.** Instalar e distinguir *device drivers* residentes e instaláveis. **4.** Configurar o sistema operativo cliente. **5.** Instalar os diversos componentes do sistema operativo.	

Conteúdos

1. Instalação e configuração de um sistema operativo

2. Particionamento e formatação do disco(s)

3. Opções de instalação

4. Optimização de recursos

5. Instalação de dispositivos e *device drivers*

6. Configuração do sistema de acordo com o *hardware* específico

7. Múltiplas configurações do sistema

8. Resolução de problemas

5114	**Sistema operativo servidor (plataforma proprietária)**	25 horas

Objetivos	**1.** Efectuar o levantamento das necessidades de utilização e selecionar o sistema operativo servidor mais adequado. **2.** Instalar sistema operativo servidor. **3.** Instalar e distinguir *device drivers* residentes e instaláveis. **4.** Configurar o sistema operativo servidor. **5.** Optimizar o sistema operativo. **6.** Efectuar *backup* e conhecer sistemas de proteção contra falhas. **7.** Definir e parametrizar utilizadores. **8.** Efectuar a gestão de recursos. **9.** Administrar as ferramentas. **10.** Instalar e configurar clientes de acordo com a configuração do servidor e da rede.

Conteúdos

1. Instalação do sistema operativo servidor

2. Optimização do sistema operativo servidor

3. *Backup* e sistemas de proteção contra falhas

4. Utilizadores – Criação e configuração de contas

5. Gestão de recursos

6. Ferramentas de administração

7. Instalação e configuração de clientes de acordo com a configuração da rede e do servidor

5101	**Hardware e redes de computadores**	25 horas
Objetivos	**1.** Conhecer os conceitos básicos relacionados com as redes de computadores, nomeadamente o que é e quais as tarefas de uma rede de computadores. **2.** Caracterizar as várias arquiteturas de redes de computadores. **3.** Caracterizar os modelos OSI e TCP/IP. **4.** Caracterizar equipamentos de rede de computadores. **5.** Caracterizar as tecnologias *Ethernet*, *Token Ring,* FDDI.	

Conteúdos

1. Introdução às redes de computadores

- **1.1.** Funcionalidades de uma rede de computadores
- **1.2.** Tarefas de uma rede de computadores
- **1.3.** Redes de dados e suas implementações
- **1.4.** Noção e classificação de redes de computadores

2. Modelo geral de comunicação

- **2.1.** Abordagem dos modelos por camadas

2.2. Origem, destino e pacotes de dados

3. O modelo OSI

3.1. Objectivo do modelo

3.2. Descrição das sete camadas do modelo

3.3. Encapsulamento de dados

4. O modelo TCP/IP

4.1. A importância do modelo

4.2. Descrição das camadas do modelo

4.3. Protocolos TCP/IP

4.4. Comparação entre o modelo OSI e o modelo TCP/IP

5. Redes de computadores locais (LANs)

5.1. Placas de rede

5.2. Meio físicos de transmissão de dados

5.3. Equipamentos usados em LANs: repetidores, *hubs, bridges, switches* e *routers*

5.4. Noção de segmento numa LAN

6. Topologias de redes

6.1. *Bus, ring, dual ring, star,* árvore, *mesh,* células *wireless*

7. Cablagem de redes

7.1. Cabo STP, UTP, coaxial e fibra óptica

7.2. Comunicações sem fios

7.3. Especificações TIA/EIA

7.4. Terminadores

7.5. Testes de cabos 10/100BaseTX

8. Componentes da camada 1 do modelo OSI

8.1. Fichas, tomadas, cabos *patch panels, transceivers,* repetidores e *hubs*

9. Colisões e domínios de colisões

9.1. Ambientes de partilha de meio físico

9.2. Sinais numa colisão

9.3. Acessos a meios partilhados

9.4. Acesso ao meio como domínios de colisão

10. Camada 2 do modelo OSI

10.1. Endereçamento MAC

10.2. Constituição das *frames*

10.3. Controlo de acesso ao meio

10.4. - Tecnologia *Token Ring*

10.5. Tecnologia FDDI

10.6. Tecnologias Ethernet e IEEE 802.3

10.7. Funções e operações de camada 2 das placas de rede, *bridges* e *switchs*

10.8. Segmentação do domínio de colisão através de *bridges, switchs* e *routers*

10.9. Detecção de avarias

11. Projecto de cablagem estruturada

11.1. Noções sobre planeamento do projecto

11.2. Instalação da cablagem (UTP)

11.3. Ligação dos cabos no *rack: patch panels* e *patch cables*

5102	**Redes de computadores (avançado)**	25 horas
Objetivos	**1.** Caracterizar as funções das camadas superiores do modelo OSI. **2.** Caracterizar e descrever o funcionamento de Routers. **3.** Realizar *subnetting* de redes. **4.** Caracterizar a interligação de redes. **5.** Utilizar os utilitários mais comuns de administração de redes locais.	

Conteúdos

1. A camada rede do modelo OSI

- **1.1.** *Routers* e portos de interfaces de *routers*
- **1.2.** Comunicações entre redes
- **1.3.** Conceitos sobre ARP e tabelas de ARP
- **1.4.** Protocolos de *routing*

2. A camada transporte do modelo OSI

- **2.1.** Objectivo da camada 4
- **2.2.** Protocolos TCP e UDP
- **2.3.** Métodos de conexão por TCP

3. *Routing* e endereçamento

- **3.1.** Determinação de caminhos no *routing* de pacotes
- **3.2.** Classes e endereços IP e endereços reservados
- **3.3.** *Network* ID e cálculo de *hots* por classe de IP
- **3.4.** Noção de *subnetting*
- **3.5.** Criação de *subnets*

4. Noções sobre as camadas de sessão e apresentação do modelo OSI

5. A camada de aplicação do modelo OSI

- **5.1.** Objectivo da camada 7
- **5.2.** Aplicações de rede
- **5.3.** Utilitários de administração de redes

5104	**Instalação de redes locais**	50 horas
Objetivos	**1.** Cravar e testar cabos RJ45 diretos e cruzados. **2.** Instalar cabos e equipamentos em bastidores. **3.** Instalar equipamentos ativos de rede com e sem fios.	

Conteúdos

1. Montagem de cablagem de redes estruturadas

2. Instalação de tomadas
3. Instalação e configuração de equipamento ativo de rede
   - **3.1.** Concentradores de rede de dados: hubs, switchs
   - **3.2.** Routers (interligação entre diversas redes de dados)
   - **3.3.** Bridges
   - **3.4.** Pontos de acesso a redes sem fios
   - **3.5.** Firewalls
   - **3.6.** Gateways de Voip

5106	**Serviços de rede**	25 horas
Objetivos	**1.** Caracterizar, instalar e configurar o serviço DHCP. **2.** Caracterizar, instalar e configurar o serviço DNS. **3.** Caracterizar, instalar e configurar serviços de routeamento de dados. **4.** Caracterizar, instalar e configurar servidores de páginas *web*.	

Conteúdos

1. Serviço DHCP
   - **1.1.** Funcionamento do DHCP
   - **1.2.** Instalação e configuração do DHCP: Utilização do DHCP Manager e manipulação de *scopes*
   - **1.3.** Clientes estáticos e reserva de endereços
   - **1.4.** Manutenção das configurações: *backups* e recuperações
2. Serviço DNS
   - **2.1.** Funcionamento do DNS
   - **2.2.** *Name space* e *zones*
   - **2.3.** Tipos de servidores DNS
   - **2.4.** Instalação e configuração do DNS: Utilização do DNS Manager, criação de zonas, adição de registos e
3. integração com o WINS
   - **3.1.** Configuração de clientes
     - **3.1.1.** Serviços de routeamento
     - **3.1.2.** Servidores de páginas *web*
   - **3.2.** Internet Information Server
   - **3.3.** Apache

5892	**Modelos de gestão de redes e de suporte a clientes**	25 horas
Objetivos	**1.** Identificar os modelos de gestão de redes. **2.** Aplicar as técnicas de suporte a clientes.	

Conteúdos

1. Modelo eTOM
2. Enquadramento
3. O Contexto das relações de negócio
4. O Modelo eTOM
5. ITIL
6. História e contexto de negócio do ITIL
7. Os processos nucleares ITIL
8. Abordagem ITIL à gestão de serviços
9. Relação entre eTOM e ITIL
10. Associação ITIL / eTOM
11. Estrutura em camadas
12. Harmonização da terminologia
13. Mapeamentos entre os dois quadros de referência
14. A incorporação do ITIL no eTOM

9188	**Fundamentos de cibersegurança**	25 horas
Objetivos	1. Identificar os fundamentos da cibersegurança. 2. Reconhecer os diferentes tipos de ameaças cibernéticas. 3. Reconhecer o perfil e a motivação dos ataques cibernéticos. 4. Desenvolver mecanismos de proteção do local de trabalho face aos diferentes tipos de *malware*.	

Conteúdos

1. Ameaças cibernéticas
   - **1.1.** BOTNETS
   - **1.2.** Ciber-espionagem
   - **1.3.** Armas cibernéticas
   - **1.4.** Internet *banking*
   - **1.5.** *Mobile malware*
2. Mercado negro da internet
3. *Spam e phishing*
4. Classes populares de malware
   - **4.1.** *Bankers* (PC, dispositivos móveis, pontos de venda, ATM)
   - **4.2.** *Mobile*
   - **4.3.** *Exploits*
   - **4.4.** *Ransoms*
   - **4.5.** *Spies*

5. Técnicas modernas de distribuição de ameaças
6. Armas cibernéticas – ameaças avançadas persistentes (APT) e ameaças industriais
7. Segurança contra ameaças cibernéticas no posto de trabalho

9189	**Tecnologias de análise de evidências**	50 horas
Objetivos	**1.** Identificar as fontes de informação mais relevantes usadas na análise de evidências para os principais tipos de incidentes. **2.** Reconhecer a alto nível expressões regulares e sua representação nas linguagens mais comuns de *scripting*. **3.** Identificar a estrutura e propriedades dos elementos de informação relevantes a extrair dessas fontes de informação. **4.** Identificar as representações textuais mais comuns de "*timestamps*". **5.** Identificar os scripts simples de extração de informação de logs nas linguagens mais comuns de *scripting*. **6.** Identificar as principais fontes de informação pública sobre vulnerabilidades, reputação e ameaças. **7.** Reconhecer a alto nível o funcionamento de sistemas de extração, filtragem, transporte e registo de logs. **8.** Reconhecer a alto nível o funcionamento de sistemas de indexação e correlação sobre logs. **9.** Reconhecer a alto nível o funcionamento de sistemas de *Complex Event Processing* (CEP). **10.** Reconhecer a alto nível o funcionamento de sistemas *Security Information and Event Managment* SIEM.	

Conteúdos

1. Composição e estrutura dos *Logs*: DHCP
   - **1.1.** *Microsoft Active Directory* (AD)
   - **1.2.** *Domain name server* (DNS)
   - **1.3.** RADIUS
   - **1.4.** *Squid Proxy Logs*
   - **1.5.** *Microsoft Exchange*
   - **1.6.** *WebServers*: IIS e *Apache*
   - **1.7.** *WebApplication Servers: JBoss*
   - **1.8.** *Windows EventLogs*
   - **1.9.** *Windows Registry*
   - **1.10.** *Unix/Linux SystemLogs*
2. Fontes públicas de informação sobre IPs e sua reputação
3. Fontes de informação sobre vulnerabilidades em formato CVE (*Common Vulnerabilities and Exposures*)
4. Arquitetura e funcionamento para análise de evidências
   - **4.1.** *SyslogNG*
   - **4.2.** *LogStash*
   - **4.3.** *Splunk*
   - **4.4.** ESPER

4.5. OSSIM

5. Deteção e análise de BOTNETs usados em ataques "*brute force*"

9190	**Introdução à programação aplicada à cibersegurança**	25 horas
Objetivos	**1.** Elaborar pequenos scripts sequenciais, utilizando linguagem moderna de *scripting*. **2.** Aplicar técnicas de extração, filtragem e normalização de informação de logs aplicacionais ou de sistema. **3.** Aplicar expressões regulares simples na extração de informação em linhas de *logs*.	

Conteúdos

1. Instalação do *Ruby*

2. Variáveis e seu escopo

3. Constantes e símbolos

4. Tipos de dados elementares do *Ruby*

4.1. Booleanos

4.2. Números e intervalos

4.3. *Strings*

5. Tipos de dados não elementares

5.1. *Arrays*

5.2. *Hashes*

5.3. Ficheiros

5.4. Blocos de código

5.5. *Procs*

6. Estruturas de controlo -- operadores condicionais

6.1. *If / elsif / else / end*

6.2. *case / when / else / end*

7. Estruturas de controlo -- operadores de *loop*

7.1. *While*

7.2. *For*

7.3. *Until*

7.4. *Loop*

8. Blocos

9. Expressões regulares

10. Classes e métodos

11. Módulos

12. Exceções

9191	**Introdução às técnicas de análise de evidências**	50 horas

Objetivos	**1.** Elaborar *scripts*, utilizando uma linguagem moderna de *scripting*, de extração, filtragem e normalização de informação de logs aplicacionais e de sistema. **2.** Normalizar timestamps em torno do referencial global UTC (*Universal Time Coordinated*). **3.** Reconhecer e validar endereços de email com autenticação. **4.** Reconhecer, resolver e normalizar URIs, domínios e IPs ou ranges de IPs (v4 e v6). **5.** Utilizar bibliotecas de operações especializadas sobre timestamps, endereços de email, URIs, domínios e IPs ou *ranges* de IPs (v4 e v6). **6.** Utilizar bibliotecas de operações especializadas na geolocalização aproximada de IPs e suas distâncias. **7.** Utilizar bibliotecas de algoritmos de medição da distância lexical entre *strings*. **8.** Detetar e analisar BOTNETs.

Conteúdos

1. Idiomas Ruby para extração, filtragem e normalização de *logs* em

- **1.1.** *Filesystem*
- **1.2.** Ambiente *Syslog*

2. Tipos mais comuns de codificação de strings em *logs*

- **2.1.** ASCII
- **2.2.** UTF-8

3. Expressões regulares para identificação e extração de

- **3.1.** *Timestamps*
- **3.2.** Endereços de email
- **3.3.** IPs ou *ranges* de IPs
- **3.4.** Domínios (DNS)

4. Bibliotecas especializadas para manipular

- **4.1.** URIs
- **4.2.** Verificar a existência de endereços de email
- **4.3.** Resolver domínios Internet (DNS) em IPs
- **4.4.** IPs e *ranges* de IPs (v4 e v6)
- **4.5.** Geolocalização aproximada de IPs (v4 e v6)
- **4.6.** Operações sobre IPs e *ranges* de IPs

5. Introdução a outras bibliotecas relevantes e sua aplicação em cibersegurança

- **5.1.** Distância *Levenshtein* entre *strings*
- **5.2.** API Google Maps

6. BOTNETs e seus padrões de comportamento

9192	**Análise de vulnerabilidades – iniciação**	50 horas

Objetivos	**1.** Identificar o conjunto de vulnerabilidades *web* inventariadas pelo *Open Web Application Security Project* (OWASP). **2.** Identificar as técnicas mais comuns na deteção de vulnerabilidades OWASP. **3.** Ler *scripts* simples em *JavaScript* e PHP e analisar falhas de segurança. **4.** Utilizar ferramentas de busca e análise de vulnerabilidades OWASP e interpretar os resultados obtidos.

Conteúdos

1. As top 10 vulnerabilidades *Web* inventariadas pelo *Open Web ApplicationSecurity Project* (OWASP)

- **1.1.** *Injection*
- **1.2.** *Broken Authentication and Session Management*
- **1.3.** *Cross-Site Scripting* (XSS)
- **1.4.** *Insecure Direct Object References*
- **1.5.** *Security Misconfiguration*
- **1.6.** *Sensitive Data Exposure*
- **1.7.** *Missing Function Level Access Control*
- **1.8.** *Cross-Site Request Forgery* (CSRF)
- **1.9.** *Using Known Vulnerable Components*
- **1.10.** *Insecure cryptographic storage* (ICS)

2. Introdução básica ao *JavaScript* e PHP

3. Análise de *scripts JavaScript* com vulnerabilidades

4. Análise de *scripts* PHP com vulnerabilidades

5. Introdução ao *ZedAttack Proxy* (ZAP) e sua aplicação no contexto OWASP

6. Introdução ao *OpenVASe* sua aplicação no contexto OWASP

7. Utilização do ZAP e *Open*VAS na descoberta e análise de vulnerabilidades em web sites

9193	**Análise de vulnerabilidades - desenvolvimento**	50 horas
Objetivos	**1.** Identificar as boas práticas de segurança na configuração e gestão de sistemas de rede e de IT e seus protocolos operacionais. **2.** Identificar vulnerabilidades em equipamentos de rede. **3.** Identificar vulnerabilidades em servidores Linux/Unix e Windows. **4.** Interpretar o dicionário público "CVE" (*Common Vulnerabilities and Exposures*) com informação de referência sobre vulnerabilidades conhecidas. **5.** Aplicar as técnicas, baseadas em agentes, na deteção de vulnerabilidades de segurança em servidores Linux/Unix e Windows. **6.** Aplicar as técnicas, baseadas em sondas de rede, na descoberta de vulnerabilidades de segurança em equipamentos de rede e servidores Linux/Unix e Windows. **7.** Utilizar as ferramentas de busca e análise de vulnerabilidades em redes e servidores e interpretar os resultados obtidos.	

Conteúdos

1. Introdução às boas práticas gerais na configuração e gestão de plataformas de rede e IT

2. Ferramentas de deteção e gestão de vulnerabilidades

2.1. Dicionário público "CVE" (*Common Vulnerabilities and Exposures*) com informação de referência sobre vulnerabilidades conhecidas

2.2. CMDBs (*configuration management database*)

2.3. Agentes OSSEC

2.4. Motor de *scanning* NESSUS

3. Configuração e gestão de plataformas de rede

3.1. Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE

3.2. Segurança na sua configuração e gestão

3.3. Aplicação de scans NESSUS

4. Configuração e gestão de servidores Linux/Unix

4.1. Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE

4.2. Segurança na sua configuração e gestão

4.3. Aplicação de agentes OSSEC

4.4. Aplicação de scans NESSUS

5. Configuração e gestão de servidores Windows

5.1. Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE

5.2. Segurança na sua configuração e gestão

5.3. Aplicação de agentes OSSEC

5.4. Aplicação de scans NESSUS

6. Configuração e gestão de servidores Web

6.1. Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE

6.2. Segurança na sua configuração e gestão

6.3. Aplicação de agentes OSSEC

6.4. Aplicação de scans NESSUS

7. Configuração e gestão de *desktops Windows*

7.1. Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE

7.2. Segurança na sua configuração e gestão

7.3. Aplicação de scans NESSUS

9194	**Introdução à cibersegurança e à ciberdefesa**	50 horas

Objetivos	**1.** Identificar e caracterizar as componentes tangíveis e intangíveis do ciberespaço. **2.** Identificar as potenciais ciberameaças e os riscos individuais. **3.** Identificar as boas práticas associadas à cibersegurança e ciberdefesa. **4.** Identificar a natureza transversal das ciberameaças e o seu impacto global. **5.** Caracterizar os constrangimentos operacionais decorrentes do enquadramento legal aplicável à cibersegurança (direito nacional) e ciberdefesa (direito internacional). **6.** Reconhecer a importância da ciberdefesa das organizacões tanto numa perspetiva nacional como internacional. **7.** Identificar as políticas de cibersegurança e ciberdefesa. **8.** Reconhecer as potenciais ameaças cibernéticas e riscos para as organizações. **9.** Identificar as responsabilidades do indivíduo e o seu papel enquanto agente ativo da cibersegurança e ciberdefesa das organizações.

Conteúdos

1. Introdução ao ciberespaço e terminologia

2. Tipos de ataque e de atacantes, métodos e técnicas de proteção correspondentes

3. Impacto e boas práticas individuais de cibersegurança

- **3.1.** Desktop e web

4. Regulação e enquadramento legal do ciberespaço

- **4.1.** Lei do cibercrime
- **4.2.** Leis internacionais
- **4.3.** Conflitos armados no ciberespaço

5. Impacto e boas práticas de segurança das redes sociais

6. Estratégia Nacional de cibersegurança e de ciberdefesa

7. Cibersegurança em operações militares e ciberdefesa

8. Compreensão e avaliação do ambiente da ameaça cibernética

9. Tecnologias emergentes

10. Gestão dinâmica do risco

11. Política de cibersegurança das organizações

- **11.1.** Finalidade e nível de ambição
- **11.2.** Objetivos a atingir
- **11.3.** Linhas de ação e definição de prioridades
- **11.4.** Controlo de execução e alinhamento das ações a desenvolver

9195	**Enquadramento operacional da cibersegurança**	50 horas

Objetivos	**1.** Identificar ameaças à cibersegurança. **2.** Comparar ferramentas de autenticação. **3.** Utilizar sistemas de deteção de intrusão. **4.** Identificar e utilizar a criptografia e assinaturas digitais. **5.** Descrever os fundamentos da segurança da rede. **6.** Distinguir o *hacking* do *hacking* ético.

Conteúdos

1. Segurança da informação

- **1.1.** Relatórios de ameaças de segurança
- **1.2.** Vulnerabilidades web mais relevantes
- **1.3.** Terminologias comuns
- **1.4.** Elementos de segurança da informação
- **1.5.** Estatísticas relacionadas com a segurança
- **1.6.** Ataque em sites de redes sociais para roubo de identidade

2. Tratamento de ameaças

- **2.1.** Características de ameaça: Ameaça interna
- **2.2.** *Sniffing*
- **2.3.** Tipos de ameaças externas

3. *Backdoors*, vírus, *worms e trojan*

4. *Passwords*

- **4.1.** Mecanismos de autenticação
- **4.2.** *Password cracker*
- **4.3.** Modus operandi de um atacante usando *password cracker*
- **4.4.** Classificação de ataques
- **4.5.** *Web password*
- **4.6.** Senhas geradores

5. Criptografia

- **5.1.** Criptografia de chave pública
- **5.2.** Assinatura digital
- **5.3.** RSA (*Rivest Shamir Adleman*)
- **5.4.** Criptografia de disco
- **5.5.** Ataques de criptografia
- **5.6.** Ferramentas *Microsoft Cryptography*

6. Servidores e aplicações web

- **6.1.** Funcionamento de servidores web
- **6.2.** Vulnerabilidades de aplicativos e suas categorias
- **6.3.** Ferramentas de deteção de vulnerabilidades IIS
- **6.4.** Vulnerabilidades apache
- **6.5.** Segurança do servidor web
- **6.6.** Falhas *cross-site scripting* / XSS
- **6.7.** SQL *injection*

6.8. Falhas de injeção e comandos

7. Redes *wireless*

7.1. Componentes de rede WLAN

7.2. Tipos de rede WLAN

7.3. Deteção de uma rede WLAN

7.4. Como aceder a uma WLAN

7.5. Técnicas para detetar redes abertas wireless

7.6. Diretrizes de segurança WLAN

8. Sistema de deteção de intrusão

8.1. Tipos de *Intrusion Detection Systems*

8.2. Sistema de Integridade *Verifiers* (SIV)

8.3. Indicações gerais de intrusões

8.4. Ferramentas de deteção de intrusão

9. *Firewalls*

9.1. Características e funcionalidades de uma *firewall*

9.2. Tipos de *firewall*

9.3. Colocar o backdoors através de *firewall*

10. Ciclo *hacking*

10.1. História do *hacking*

10.2. Perfil do *hacker*

10.3. Tipos de *hackers*

11. *Hacking* ético

11.1. Classes de *hacker*

11.2. Características e limitações do *hacking* ético

11.3. Competências de um *hacker* ético

11.4. Classificação de *hacker* ético

12. Segurança na rede

12.1. Mapeamento internet protocol para OSI

12.2. Ameaças de segurança sobre uma rede

12.3. Políticas de segurança de rede

13. Segurança nos protocolos de rede

13.1. Protocolo de Segurança E-mail - S / MIME

13.2. Protocolo de Segurança E-mail - PGP

13.3. Protocolo de Segurança Web - SSL

13.4. Protocolo de Segurança Web - SSH

13.5. Protocolo de Segurança Web -http

13.6. Protocolo de Segurança Web -HTTPS

14. Autenticação

15. Validação e autenticação de equipamentos por *radius server*/ tacacs

9196	**Cibersegurança ativa**	50 horas

Objetivos	**1.** Descrever a resposta a incidentes na informática forense. **2.** Identificar evidências digitais. **3.** Utilizar ferramentas de análise e recolha de logs e mecanismos de salvaguarda. **4.** Identificar evidências de incidentes informáticos. **5.** Elaborar relatórios de investigação forense.

Conteúdos

1. Ataques na rede

- **1.1.** *Packet sniffing*
- **1.2.** IP *Spoofing*
- **1.3.** ARP *Spoofing*
- **1.4.** *Session Hijacking*
- **1.5.** *Eavesdropping*

2. Servidores e *Demilitarized Zone* (DMZ)

- **2.1.** Definição de DMZ Características de uma DMZ
- **2.2.** Benefícios da DMZ

3. Servidores de *proxy*

- **3.1.** Características e funcionalidade de servidores *proxy*
- **3.2.** Comunicação via servidores *proxy*

4. Redes privadas virtuais:

- **4.1.** Virtual Private Network (VPN)
- **4.2.** Caraterísticas
- **4.3.** Segurança
- **4.4.** Introdução ao *Internet Protocol Security* (IPSec)
- **4.5.** Serviços IPSec
- **4.6.** A combinação de VPN e Firewalls
- **4.7.** Vulnerabilidades VPN

5. Segurança de redes wireless

- **5.1.** Ferramentas para detetar pontos de acesso de Rogue
- **5.2.** Características *Wired Equivalent Privacy* (WEP)
- **5.3.** Transporte sem fio Layer Security (WTLS)
- **5.4.** Segurança máxima: Adicionar VPN para *Wireless* LAN

6. Segurança de voz sobre IP

- **6.1.** Arquitetura VoIP
- **6.2.** Ameaças VoIP
- **6.3.** Vulnerabilidades VoIP
- **6.4.** Benefícios do VoIP

7. Computação forense

- **7.1.** Ciência forense
- **7.2.** Evolução
- **7.3.** Objetivos
- **7.4.** Fundamentação

7.5. Crime cibernético

7.6. Desafios em matéria de cibercrime

8. Análise forense de redes e *Routing*

8.1. Desafios na análise forense de redes

8.2. Fontes de evidências sobre uma rede

8.3. Ferramentas de análise de tráfego

8.4. Ferramentas para documentar as provas reunidas numa rede

8.5. Volatilidade da recolha de provas

9. Resposta forense a incidentes

9.1. Informações preliminares de incidentes de segurança

9.2. Processo de resposta a incidentes

9.3. Política de resposta a incidentes

10. Evidências digitais

10.1. Características de evidências digitais

10.2. Fragilidade de evidências digitais

10.3. Tipos de dados digitais

10.4. Regulamento de Provas

11. Esteganografia

11.1. Definição

11.2. Modelo

11.3. Aplicação

11.4. Classificação

12. Esteganografia Vs Criptografia

13. Crimes através de e-mail e evidências informáticas

13.1. Cliente e servidor de e-mail

13.2. Funções do cliente e servidor em e-mail

13.3. Ataque de *phishing*

14. Relatório de investigação forense

9197	**Wargamming**	50 horas
Objetivos	**1.** Desenvolver os procedimentos de segurança de Informação de acordo com o tipo de ameaças e incidentes. **2.** Caracterizar os diferentes tipos de operações em redes de computadores no contexto da cibersegurança e ciberdefesa. **3.** Instalar e parametrizar ferramentas destinadas a garantir a cibersegurança e ciberdefesa em contexto de ambiente de simulação virtual (*Cyber Range*).	

Conteúdos

1. Aspetos diferenciadores da cibersegurança e ciberdefesa

2. Impacto estratégico e operacional das ciberameaças

3. Operações em redes de computadores

3.1. Defesa

- **3.2.** Ataque
- **3.3.** Exploração

4. Identificação de dados críticos para as organizações

5. A cadeia de ataque (*KillChain*)

6. Articulação entre defesa e ataque

- **6.1.** Prevenir
- **6.2.** Detetar
- **6.3.** Responder

7. Conhecimento das redes da organização

8. Defesa em profundidade

9. Definição de métricas

10. Desenvolvimento de cenários de cibersegurança e ciberdefesa

- **10.1.** Construção de narrativas de acontecimentos
- **10.2.** Identificação de incidentes associados a uma situação de crise
- **10.3.** Identificação de objectivos e possíveis audiências de treino

11. Enquadramento da utilização de exercícios de simulação ("*Capture the Flag*" e "*Red and Blue*")