REFERENCIAL DE DUPLA CERTIFICAÇÃO

EM VIGOR

Nível de Qualificação: 5

Área de Educação e Formação	**481 . Ciências Informáticas**
Código e Designação da qualificação	**481RA057 - Técnico/a Especialista em Cibersegurança**
Modalidades de Educação e Formação	**Aprendizagem +** **Cursos de Especialização Tecnológica** **Formação Modular**
Total de pontos de crédito	**106,50** **(inclui 15 pontos de crédito da Formação em Contexto de Trabalho)**
Publicação e atualizações	Publicado no Boletim do Trabalho e Emprego (BTE) N.º 17 de 08 de maio de 2025 com entrada em vigor a 08 de maio de 2025.
Observações	

1. Descrição Geral da Qualificação (Missão)

Implementar e gerir sistemas de segurança em organizações, contribuindo para a prevenção, deteção e mitigação de ameaças cibernéticas.

2. Atividades Principais

- Instalar, configurar e colocar em produção plataformas de cibersegurança ao nível das infraestruturas de comunicações e de segurança perimétrica, de tecnologias de informação (servidores web, aplicacionais e de bases de dados), e de suporte aos ambientes colaborativos.
- Assegurar a privacidade e proteção de dados pessoais
- Monitorizar eventos no ciberespaço e detetar ameaças à cibersegurança.
- Realizar testes de penetração.
- Responder (em 1ª linha) a situações anómalas e incidentes de cibersegurança.
- Recolher e efetuar o tratamento de informação e evidências, utilizando ferramentas especializadas.
- Apoiar na elaboração de relatórios forense.

3. Unidades De Competência (UC)

Componente Geral e Científica			
OBRIGATÓRIAS			
Código[1]	**N.º UC**	**Unidades de Competência**	**Pontos de Crédito**
UC01476	1	Implementar a legislação relativa à cibersegurança	2,25
UC01477	2	Aplicar métodos estatísticos	4,5
UC00598	3	Efetuar operações e cálculos matemáticos aplicados a projetos da área de informática	4,5
UC00599	4	Interagir em inglês nas atividades do setor da informática	4,5
	Total de Pontos de Crédito da Componente Geral e Científica: 15		

[1]Os códigos assinalados a preto correspondem a UC específicas desta qualificação. Os códigos assinalados a laranja correspondem a UC que são comuns a outras qualificações.

Componente Tecnológica			
OBRIGATÓRIAS			
Código[1]	**N.º UC**	**Unidades de Competência**	**Pontos de Crédito**
UC00245	1	Desenvolver algoritmos	2,25
UC00606	2	Desenvolver programas em linguagem estruturada	4,5
UC00602	3	Modelar bases de dados relacionais	2,25
UC00631	4	Planear e instalar a infraestrutura de redes locais	4,5
UC01478	5	Configurar redes de computadores	2,25
UC00634	6	Instalar, configurar e manter sistema operativo de cliente	2,25
UC00633	7	Instalar e parametrizar sistemas operativos de servidor (plataforma proprietária)	4,5
UC00635	8	Configurar serviços de rede	2,25
UC01479	9	Implementar mecanismos de proteção contra ameaças cibernéticas	2,25
UC01480	10	Analisar evidências de ataques cibernéticos	4,5
UC01481	11	Desenvolver scripts aplicados à cibersegurança	2,25
UC01482	12	Programar scripts de normalização e filtragem de logs	4,5
UC01483	13	Detetar e analisar vulnerabilidades em soluções web	4,5
UC01484	14	Detetar e analisar vulnerabilidades em sistemas de rede	4,5
UC01485	15	Instalar e configurar ferramentas de análise e recolha de logs e evidências	4,5
UC01486	16	Gerir sistemas de deteção de intrusos (IDS)	4,5
UC01487	17	Simular cenários de cibersegurança e ciberdefesa (wargamming)	4,5
UC00616	18	Implementar as normas de segurança e saúde no trabalho no setor de Informática	2,25
		Total de pontos de crédito:	**63,00**

[1]Os códigos assinalados a preto correspondem a UC específicas desta qualificação. Os códigos assinalados a laranja correspondem a UC que são comuns a outras qualificações.

Para obter a qualificação de Técnico/a Especialista em Cibersegurança , para além das UC Obrigatórias, **terão também de ser realizadas UC Opcionais correspondentes ao total de 13,5 pontos de crédito.**

OPCIONAIS

Código[1]	N.º UC	Unidades de Competência	Pontos de Crédito
UC00033	1	Comunicar e interagir em contexto profissional	4,5
UC00034	2	Colaborar e trabalhar em equipa	4,5
UC00600	3	Analisar as funções e estrutura da organização	2,25
UC00613	4	Gerir políticas de segurança em sistemas informáticos	2,25
UC01488	5	Gerir a segurança da informação e criptografia	2,25
UC01489	6	Implementar procedimentos de recolha e análise forense digital	4,5
UC01490	7	Executar técnicas de hacking ético	2,25
UC00627	8	Instalar e configurar servidores Web	2,25
UC01491	9	Projetar e administrar sistemas de bases de dados	4,5

Total de pontos de crédito da Componente Tecnológica:	**76,50**

[1]Os códigos assinalados a preto correspondem a UC específicas desta qualificação. Os códigos assinalados a laranja correspondem a UC que são comuns a outras qualificações.

4. Desenvolvimento das Unidades de Competência

Componente Geral e Científica

UC01476	Implementar a legislação relativa à cibersegurança
Pontos de crédito	2,25

Realizações

- **Aplicar a legislação nacional e comunitária de proteção de dados.**
- **Aplicar a legislação nacional sobre manuseamento de informação classificada.**
- **Analisar a legislação nacional sobre cibercriminalidade.**

Conhecimentos

- Declaração Universal dos Direitos Humanos - princípios.
- Direito de imagem.
- Princípios da Carta dos Direitos Fundamentais da União Europeia aplicados à cibersegurança.
- Regulamento Geral de Proteção de Dados.
- Constituição da República Portuguesa (CRP) e os preceitos constitucionais respeitantes aos direitos, liberdades e garantias.
- Privacidade, dados pessoais e dados sensíveis -conceitos.
- Matéria de administração eletrónica e proteção de dados – conceitos nacionais e comunitários, direito de informação, direito de acesso, direito de oposição, direito de retificação e eliminação, código de procedimento administrativo.
- Matéria informação classificada – conceitos nacionais e comunitários, Princípio da necessidade de conhecer, manuseamento e classificação.
- Cibercrime -Conceitos.
- Competências de investigação criminal em cibercriminalidade - conceitos.
- Normas processuais na investigação de cibercrimes - conceitos.

Aptidões

- Interpretar os princípios da Declaração Universal dos Direitos Humanos.
- Interpretar a legislação sobre direito de imagem.
- Interpretar os princípios da Carta dos Direitos Fundamentais da União Europeia aplicados à cibersegurança.
- Identificar os conceitos fundamentais de direitos, liberdades e garantias, internacionais e nacionais.
- Interpretar os conceitos nacionais e comunitários em matéria de administração eletrónica e proteção de dados.
- Interpretar legislação nacional sobre manuseamento de informação classificada.
- Interpretar legislação nacional sobre cibercriminalidade.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Implementar a legislação relativa à cibersegurança

- Cumprindo as normas gerais, as orientações e regulamentos sobre a proteção de dados.
- Garantindo o cumprimento dos procedimentos, prazos e requisitos estabelecidos.

Contexto (de uso de competência)

- Aplicável a diferentes contextos.

Recursos

- Dispositivos tecnológicos com acesso à Internet.
- Constituição da República Portuguesa (CRP).
- Código de Procedimento Administrativo.
- Regulamento Geral sobre a Proteção de Dados.

UC01477	Aplicar métodos estatísticos
Pontos de crédito	4,5

Realizações

- **Aplicar métodos de exploração, organização e apresentação de dados.**
- **Utilizar ferramentas de estatística descritiva na análise de dados das amostras ou das populações.**
- **Utilizar ferramentas básicas da inferência estatística.**

Conhecimentos

- Estatística - técnicas de recolha de dados; amostragem e características de uma amostra; representações gráficas; regressão e correlação.
- Cálculo combinatório.
- Probabilidade – acontecimentos independentes e dependentes; lei de Laplace, axiomas da probabilidade, probabilidade condicionada.

Aptidões

- Aplicar técnicas de recolha de dados.
- Determinar a dimensão de uma amostra.
- Aplicar técnicas de amostragem na recolha de dados.
- Utilizar técnicas escritas e gráficas para apresentação de resultados.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Iniciativa.

Conhecimentos	Aptidões	Atitudes
• Teorema da Probabilidade Total e Teorema de Bayes. • Distribuições de probabilidade – tipos (discretas, contínuas); normal, binomial, Poisson, uniforme, t-Student, qui-quadrado. • Inferência estatística. • Obtenção, análise e classificação de amostras – tratamento estatístico de amostras (parâmetros estatísticos); estimação de parâmetros (intervalos de confiança, estimadores pontuais). • Testes de hipóteses – teste z (normal), teste t (Student), teste qui-quadrado e teste para a taxa de Poisson. • Software de análise estatística – funcionalidades.	• Executar o cálculo de parâmetros estatísticos. • Utilizar a análise combinatória na determinação de probabilidade de um acontecimento. • Calcular probabilidade condicionada. • Aplicar leis e axiomas de probabilidade à resolução de problemas estocásticos. • Distinguir variáveis independentes e dependentes. • Aplicar o teorema da Probabilidade Total e o teorema de Bayes à resolução de problemas de probabilidade condicionada. • Aplicar distribuições de probabilidade na modelação de problemas. • Executar a estimação de parâmetros. • Determinar erro máximo da amostra e intervalos de confiança. • Aplicar testes de hipóteses a estudos estatísticos com base em amostras.	• Sentido analítico. • Sentido de organização. • Rigor. • Respeito pelas normas de segurança e saúde no trabalho.

Critérios de Desempenho

Aplicar métodos estatísticos

- Utilizando termos, símbolos e convenções próprias da linguagem matemática, científica e tecnológica.
- Respeitando regras, métodos e processos de cálculo.
- Recorrendo a propriedades e leis matemáticas.
- Adequando as ferramentas à amostra em causa.
- Extraindo conclusões dos resultados.

Contexto (de uso de competência)

- Aplicável a diferentes contextos.

Recursos

- Dispositivos tecnológicos com acesso à internet.

- Máquina de calcular.
- Biblioteca de dados.
- Software de análise estatística.
- Manuais e documentos de suporte.

UC00598	Efetuar operações e cálculos matemáticos aplicados a projetos da área de informática
Pontos de crédito	4,5

Realizações

- **Aplicar a Álgebra de Boole à resolução de problemas lógicos.**
- **Aplicar o cálculo matricial à resolução de problemas de otimização com múltiplas variáveis lineares e interligadas.**
- **Aplicar a Teoria de grafos à resolução de problemas relacionais e análise de ligações.**
- **Realizar estudos estatísticos simples.**
- **Aplicar o teorema de Bayes à resolução de problemas de probabilidade condicionada.**

Conhecimentos

- Sistemas de numeração – decimal, binário, octal e hexadecimal; conversão entre sistemas.
- Aritmética binária – adição e subtração binária; complemento a dois e a um; representação de número binário com bit de sinal.
- Deteção de erros através do bit de paridade.
- Teoria de conjuntos e lógica – representação de conjuntos, relação de pertença e inclusão de conjuntos; operações sobre conjuntos (reunião, interseção, diferença e complementação); valor lógico de uma proposição; cálculo proposicional: negação, conjunção, disjunção de proposições (tabelas de verdade).
- Álgebra de Boole – elementos; operações Lógicas (AND, OR, NOT, NAND, NOR, XOR e XNOR); postulados e teoremas.

Aptidões

- Representar números inteiros e fracionários numa dada base.
- Identificar o valor de um dígito numa dada base de numeração.
- Converter números inteiros e fracionários entre sistemas de numeração.
- Realizar operações aritméticas no sistema binário.
- Determinar o valor lógico de uma proposição.
- Distinguir conjunto de pertença.
- Representar graficamente os uniões e interseções de conjuntos.
- Aplicar os postulados e teoremas da álgebra de Boole à execução de operações lógicas.
- Aplicar o método da condensação na resolução de sistemas.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções e atribuições.
- Empenho e persistência na resolução de problemas.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Matrizes – definição e representação de uma matriz mxn; tipos (matriz transposta; matriz simétrica; matriz unidade; matriz inversa); igualdade de matrizes.	• Aplicar a representação matricial a problemas práticos.
• Cálculo matricial – cálculo da matriz inversa pelo método da condensação e resolução de sistemas de equações lineares pelo método da condensação; matriz de um sistema linear e dimensão de uma matriz.	• Resolver problemas graficamente.
• Matrizes especiais - linha e coluna, quadrada, diagonal, identidade e simétrica.	• Determinar caminhos e graus de vértices em grafos.
• Operações com matrizes – adição, produto por um escalar, transposição e multiplicação de matrizes.	• Aplicar grafos à resolução de problemas de redes e otimização, de análise de circuitos e de algoritmia.
• Grafos - grafo (não orientado) e sua representação, lacete; grafo simples, multigrafo; grafo conexo, grafo completo e grau de um vértice.	• Aplicar técnicas de recolha de dados.
• Caminhos de um grafo – simples, elementar, circuito e ciclo.	• Determinar a dimensão de uma amostra.
• Matriz de adjacência de um grafo.	• Aplicar técnicas de amostragem na recolha de dados.
• Potências da matriz de adjacência.	• Utilizar a análise combinatória na determinação de probabilidade de um acontecimento.
• Estatística - técnicas de recolha de dados; amostragem e características de uma amostra; representações gráficas; regressões.	• Calcular probabilidade condicionada.
• Cálculo combinatório.	• Aplicar leis e axiomas de probabilidade à resolução de problemas estocásticos.
• Probabilidade - lei de Laplace, axiomas da probabilidade, probabilidade condicionada, independência.	• Distinguir variáveis independentes e dependentes.
• Teorema da Probabilidade Total e Teorema de Bayes.	• Aplicar o teorema da Probabilidade Total e o teorema de Bayes à resolução de problemas de probabilidade condicionada.
• Distribuições de probabilidade - binomial e normal – propriedades.	• Aplicar distribuições de probabilidades na modelação de problemas.

Critérios de Desempenho

Efetuar operações e cálculos matemáticos aplicados a projetos da área de informática

- Utilizando termos, símbolos e convenções próprias da linguagem matemática, científica e tecnológica.
- Respeitando regras, métodos e processos de cálculo.

- Recorrendo a propriedades e leis matemáticas.
- Adequando as ferramentas à amostra em causa.
- Extraindo conclusões dos resultados.

Contexto (de uso de competência)

- Aplicável a diferentes contextos.

Recursos

- Dispositivos tecnológicos com acesso à internet.
- Folha de cálculo.
- Máquina de calcular.
- Manuais e documentos de suporte.

UC00599	Interagir em inglês nas atividades do setor da informática
Pontos de crédito	4,5

Realizações

- **Interpretar e selecionar informação especializada, verbal e não verbal, em suportes variados nas atividades do setor da informática**
- **Transmitir enunciados orais coerentes no âmbito das atividades no setor da informática.**
- **Redigir textos articulados e coesos relacionados com as atividades no setor da informática.**

Conhecimentos	Aptidões	Atitudes
• Léxico (vocabulário) relacionado com a Informática	• Identificar o sentido de mensagens em contexto profissional e reconhecer léxico específico da área profissional num discurso oral.	• Responsabilidade pelas suas ações.
• Funções da linguagem.	• Descodificar perguntas e informações.	• Autonomia no âmbito das suas funções.
• Estruturas do funcionamento da língua – sons, entoações e ritmos da língua, símbolos fonéticos; nomes, pronomes, adjetivos, advérbios, determinantes e artigos, elementos de ligação frásica, verbos.	• Distinguir informação essencial da informação acessória em textos e suportes diversificados.	• Assertividade.
• Sintaxe.	• Responder a perguntas diretas.	• Empatia
• Fluência de leitura.	• Iniciar, manter e terminar conversas de âmbito profissional.	• Empenho e persistência na resolução de problemas.
		• Escuta ativa.

Conhecimentos	Aptidões	Atitudes
• Regras de produção de documentos escritos. • Regras de cortesia e convenções linguísticas.	• Descrever, narrar e expressar pontos de vista num discurso oral. • Redigir notas, mensagens, relatórios e preencher formulários. • Escrever ou responder a uma carta, e-mail e outro tipo de mensagens. • Utilizar vocabulário específico da área profissional. • Adequar o código oral e escrito à sua finalidade. • Identificar sequência e causalidade. • Contextualizar o texto no tempo e no espaço. • Respeitar as regras da morfologia e da sintaxe na produção oral e escrita. • Usar linguagens não verbais. • Mobilizar recursos linguísticos relacionando informação de áreas e fontes diversificadas. • Utilizar procedimentos de pesquisa e recolha de informação.	• Respeito pelas diferenças individuais. • Sentido crítico. • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Interagir em inglês nas atividades do setor da informática

- Identificando o contexto, a ideia principal, distinguindo informações simples e de maior complexidade do discurso oral e do texto escrito.
- Comunicando oralmente de forma precisa e eficaz, com ritmo e entoação apropriados e adaptando o discurso ao registo do interlocutor.
- Utilizando vocabulário, estruturas frásicas diversas e formas de tratamento adequados à situação comunicativa oral e escrita e ao público-alvo.
- Produzindo um texto escrito de forma clara e articulada, de acordo com a sua finalidade e público-alvo.
- Aplicando técnicas de redação de documentos profissionais e usando as regras de ortografia, de pontuação e de acentuação.

Contexto (de uso de competência)

- Nas atividades profissionais no setor da informática.

Recursos

- Dispositivos tecnológicos com acesso à Internet.
- Conteúdos multimédia.
- Ferramentas de tradução, dicionários, entre outros.

Componente Tecnológica

UC00245	Desenvolver algoritmos
Pontos de crédito	2,25

Realizações

- **Definir o problema.**
- **Planear as etapas de criação do algoritmo.**
- **Estruturar algoritmos em pseudocódigo.**
- **Desenhar algoritmos em fluxograma.**
- **Testar e depurar algoritmos.**

Conhecimentos

- Pensamento computacional - princípios.
- Algoritmo – conceitos, noções de ação e estado da ação; etapas e desenvolvimento.
- Tipos de dados – constantes e variáveis.
- Entrada e saída de dados - elementos de linguagem.
- Estruturas lógicas básicas - estrutura sequencial, alternativa e repetitiva; condições e regras de inicialização e alteração; estruturas diagramáticas como representação algorítmica.

Aptidões

- Reconhecer os princípios do pensamento computacional.
- Reconhecer os princípios do pensamento computacional.
- Definir os inputs e os outputs esperados, as restrições e as condições que o algoritmo deve cumprir.
- Decompor um problema em subproblemas ou etapas menores.
- Aplicar estruturas de dados, estruturas lógicas e técnicas de construção de algoritmos.
- Utilizar aplicações de desenho de algoritmos.
- Utilizar métodos de teste e depuração de algoritmos.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Empenho e persistência na resolução de problemas.
- Iniciativa.
- Rigor.
- Sentido analítico.
- Sentido de organização.

Conhecimentos	Aptidões
• Técnicas de construção/desenho de algoritmos – contadores, totalizadores, expressões aritméticas, funções predefinidas, validação de dados.	• Aplicar estratégias de otimização de algoritmos.

Critérios de Desempenho

Desenvolver algoritmos

- Aplicando as técnicas de construção.
- Utilizando aplicações de representação diagramática.
- Garantindo a resolução do problema.

Contexto (de uso de competência)

- Empresas do setor da informática.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da administração pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à internet.
- Editor de texto.
- Ambientes integrados de desenvolvimento.
- Compiladores.
- Aplicações de desenho de algoritmos e fluxogramas.

UC00606	Desenvolver programas em linguagem estruturada
Pontos de crédito	4,5

Realizações

- **Planear as etapas de desenvolvimento de um programa.**
- **Criar programas com funções e estruturas de controlo.**
- **Testar e depurar os programas.**

Conhecimentos	Aptidões	Atitudes
• Ciclo de vida do software. • Pensamento computacional - princípios. • Desenvolvimento de software - metodologias. • Algoritmos. • Linguagem estruturada- conceitos; características; estrutura de um programa. • Dados - variáveis, declarações e expressões; constantes; tipos de dados simples. • Estruturas de controlo: sequência; seleção; repetição • Subprogramas - estrutura (funções e procedimentos); variáveis locais e globais; passagem de variáveis por parâmetros. • Funcionalidades de um editor de texto. • Regulamento geral de proteção de dados. • Normas e regulamentos aplicáveis.	• Interpretar manuais, guiões e tutoriais técnicos. • Interpretar os princípios e conceitos relacionados com algoritmia. • Interpretar os princípios e conceitos relacionados com programação estruturada. • Utilizar orientações metodológicas para planear as etapas de criação do programa. • Instalar e configurar o ambiente de programação. • Utilizar a sintaxe da linguagem no desenvolvimento do programa. • Definir os tipos de dados, operadores, constantes, variáveis e estruturas de controlo no desenvolvimento. • Definir funções e estruturas de dados. • Testar e depurar o programa. • Detetar e corrigir os erros identificados. • Criar um guião técnico ou manual de utilizador do programa. • Aplicar normas e regulamentos.	• Responsabilidade pelas suas ações. • Autonomia no âmbito das suas funções. • Empenho e persistência na resolução de problemas. • Ética. • Iniciativa. • Sentido critico. • Sentido de organização. • Rigor. • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Desenvolver programas em linguagem estruturada

- Seguindo as orientações técnicas e metodológicas no desenvolvimento de software.
- Utilizando o ambiente de programação.
- Cumprindo as regras de programação.
- Executando a programação e corrigindo erros.

Contexto (de uso de competência)

- Empresas do setor da informática.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Aplicações de programação estruturada.
- Ambientes integrados de desenvolvimento.
- Compiladores.
- Editor de texto.

UC00602	Modelar bases de dados relacionais
Pontos de crédito	2,25

Realizações

- **Definir a estrutura de uma base dados relacionais**
- **Representar modelos relacionais.**
- **Normalizar dados não normalizados.**

Conhecimentos

- Sistemas de Gestão de Bases de Dados (SGBD) – conceitos.
- Bases de dados - conceito de dados e de modelo de dados; arquitetura; ficheiros.
- Arquitetura de um sistema de gestor de base de dados.
- Modelo relacional- estrutura de dados relacional; regras de integridade; gestão de dados.
- Tabelas, registos, campos e chaves.
- Modelo de entidades e relações: conceitos e tipo de atributos.
- Modelos físicos de dados
- Representação das fronteiras do sistema

Aptidões

- Interpretar manuais, guiões e tutoriais técnicos.
- Interpretar os conceitos sobre a gestão da informação em bases de dados.
- Identificar as entidades e os seus atributos.
- Utilizar modelos relacionais para modelar e representar a informação.
- Utilizar modelos de diagramas para modelar e representar a informação.
- Usar regras e notações para representação das fases da normalização de dados.
- Aplicar as regras que contribuem para a integridade da informação.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções
- Empenho e persistência na resolução de problemas.
- Iniciativa.
- Sentido analítico
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Representação do comportamento do sistema • Representação da implementação do sistema • Normalização - representação na forma não normalizada; tipo de notação; integridade da informação. • Regime Geral de Proteção de Dados • Normas e regulamentos aplicáveis.	• Aplicar normas e regulamentos.

Critérios de Desempenho

Modelar bases de dados relacionais

- Seguindo orientações metodológicas para modelar a informação.
- Cumprindo as fases de normalização de dados em diversas notações.
- Cumprindo as normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática, redes e telecomunicações.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Aplicações para a criação de modelos relacionais e normalização de dados.

UC00631	Planear e instalar a infraestrutura de redes locais
Pontos de crédito	4,5

Realizações

- **Planear e projetar o layout de uma rede local.**

Realizações

- **Preparar a cablagem e infraestrutura.**
- **Montar a cablagem e a infraestrutura de rede.**

Conhecimentos

- Redes de computadores – conceitos, classificação, funcionalidades, tarefas.
- Redes de dados.
- Arquitetura de redes de computadores.
- Modelo OSI
- Modelo TCP/IP.
- Redes de computadores locais (LANs):
- Topologias de redes.
- Cablagem de redes.
- Equipamento ativo de rede.
- Planeamento de redes estruturadas.
- Orientações de montagem e instalação do equipamento.
- Normas de segurança e saúde no trabalho.
- Normas de proteção ambiental.

Aptidões

- Interpretar manuais do fabricante, guiões e tutoriais técnicos.
- Interpretar conceitos, funcionalidades e tarefas.
- Interpretar arquiteturas de redes de computadores.
- Comparar o modelo OSI e o modelo TCP/IP.
- Distinguir tipologias de redes.
- Selecionar a tipologia de rede.
- Analisar as caraterísticas dos equipamentos, tendo em conta as orientações do fabricante e os requisitos técnicos para criar a rede local.
- Selecionar os componentes para a infraestrutura de uma rede local.
- Selecionar os equipamentos ativos/passivos e recursos para uma rede local.
- Planear as etapas de instalação e configuração de uma rede local.
- Aplicar técnicas para descarnar cabos e cravar fichas de rede.
- Montar a cablagem de redes estruturadas.
- Instalar a infraestrutura de rede
- Interpretar normas e procedimentos de gestão da segurança do equipamento.
- Aplicar normas de segurança na montagem e manutenção dos componentes dos equipamentos informáticos.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Iniciativa.
- Sentido de organização.
- Rigor.
- Respeito pelas normas de segurança e saúde no trabalho.

Aptidões

- Aplicar as normas de proteção ambiental.

Critérios de Desempenho

Planear e instalar a infraestrutura de redes locais

- Respeitando o layout definido.
- Seguindo as orientações técnicas para preparar e montar a infraestrutura de rede.
- Cumprindo as normas e regras de segurança.

Contexto (de uso de competência)

- Empresas do setor da informática.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais do fabricante, guiões e tutoriais técnicos.
- Placas de rede.
- Routers.
- Switches.
- Cabos.
- Fichas.
- Ferramentas e máquinas.
- Computadores.
- Outros equipamentos.

UC01478	Configurar redes de computadores
Pontos de crédito	2,25

Realizações

- **Analisar os requisitos técnicos para a configuração de redes.**
- **Planear e configurar IP com subnetting e VLSM.**
- **Instalar e utilizar aplicações de gestão de redes.**

Conhecimentos	Aptidões	Atitudes
• Redes de computadores – conceitos, funcionalidades e tarefas. • Arquiteturas e tipos de redes. • Componentes de uma rede. • Cablagem e ligações. • O modelo OSI – camadas e encapsulamento. • Camada rede do modelo OSI – routers e portos de interfaces, comunicação entre redes, conceitos e tabelas sobre ARP, protocolos de routing. • A camada transporte do modelo OSI – objetivo camada 4, protocolos TCP e UDP, métodos de conexão por TCP. • O TCP/IP e seus Protocolos - IP, HTTP, SMTP, FTP, SNMP, TCP, UDP, ICMP, IGMP, entre outros. • Classes de redes. • Comandos principais do TCP/IP. • Routing e endereçamento – caminhos no routing de pacotes, classes e endereços IP e endereços reservados, Network ID e cálculo de hots por classe de IP, subnetting e subnets. • Camadas de sessão e apresentação do modelo OSI – fundamentos. • Camada de aplicação do modelo OSI – objetivo da camada 7. • Aplicações de rede. • Utilitários de administração de redes. • Normas de segurança e saúde no trabalho. • Normas de proteção ambiental. • Normas de gestão da segurança da informação e na comunicação. • Mecanismos de segurança.	• Interpretar manuais, guiões e tutoriais técnicos. • Interpretar os fundamentos das arquiteturas de redes de comunicação. • Interpretar as funções das camadas superiores do modelo OSI. • Determinar caminhos no routing de pacotes. • Cálcular hots por classe de IP. • Aplicar procedimentos técnicos para interligar redes. • Utilizar os utilitários de administração de redes locais. • Aplicar normas e procedimentos de gestão da segurança do equipamento e da informação. • Aplicar as normas de proteção ambiental. • Aplicar as normas e regulamentos.	• Responsabilidade pelas suas ações e pelas de terceiros. • Autonomia no âmbito das suas funções. • Cooperação com a equipa. • Empenho e persistência na resolução de problemas. • Ética. • Iniciativa. • Sentido de organização. • Rigor. • Respeito pelas normas de segurança e saúde no trabalho

Critérios de Desempenho

Configurar redes de computadores

- Reconhecendo as funções do modelo OSI.
- Otimizando o seu funcionamento e segurança.
- Cumprindo as normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e redes.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Placas de rede.
- Routers.
- Switchs.
- Cabos.
- Fichas.
- Ferramentas e máquinas.
- Computadores.
- Outros equipamentos.
- Utilitários de rede
- Aplicações de rede.

UC00634	Instalar, configurar e manter sistema operativo de cliente
Pontos de crédito	2,25

Realizações

- **Instalar o sistema operativo cliente.**
- **Proceder à parametrização do sistema operativo.**
- **Proceder a configurações de rede e contas de utilizador.**
- **Instalar e configurar drivers para o funcionamento do hardware nos dispositivos clientes.**

Conhecimentos	Aptidões	Atitudes
• Redes: Conceitos. • Sistema operativo cliente – funções, características, tipos e sistemas; aquisição e licenciamento. • Requisitos do sistema. • Opções de instalação e configuração sistemas operativos. • Particionamento e formatação do disco(s). • O núcleo e a interface. • Gestão de processos. • Gestão de memória. • Entrada e saída de dados. • O sistema de ficheiros. • Proteção, segurança e fiabilidade. • Grupos e utilizadores. • Regulamento Geral de Proteção de Dados. • Normas e regulamentos aplicáveis.	• Interpretar manuais, guiões e tutoriais técnicos. • Verificar os requisitos técnicos recomendados para o sistema operativo cliente. • Executar procedimentos técnicos para instalação dos diversos componentes do sistema operativo cliente. • Verificar espaço disponível no disco e determinar as opções de partição. • Instalar e configurar as placas de interface de rede e os protocolos associados. • Definir o perfil de utilizador. • Configurar privilégios de acesso à rede. • Configurar a gestão de dados e unidades de armazenamento. • Configurar o DHCP, DNS e outros serviços de rede. • Instalar dispositivos e device drivers. • Aplicar as normas e regulamentos.	• Responsabilidade pelas suas ações. • Autonomia no âmbito das suas funções. • Empenho e persistência na resolução de problemas. • Iniciativa. • Rigor • Sentido de organização. • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Instalar, configurar e manter sistema operativo de cliente

- Cumprindo as orientações técnicas.
- Garantindo os requisitos técnicos e de compatibilidade.
- Cumprindo as normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e redes.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Computadores e outros equipamentos de rede.
- Sistema operativo.

UC00633	Instalar e parametrizar sistemas operativos de servidor (plataforma proprietária)
Pontos de crédito	4,5

Realizações

- **Instalar sistemas operativos servidores.**
- **Configurar sistemas de backup.**
- **Desenvolver planos de recuperação de desastres.**
- **Gerir as contas de utilizador e permissões de acesso aos recursos dos servidores.**

Conhecimentos

- Sistema operativo servidor – funções, características, tipos.
- Aquisição e licenciamento.
- Requisitos do sistema.
- Gestão de processos e de memória.
- Sistema de ficheiros.
- Gestão de recursos.
- Monitorização de segurança e análise do sistema.
- Grupos e utilizadores.
- Servidores e serviços - domínios, segurança, perfis, ficheiros, file server, print server, acesso remoto, rede, backups, redundância, entre outros.
- Gestão e monitorização de redes e aplicações.

Aptidões

- Interpretar manuais, guiões e tutoriais técnicos.
- Verificar os requisitos técnicos recomendados para o sistema operativo servidor.
- Executar procedimentos técnicos para instalação de um sistema operativo servidor.
- Utilizar procedimentos técnicos para otimização do sistema operativo servidor.
- Criar grupos de trabalho, gerir e parametrizar utilizadores.
- Gerir os recursos partilhados.
- Administrar as ferramentas.
- Configurar o acesso remoto.
- Definir planos de backup, migração e reposição.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Empenho e persistência na resolução de problemas.
- Iniciativa.
- Rigor
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Planos de backup, migração, virtualização e de reposição de sistemas operativos.	• Utilizar metodologias para planeamento de recuperação de desastres.
• Regulamento Geral de Proteção de dados,	• Utilizar procedimentos técnicos para instalar e configurar clientes.
• Normas e regulamentos aplicáveis.	• Instalar ferramentas para monitorizar o desempenho da rede.
	• Aplicar procedimentos de segurança nas redes.
	• Aplicar normas e regulamentos.

Critérios de Desempenho

Instalar e parametrizar sistemas operativos de servidor (plataforma proprietária)

- Cumprindo as orientações técnicas.
- Garantindo a proteção dos dados armazenados nos servidores.
- Cumprindo as políticas de segurança estabelecidas na gestão de utilizadores e permissões de acesso aos recursos dos servidores.
- Cumprindo as normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática, redes e telecomunicações
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Computadores e outros equipamentos de rede.
- Sistema operativo.

UC00635	Configurar serviços de rede
Pontos de crédito	2,25

Realizações

- **Instalar e configurar o serviço DHCP.**

Realizações

- **Instalar e configurar o serviço DNS.**
- **Instalar e configurar serviços de routeamento de dados.**
- **Instalar e configurar servidores de páginas web.**

Conhecimentos

- Serviço DHCP – funcionamento, DHCP Manager, Scopes, clientes estáticos e reserva de endereços, backups e recuperações.
- Serviço DNS - funcionamento, Namespace e zones, tipos de servidores DNS, DNS Manager, zonas, registos.
- WINS - funcionamento, clientes.
- Serviços de roteamento
- Servidores Web - Internet Information Services (IIS), Apache.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar manuais, guiões e tutoriais técnicos.
- Caracterizar o serviço DHCP
- Utilizar procedimentos técnicos para instalar o serviço DHCP.
- Configurar o serviço DHCP
- Utilizar o DHCP Manager e manipular scopes.
- Configurar endereços IP estáticos e reservas para dispositivos específicos na rede
- Configurar backups e restaurar configurações.
- Utilizar o DNS Manager para criar zonas e adicionar registos e integração com o WINS.
- Utilizar o DNS Manager para criar zonas e adicionar registos
- Configurar serviços WINS.
- Parametrizar serviços de roteamento de dados.
- Parametrizar servidores de páginas web (IIS e Apache).
- Aplicar as normas e regulamentos.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Empenho e persistência na resolução de problemas.
- Ética.
- Iniciativa.
- Rigor
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Configurar serviços de rede

- Cumprindo os procedimentos técnicos na instalação.
- Minimizando os tempos de resposta.
- Garantindo a disponibilidade e confiabilidade dos serviços.

- Cumprindo as normas e os regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e redes.
- Lojas de informática.
- Serviços de apoio técnico.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Computadores e outros equipamentos de rede.

UC01479	Implementar mecanismos de proteção contra ameaças cibernéticas
Pontos de crédito	2,25

Realizações

- **Efetuar auditorias de segurança aos sistemas informáticos.**
- **Instalar e configurar mecanismos de proteção.**

Conhecimentos

- Ameaças cibernéticas – conceitos, BOTNETS, ciberespionagem, armas cibernéticas, Internet banking, mobile malware.
- Mercado negro da Internet.
- Spam e phishing.
- Classes de malware - Bankers (PC, dispositivos móveis, pontos de venda, ATM), Mobile, Exploits, Ransoms, Spies.
- Técnicas emergentes de distribuição de ameaças.
- Armas cibernéticas – ameaças avançadas persistentes (APT) e ameaças industriais.
- Segurança contra ameaças cibernéticas no posto de trabalho.

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Identificar e caraterizar os fundamentos da cibersegurança.
- Interpretar os conceitos relacionados com ameaças cibernéticas.
- Distinguir tipos de ameaças cibernéticas.
- Interpretar técnicas emergentes de distribuição de ameaças.
- Executar procedimentos técnicos para comprovar a segurança dos sistemas informáticos.
- Avaliar a necessidade de atualização dos sistemas.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Normas e regulamentos aplicáveis.	• Instalar e configurar sistemas antivírus e anti-malware. • Definir permissões. • Aplicar normas e regulamentos.

Critérios de Desempenho

Implementar mecanismos de proteção contra ameaças cibernéticas

- Testando os sistemas para detetar vulnerabilidades.
- Assegurando que os sistemas informáticos estão protegidos contra acessos não autorizados.
- Cumprindo normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática cibersegurança, redes ou desenvolvimento de software.
- Empresas de consultoria TI
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ferramentas de sistema.
- Regulamento Geral de Proteção de Dados (RGPD).

UC01480	Analisar evidências de ataques cibernéticos
Pontos de crédito	4,5

Realizações

- **Instalar e configurar um serviço de registo de logs centralizado.**
- **Efetuar pesquisas em fontes de informação pública sobre vulnerabilidades, reputação e ameaças.**
- **Monitorizar a rede de uma organização.**

Conhecimentos	Aptidões	Atitudes
• Evidências -conceitos. • Composição e estrutura dos Logs – DHCP, Microsoft Active Directory (AD), Domain name server (DNS), RADIUS, Squid Proxy Logs, Microsoft Exchange, WebServers, IIS e Apache, WebApplication Servers: JBoss, Windows EventLogs, Windows Registry, Unix/Linux SystemLogs. • Fontes públicas de informação sobre IPs e sua reputação. • Fontes de informação sobre vulnerabilidades em formato CVE (Common Vulnerabilities and Exposures). • Arquitetura e funcionamento para análise de evidências – SyslogNG, LogStash, Splunk, ESPER, OSSIM. • Deteção e análise de BOTNETs usados em ataques "brute force". • Normas e regulamentos aplicáveis.	• Interpretar regulamentos, manuais, guiões e tutoriais técnicos. • Interpretar conceitos relacionados com evidências. • Reconhecer as fontes de informação usadas na análise de evidências para os principais tipos de incidentes. • Interpretar a estrutura e propriedades dos elementos de informação relevantes a extrair dessas fontes de informação. • Interpretar as representações textuais mais comuns de "timestamps" • Interpretar os scripts simples de extração de informação de logs nas linguagens mais comuns de scripting. • Instalar e utilizar ferramentas de registo de evidências. • Instalar e utilizar sistemas de análise de evidências. • Selecionar e utilizar fontes de informação sobre IPs e a sua reputação. • Utilizar fontes de informação pública sobre vulnerabilidades em formato CVE (Common Vulnerabilities and Exposures). • Analisar logs de múltiplos serviços. • Analisar logs de diferentes serviços de um Sistema Operativo. • Aplicar expressões regulares na análise e pesquisa de logs. • Aplicar normas e regulamentos.	• Responsabilidade pelas suas ações e pelas de terceiros. • Autonomia no âmbito das suas funções e atribuições. • Empenho e persistência na resolução de problemas. • Ética. • Rigor. • Sentido crítico. • Sentido de organização. • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Analisar evidências de ataques cibernéticos

- Reconhecendo a estrutura de um registo no ficheiro de logs.
- Utilizando fontes de informação pública.
- Utilizando ferramentas de monitorização.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos tecnológicos com acesso à Internet.
- Sistemas de análise de evidências

UC01481	Desenvolver scripts aplicados à cibersegurança
Pontos de crédito	2,25

Realizações

- **Criar scripts com recurso a linguagem de programação de scripting.**
- **Extrair, filtrar e normalizar informação de logs aplicacionais ou de sistema.**
- **Testar os scripts.**

Conhecimentos

- Linguagens de programação de scripts e linguagens compiladas - conceitos.
- Linguagens interpretadas versus linguagens compiladas.
- Ambiente de programação.
- Variáveis, constantes e símbolos.
- Tipos de dados elementares – boleanos, números e intervalos, strings.
- Tipos de dados não elementares – Arrays, hashes, ficheiros, blocos de código, Pocs.
- Estruturas de controlo - operadores condicionais: If/elsif / else / end /case/ when/ else/ end.

Aptidões

- Interpretar regulamentos, manuais, guiões e tutoriais técnicos.
- Interpretar os princípios e conceitos relacionados com linguagens de programação de scripts e linguagens compiladas
- Reconhecer as características de linguagens de programação de scripts.
- Instalar o ambiente de programação.
- Utilizar as funcionalidades do ambiente de programação.
- Utilizar variáveis, constantes símbolos, tipos de dados e estruturas de controlo para elaborar scripts sequenciais.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Estruturas de controlo - operadores de loop: While; for, until, Loop. • Blocos. • Expressões regulares. • Classes e métodos. • Módulos. • Exceções. • Scripts. • Normas e regulamentos aplicáveis.	• Aplicar técnicas de extração, filtragem e normalização de informação de logs. • Aplicar expressões regulares simples na extração de informação em linhas de logs. • Utilizar classes, métodos e módulos para extrair a informação. • Detetar e corrigir anomalias. • Aplicar normas e regulamentos.

Critérios de Desempenho

Desenvolver scripts aplicados à cibersegurança

- Cumprindo as regras no uso dos elementos e sintaxe da linguagem de programação de scripts.
- Prevendo a possibilidade de ocorrer erros e implementar exceções.
- Cumprindo normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ambiente de desenvolvimento.
- Editor de texto.

UC01482	Programar scripts de normalização e filtragem de logs
Pontos de crédito	4,5

Realizações

- **Elaborar scripts para aplicar em logs (registos).**
- **Manipular os dados extraídos dos logs para cálculo de distância lexical.**
- **Executar operações sobre endereços IPv4.**
- **Detetar e analisar BOTNETs.**

Conhecimentos

- Linguagens de programação de scripts e linguagens compiladas - conceitos.
- Idiomas Ruby para extração, filtragem e normalização de logs em – filesystem, ambiente syslog.
- Tipos de codificação de strings em logs – ASCII, UTF-8.
- Expressões regulares para identificação e extração de – timestamps, endereços de email, IPs ou ranges de IPs, domínios (DNS).
- Bibliotecas especializadas para manipular – URIs, endereços de email, domínios Internet (DNS) em IPs, IPs e ranges de IPs (v4 e v6), geolocalização aproximada de IP (v4 e v6), operações sobre IPs e ranges de IPs
- Outras bibliotecas relevantes para a cibersegurança.
- BOTNETs e seus padrões de comportamento.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar regulamentos, manuais, guiões e tutoriais técnicos.
- Interpretar os princípios e conceitos relacionados com linguagens de programação de scripts e linguagens compiladas
- Reconhecer as características de linguagens de programação de scripts.
- Instalar o ambiente de programação.
- Utilizar as funcionalidades do ambiente de programação.
- Elaborar scripts em linguagem de scripting para extrair informação dos ficheiros de logs.
- Utilizar expressões regulares para identificação e extração de timestamps.
- Utilizar expressões regulares para identificação e extração de endereços de correio eletrónico.
- Utilizar bibliotecas de operações especializadas sobre timestamps, endereços de email, URIs, domínios e IPs ou ranges de IPs (v4 e v6).
- Utilizar bibliotecas de operações especializadas na geolocalização aproximada de IPs e suas distâncias.
- Utilizar bibliotecas de algoritmos de medição da distância lexical entre strings.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Aptidões

- Detetar e analisar BOTNETs e mapear padrões de comportamento.
- Aplicar normas e regulamentos.

Critérios de Desempenho

Programar scripts de normalização e filtragem de logs

- Utilizando a linguagem de scripting.
- Manuseando bibliotecas especializadas para manipular os dados extraídos.
- Manuseando bibliotecas especializadas para realizar operações sobre endereços IPv4
- Identificando o comportamento e as ações de BOTNETs.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ambiente de desenvolvimento.
- Editor de texto.

UC01483	Detetar e analisar vulnerabilidades em soluções web
Pontos de crédito	4,5

Realizações

- **Detetar vulnerabilidades em scripts.**
- **Utilizar as ferramentas automáticas para análise de vulnerabilidades.**
- **Avaliar e classificar o risco de vulnerabilidade.**

Conhecimentos	Aptidões	Atitudes
• Vulnerabilidades: Conceitos. • As vulnerabilidades web inventariadas pelo Open Web ApplicationSecurity Project (OWASP). • Linguagem JavaScript e PHP. • Scripts JavaScript com vulnerabilidades. • Scripts PHP com vulnerabilidades. • Ferramentas de análise de vulnerabilidades. • O ZedAttack Proxy (ZAP) e a sua aplicação no contexto OWASP. • O OpenVAS e a sua aplicação no contexto OWASP. • Normas de segurança e proteção dos dados.	• Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos. • Interpretar os conceitos relacionados com vulnerabilidades. • Interpretar o conjunto de vulnerabilidades web inventariadas pelo Open Web Application Security Project (OWASP). • Aplicar técnicas na deteção de vulnerabilidades OWASP. • Analisar scripts JavaScript com vulnerabilidades. • Analisar scripts PHP com vulnerabilidades. • Instalar ferramentas de análise de vulnerabilidades. • Utilizar ZAP e OpenVAS na descoberta e análise de vulnerabilidades em websites. • Aplicar procedimentos de segurança e proteção dos dados.	• Responsabilidade pelas suas ações e pelas de terceiros. • Autonomia no âmbito das suas funções e atribuições. • Cooperação com a equipa. • Empenho e persistência na resolução de problemas. • Ética. • Rigor. • Sentido crítico. • Sentido de organização. • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Detetar e analisar vulnerabilidades em soluções web

- Analisando falhas de segurança em scripts.
- Interpretando os resultados e propondo formas de mitigar as vulnerabilidades.
- Cumprindo normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Função Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ferramentas de analise.

- Regulamento e normativos de proteção de dados.
- Editor de texto.

UC01484	Detetar e analisar vulnerabilidades em sistemas de rede
Pontos de crédito	4,5

Realizações

- **Detetar vulnerabilidades em servidores e outros equipamentos em rede.**
- **Utilizar as ferramentas automáticas para análise de vulnerabilidades.**
- **Avaliar e classificar o risco de vulnerabilidade da rede.**

Conhecimentos

- Ferramentas de deteção e gestão de vulnerabilidades - Dicionário público "CVE" (Common Vulnerabilities and Exposures), CMDBs (configuration management database), agentes OSSEC, motor de scanning NESSUS.
- Configuração e gestão de plataformas de rede, servidores Linux, servidores Windows, servidores Web e desktops Windows.
- Vulnerabilidades e tipos de ataque mais comuns - codificação CVE.
- Segurança na configuração e gestão.
- Aplicação de scans NESSUS.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Aplicar os mecanismos definidos na política de segurança.
- Interpretar o dicionário público "CVE" (Common Vulnerabilities and Exposures) com informação de referência sobre vulnerabilidades conhecidas.
- Configurar e gerir sistemas de rede e de IT.
- Aplicar as técnicas, baseadas em agentes, na deteção de vulnerabilidades de segurança em servidores.
- Aplicar as técnicas, baseadas em sondas de rede.
- Utilizar ferramentas de deteção e gestão de vulnerabilidades para interpretar os resultados obtidos.
- Aplicar normas e regulamentos.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Detetar e analisar vulnerabilidades em sistemas de rede

- Interpretando os resultados e propondo formas de mitigar as vulnerabilidades.
- Implementando mecanismos de segurança na configuração e gestão de redes.
- Cumprindo as normas e regulamentos aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ferramentas de análise.
- Regulamento e normativos de proteção de dados.
- Editor de texto.

UC01485	Instalar e configurar ferramentas de análise e recolha de logs e evidências
Pontos de crédito	4,5

Realizações

- **Detetar evidências digitais.**
- **Analisar evidências digitais com recurso a ferramentas de análise de logs.**
- **Colaborar na elaboração de relatórios de investigação forense.**

Conhecimentos

- Incidentes cibernéticos - conceitos.
- Ataques na rede - Packet sniffing, IP Spoofing, ARP Spoofing, Session Hijacking, Eavesdropping.
- Servidores e Demilitarized Zone (DMZ) – definição, características e benefícios.
- Servidores de proxy – características, funcionalidades e comunicação.

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Interpretar conceitos relacionados com incidentes cibernéticos.
- Interpretar os tipos de ataques de rede.
- Analisar servidores DMZ.
- Analisar servidores de proxy.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.

Conhecimentos	Aptidões	Atitudes
• Redes privadas virtuais – características, segurança, Virtual Private Network (VPN), Internet Protocol Security (IPSec), serviços IPSec, combinação de VPN e Firewalls, vulnerabilidades VPN.	• Analisar Redes Privadas Virtuais.	• Sentido crítico.
• Segurança de redes wireless - ferramentas para detetar pontos de acesso de Rogue, Wired Equivalent Privacy (WEP), transporte sem fio Layer Security (WTLS) e segurança máxima.	• Analisar a segurança de redes wireless.	• Sentido de organização.
• Segurança de voz sobre IP – arquitetura, ameaças, vulnerabilidades e benefícios.	• Analisar a segurança de voz sobre IP	• Respeito pelas regras e normas definidas.
• Computação forense – ciência, evolução, objetivos, fundamentação, crime cibernético e desafios.	• Interpretar conceitos relacionados com computação forense.	
• Análise forense de redes e Routing – desafios, fontes de evidências, ferramentas de análise de tráfego, ferramentas para documentar provas, volatilidade da recolha de provas.	• Aplicar os procedimentos técnicos e funcionalidades das ferramentas de analise de tráfego.	
• Resposta forense a incidentes – informação preliminares, processo e política de resposta.	• Aplicar procedimentos metodológicos para desenvolver resposta forense a incidente.	
• Evidências digitais – características, fragilidades, tipos de dados e regulamentos de provas.	• Decifrar mensagens ocultas.	
• Esteganografia – definição, modelo, aplicação, classificação.	• Decifrar crimes realizados através de e-mail.	
• Esteganografia versus Criptografia	• Configurar mecanismos de salvaguarda.	
• Crimes através de e-mail e evidências informáticas	• Descrever os procedimentos aplicados na análise forense.	
• Relatório de investigação forense.	• Recolher e organizar informação para relatórios de investigação forense.	
• Normas de segurança e proteção de dados.	• Aplicar procedimentos de segurança e proteção de dados.	

Critérios de Desempenho

Instalar e configurar ferramentas de análise e recolha de logs e evidências

- Cumprindo regulamentos e normativos relativos a incidentes cibernéticos.
- Encontrando padrões e tendências que podem indicar uma violação da segurança.
- Cumprindo procedimentos técnicos para apoiar na elaboração do relatório de investigação forense.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos de Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ferramentas de análise.
- Editor de texto.

UC01486	Gerir sistemas de deteção de intrusos (IDS)
Pontos de crédito	4,5

Realizações

- **Instalar e configurar protocolos de autenticação**
- **Configurar equipamentos de IDS e firewall.**
- **Ativar os protocolos de segurança para conter a intrusão.**

Conhecimentos

- Ciberespaço -terminologia, tipos de ataque e de atacantes, métodos e técnicas de proteção.
- Cibersegurança - boas práticas, impacto, desktop e web.
- Regulação e enquadramento legal do ciberespaço.
- Impacto e boas práticas de segurança das redes sociais.
- Estratégia Nacional de cibersegurança e de ciberdefesa.
- Tecnologias emergentes
- Gestão dinâmica do risco

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Interpretar as componentes tangíveis e intangíveis do ciberespaço.
- Identificar as potenciais ciberameaças e os riscos para organizações.
- Interpretar o Plano de Segurança da organização.
- Identificar as boas práticas associadas à cibersegurança e ciberdefesa.
- Distinguir ferramentas de autenticação.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.

Conhecimentos	Aptidões	Atitudes
• Política de cibersegurança das organizações – finalidade, objetivos, linhas de ação a desenvolver. • Segurança da informação – relatórios de ameaças, vulnerabilidades web, terminologias comuns, estatísticas e ataques em sites para roubo da identidade. • Ameaças – características, tipos, tratamento, sniffing. • Passwords- mecanismos de autenticação, password cracker, modus operandi de um atacante; classificação de ataques, web password, senhas geradoras. • Criptografia – criptografia de chave pública, assinatura digital, RSA (Rivest Shamir Adleman), criptografia de disco, ataques e ferramentas. • Servidores e aplicações web – funcionamento, vulnerabilidades, ferramentas de deteção de vulnerabilidades IIS, vulnerabilidades apache, segurança do servidor web, falhas cross-site scripting/XSS, SQL injection, falhas de injeção e comandos. • Redes wireless – componentes, tipos, deteção, diretrizes de segurança. • Sistema de deteção de intrusão – tipos, sistema de integridade (SIV) e ferramentas de deteção. • Firewalls – características, funcionalidades e tipos. • Ciclo hacking – história, tipos e perfis do hacker • Hacking ético – classes, características e limitações • Segurança na rede – mapeamento internet protocol para OSI; ameaças e políticas de segurança. • Segurança nos protocolos de rede – protocolos de segurança E-mail – S/MIME e PGP, Protocolo de segurança web – SSL, SSH, HTTP e HTTPS. • Autenticação.	• Instalar e configurar Protocolos de autenticação, RADIUS e TACACS. • Utilizar sistemas de deteção de intrusão. • Configurar firewalls. • Utilizar a criptografia e assinaturas digitais. • Distinguir o hacking do hacking ético. • Aplicar procedimentos de segurança e proteção de dados.	• Respeito pelas regras e normas definidas.

Conhecimentos

- Validação e autenticação de equipamentos por radius server/ tacacs
- Normas de segurança e proteção de dados.

Critérios de Desempenho

Gerir sistemas de deteção de intrusos (IDS)

- Detetando e analisando as ameaças.
- Executando os protocolos de segurança.
- Cumprindo as regras e normas aplicáveis.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ferramentas de analise.
- Regulamento e normativos de proteção de dados.
- Editor de texto.

UC01487	Simular cenários de cibersegurança e ciberdefesa (wargamming)
Pontos de crédito	4,5

Realizações

- **Desenvolver procedimentos de segurança de informação.**
- **Instalar ambientes virtuais para simulações de cibersegurança e ciberdefesa.**

Conhecimentos	Aptidões	Atitudes
• Aspetos diferenciadores da cibersegurança e ciberdefesa.	• Interpretar manuais, guiões e tutoriais técnicos.	• Responsabilidade pelas suas ações e da sua equipa de trabalho
• Impacto estratégico e operacional das ciberameaças.	• Interpretar os diversos tipos de operações em redes e sistemas no contexto da cibersegurança e ciberdefesa.	• Autonomia no âmbito das suas funções e atribuições
• Operações em redes de computadores – defesas, ataques e exploração.	• Instalar e parametrizar ferramentas e soluções para garantir a cibersegurança e ciberdefesa em ambiente simulado virtual (Cyber Range)	• Trabalho em equipa
• Identificação de dados críticos para as organizações.	• Utilizar técnicas e ferramentas de testes de intrusão.	• Iniciativa
• A cadeia de ataque (KillChain).	• Testar diversas situações de ataque e abordagens de defesa e analisar a capacidade de resposta individual, da equipa e da organização.	• Rigor
• Articulação entre defesa e ataque – prevenir, detetar e responder.	• Desenvolver cenários de cibersegurança e ciberdefesa.	• Exatidão
• Defesa em profundidade.	• Identificar objetivos e possíveis audiências de treino.	• Sentido crítico
• Definição de métricas.	• Executar exercícios de simulação ("Capture The Flag" e "Red and Blue").	• Comportamento ético.
• Cenários de cibersegurança e ciberdefesa.	• Aplicar procedimentos de segurança e proteção de dados.	• Comunicação
• Exercícios de simulação ("Capture the Flag" e "Red and Blue") – utilização e enquadramento.		• Disposição para a aprendizagem.
• Normas de segurança e proteção de dados.		• Empenho e persistência na resolução de problemas.
		• Respeito pelas normas de segurança e proteção de dados.

Critérios de Desempenho

Simular cenários de cibersegurança e ciberdefesa (wargamming)

- Identificando incidentes associados a uma situação de crise.
- Construindo narrativas de acontecimentos.
- Aplicando os mecanismos de segurança

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.
- Organismos da Administração Pública.

Recursos

- Regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Ambiente de simulação.
- Editor de texto.

UC00616	Implementar as normas de segurança e saúde no trabalho no setor de Informática
Pontos de crédito	2,25

Realizações

- **Analisar os princípios gerais sobre segurança e saúde no trabalho.**
- **Aplicar medidas e procedimentos de segurança e saúde no trabalho.**

Conhecimentos

- Princípios de segurança e saúde no trabalho.
- Normas e disposições relativas à segurança e saúde no setor da informática – legislação.
- Plano de segurança do estabelecimento.
- Plano de prevenção de acidentes.
- Plano de prevenção de incêndios.
- Plano de evacuação.
- Plano contra roubos.
- Manuais de segurança.
- Meios e regras de segurança na informática –
- Equipamentos de proteção individual (EPI), métodos de supressão da negligência e falta de atenção, proteção de equipamentos de trabalho e ergonomia.
- Regras de segurança no manuseamento de equipamento e na movimentação de materiais - normas do vestuário, prevenção de choques elétricos, movimentação de cargas pesadas.

Aptidões

- Identificar as normas relativas à segurança e saúde no trabalho.
- Interpretar o plano de segurança do estabelecimento.
- Reconhecer os manuais de segurança.
- Aplicar medidas de prevenção do risco.
- Aplicar os procedimentos em caso de acidente de trabalho.
- Aplicar os procedimentos de emergência.
- Aplicar medidas de prevenção de roubo.
- Distinguir os diferentes tipos de incêndio e respetivos sistemas de deteção e de extinção.
- Aplicar medidas de prevenção de incêndios.
- Utilizar o extintor.
- Utilizar equipamentos de proteção individual.
- Reportar a situação de emergência.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções.
- Autocontrolo.
- Autocontrolo.
- Sentido de organização.
- Cooperação com a equipa.
- Respeito pelas normas de segurança.

Conhecimentos

- Causas de acidentes no trabalho - acidentes de movimentação, choques e quedas, acidentes provocados por ferramentas e máquinas em movimento, choques elétricos, acidentes provocados por agentes químicos e queimaduras.
- Caixa de primeiros socorros.
- Situações de emergência - perda de sentidos, feridas aberta e fechada, choque elétrico, eletrocussões, ataque cardíaco, entorses ou distensões, envenenamento, queimaduras.
- Causas de incêndio - sistema de aquecimento e cozedura, chaminé e tubos de fumo, materiais inflamáveis, aparelhos elétricos, trabalhadores e outras pessoas fumadoras.
- Tipos de incêndio.
- Sistemas de deteção.
- Tipos de extintores.
- Incêndio - plano de ataque, manipulação de extintores, acionamento do sistema automático.
- Técnicas de extinção de incêndio de gás.

Critérios de Desempenho

Implementar as normas de segurança e saúde no trabalho no setor de Informática

- Considerando os tipos de risco existentes no posto de trabalho e respetivas medidas de segurança e preventivas.
- Cumprindo as medidas de atuação em situação de emergência.
- Respeitando o protocolo interno definido.

Contexto (de uso de competência)

- Organizações do setor da informática.
- Espaço do cliente.

Recursos

- Dispositivos tecnológicos com acesso à Internet.

- Legislação sobre segurança e saúde no trabalho.
- Normativos específicos de segurança e saúde no trabalho.
- Documentação sobre segurança e saúde no trabalho (relatórios, folhetos, brochuras, outros).
- Equipamentos de proteção individual (EPI).
- Planos de prevenção de acidentes, de incêndios, de evacuação e de roubo.
- Planos de emergência.
- Equipamento de sinalização.

UC OPCIONAIS

UC00033	Comunicar e interagir em contexto profissional
Pontos de crédito	4,5

Realizações

- **Preparar a mensagem a comunicar em contexto profissional.**
- **Informar e esclarecer diferentes interlocutores em contexto presencial e não presencial.**

Conhecimentos

- Princípios da comunicação e do relacionamento interpessoal – processo, funções e elementos intervenientes.
- Fatores facilitadores e inibidores da comunicação.
- Comunicação verbal (oral e escrita) e comunicação não-verbal – cinésica (movimentos corporais, gestos, expressão facial e postura), paralinguística (tom, projeção da voz, pausas no discurso, sorriso, outros) e proxémica (distância espacial face a alguém).
- Canais de comunicação presencial e não presencial.
- Comunicação telefónica - técnicas de atendimento telefónico, expressão verbal e sorriso "telefónico".
- Comunicação através da internet (navegadores, e-mail, redes sociais, mensagens) – técnicas.

Aptidões

- Organizar a informação a comunicar.
- Adaptar a comunicação oral e escrita ao interlocutor e ao contexto.
- Interpretar informação de diferentes interlocutores em contexto presencial e não presencial.
- Identificar as expectativas do interlocutor.
- Utilizar técnicas de comunicação verbal e não verbal assertiva.
- Formular questões, pedir esclarecimentos ou colocar dúvidas para interpretar e/ou explicitar a mensagem.
- Partilhar informação com diferentes interlocutores.
- Reportar informação profissional.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Cuidado com a imagem e postura profissional.
- Assertividade.
- Escuta ativa.
- Empatia.
- Controlo emocional.
- Autoconfiança.
- Respeito pela diferença.
- Autoconhecimento.
- Sentido crítico.

Conhecimentos	Aptidões	Atitudes
• Comunicação escrita – normas. • Processo de escrita - planificação, textualização e revisão. • Caraterísticas dos estilos de comunicação - agressivo, passivo, manipulador, assertivo. • Comunicação assertiva – vantagens, componentes verbais e não-verbais, técnicas. • Escuta ativa, empatia e controlo emocional. • Processamento interno da informação – fonético, literal (significado) e reflexivo (empático). • Perguntas no processo de comunicação – abertas, fechadas, retorno, reformulação. • Mensagem - construção, adaptação, envio, receção e interpretação. • Imagem e comunicação – autoimagem e autoconceito, primeiras impressões, expectativas e motivação. • Técnicas de programação neurolinguística (PNL) na comunicação. • Relações interpessoais no trabalho. • Conflito nas relações interpessoais – tipos e técnicas de resolução de conflitos. • Avaliação do processo de comunicação – *feedback*, resposta e reação.	• Aplicar técnicas de interação orais e escritas. • Aplicar técnicas de tratamento e resolução de conflitos. • Autoavaliar o seu desempenho no âmbito do processo de comunicação.	• Cooperação com a equipa. • Sentido de organização.

Critérios de Desempenho

Comunicar e interagir em contexto profissional

- Adaptando a linguagem e a comunicação ao tipo de canal utilizado, ao público-alvo e ao contexto.
- Demonstrando assertividade e uma imagem positiva de si e da sua organização.
- Demonstrando uma comunicação verbal e não verbal empática e ajustada ao interlocutor.
- Produzindo um texto escrito de forma clara e articulada, de acordo com a norma, aplicando técnicas de redação de documentos profissionais.

- Avaliando o resultado do seu desempenho e contributo para a melhoria do processo de comunicação.

Contexto (de uso de competência)

- Aplicável a diferentes contextos.

Recursos

- Dispositivos tecnológicos com acesso à internet.
- Recursos multimédia e audiovisuais.
- Ferramentas de interação e de comunicação.
- Boas práticas na comunicação.

UC00034	Colaborar e trabalhar em equipa
Pontos de crédito	4,5

Realizações

- **Analisar a identidade pessoal e partilhada e respetivos comportamentos associados.**
- **Colaborar na aplicação de dinâmicas facilitadoras do trabalho em equipa.**
- **Colaborar na definição de estratégias de resolução de problemas e de tomada de decisão.**

Conhecimentos

- Identidade pessoal, social e profissional.
- Fenómenos da dinâmica de grupo - influência social e papel social, normas sociais, atitudes e comportamentos facilitadores e dificultadores, padrão de grupo e motivação individual.
- Trabalho em equipa - fatores pessoais, relacionais e organizacionais.

Aptidões

- Identificar e analisar os estilos comportamentais individuais.
- Identificar as competências individuais.
- Identificar os papéis dos membros da equipa - competências e responsabilidades.
- Reconhecer a fase de desenvolvimento de competências na qual a equipa se encontra.
- Identificar os valores e as principais competências necessários para a equipa atingir o(s) objetivo(s) traçado(s).

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Autoconhecimento.
- Automotivação.
- Assertividade.
- Empatia.
- Escuta ativa.
- Cooperação com a equipa.

Conhecimentos	Aptidões	Atitudes
• Equipa de trabalho - princípios de organização de grupo *vs.* equipa de trabalho, estilos comportamentais, estrutura e fases de desenvolvimento da equipa, perceção de desempenho individual, formas e técnicas de organização, cooperação e colaboração.	• Colaborar na definição dos mecanismos de coesão e controlo na equipa.	• Empenho e persistência na resolução de problemas.
• Comunicação assertiva - verbal e não-verbal, fatores facilitadores e inibidores.	• Colaborar na definição de tarefas e prazos para alcançar os objetivos traçados.	• Sentido critico.
• Canais de comunicação presencial e não presencial.	• Participar na execução de tarefas predefinidas para a equipa.	• Sentido criativo.
• Importância da comunicação no trabalho entre equipas - fluxos de comunicação, comunicação vertical e horizontal, *feedback* do desempenho.	• Aplicar técnicas de comunicação em diferentes contextos.	• Flexibilidade e adaptabilidade.
• Técnicas de negociação, de resolução de problemas e de tomada de decisão.	• Utilizar ferramentas de comunicação.	• Respeito e valorização das diferenças individuais.
• Gestão de tempo – técnicas, planeamento, autoavaliação e otimização das tecnologias.	• Partilhar informação presencialmente e/ou *online*.	• Respeito pela sensibilidade e bem-estar dos outros.
• Trabalho *online* ou teletrabalho - condições facilitadoras, equipas 4D e atitude partilhada.	• Formular ideias e sugestões em diferentes contextos comunicacionais.	• Respeito pelas regras e normas definidas.
• Saúde no trabalho - síndroma de b*urnout*.	• Trocar conhecimentos e experiências.	
• Organização das equipas na área profissional.	• Identificar os princípios subjacentes à tomada de decisão.	
	• Analisar problemas e tomar decisões.	
	• Desenvolver rotinas em equipa em momentos formais, informais, presenciais e online.	
	• Reconhecer sinais de *burnout* próprio e/ou dos colegas.	

Critérios de Desempenho

Colaborar e trabalhar em equipa

- Mobilizando os recursos pessoais para a obtenção dos melhores resultados da equipa.
- Aplicando técnicas de comunicação e negociação adequadas aos interlocutores e ao contexto.
- Analisando problemas e propondo soluções.
- Gerando oportunidades de desenvolvimento e aprendizagem colaborativa.

Contexto (de uso de competência)

- Aplicável a diferentes contextos.

Recursos

- Dispositivos tecnológicos com acesso à internet.
- Ferramentas de interação, de comunicação e produtividade.
- Recursos multimédia e audiovisuais.
- Boas práticas na comunicação.

UC00600	Analisar as funções e estrutura da organização
Pontos de crédito	2,25

Realizações

- **Caracterizar a estrutura organizacional.**
- **Elaborar organigramas.**
- **Implementar medidas de gestão e planeamento.**

Conhecimentos

- Empresa: conceito e evolução; classificação; ética, qualidade e responsabilidade social
- Constituição de uma empresa – etapas, instituições, teorias organizacionais – organização e gestão do trabalho.
- Estruturas organizacionais - conceito, tipos, organigramas.
- Comunicação organizacional – conceitos, tipos e regras.
- Planeamento – objetivos, tipos e gestão de tempo.
- Aplicações digitais para elaboração organogramas e cronogramas.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar normativos e regras empresariais.
- Diferenciar os tipos de empresa.
- Reconhecer as diferentes etapas da constituição de uma empresa.
- Identificar hierarquias e distinguir funções.
- Caracterizar os fluxos de trabalho.
- Utilizar técnicas para estruturar organigramas.
- Reconhecer os diferentes tipos de canais de comunicação
- Utilizar o protocolo de comunicação da empresa
- Elaborar cronogramas de planeamento tarefas.
- Usar procedimentos e técnicas de planeamento numa empresa.
- Aplicar normas e regulamentos.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Conduta profissional.
- Empenho e persistência.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Analisar as funções e estrutura da organização

- Identificando a estrutura organizacional.
- Aplicando os critérios de classificação.
- Reconhecendo os processos de trabalho.
- Propondo medidas para melhorar a eficiência.

Contexto (de uso de competência)

- Aplicável a diferentes contextos pessoais e profissionais.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos tecnológicos com acesso à internet.
- Documentos estratégicos e operacionais da organização (plano estratégico, plano de atividades, manual de qualidade, regulamentos).
- Aplicações digitais para elaboração de organogramas e planeamento.

UC00613	Gerir políticas de segurança em sistemas informáticos
Pontos de crédito	2,25

Realizações

- **Configurar mecanismos de segurança no sistema de rede.**
- **Monitorizar a segurança do sistema.**
- **Realizar cópias de segurança.**

Conhecimentos	Aptidões	Atitudes
• Segurança da informação – conceitos, vulnerabilidades, ameaças e ataques; políticas e mecanismos de segurança; segurança em sistemas distribuídos; criptografia, gestão de chaves.	• Interpretar manuais, guiões e tutoriais técnicos.	• Responsabilidade pelas suas ações e pelas de terceiros.
	• Instalar ferramentas de monitorização.	• Autonomia no âmbito das suas funções.
• Firewall – tipologia, implementação.	• Utilizar ferramentas de diagnóstico e análise de redes.	• Empenho e persistência na resolução de problemas.
• Sistemas de deteção de intrusões (IDS) – arquitetura, classificação e aplicação.	• Configurar parâmetros de rede.	• Ética.

Conhecimentos	Aptidões	Atitudes
• Redes privadas virtuais (VPN) – tipos, dispositivos, túneis e protocolos, estabelecimentos. • Regulamento geral de proteção de dados. • Normas e regulamentos aplicáveis.	• Aplicar autenticação e criptografia a ligações de rede. • Executar as operações técnicas necessárias para a segurança dos equipamentos ligados à rede. • Gerir uma firewall. • Planear e configurar a realização de backups de segurança. • Configurar redes privadas virtuais. • Detetar anomalias decorrentes de ataques ou tentativas de ataques. • Bloquear conteúdos indevidos. • Aplicar normas e regulamentos.	• Proatividade. • Sentido de organização. • Rigor • Respeito pelas regras e normas definidas.

Critérios de Desempenho

Gerir políticas de segurança em sistemas informáticos

- Aplicando medidas de segurança relativas à confidencialidade, integridade e disponibilidade de dados.
- Operando com as ferramentas de análise do estado e monitorização do sistema.
- Planeando a realização de cópias de segurança com regularidade.

Contexto (de uso de competência)

- Empresas do setor da informática e redes.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos tecnológicos com acesso à Internet.
- Servidor.
- Software de monitorização.

UC01488	Gerir a segurança da informação e criptografia
Pontos de crédito	2,25

Realizações

- **Planear a implementação de políticas de segurança.**
- **Criar sistemas criptográficos para a organização.**
- **Implementar mecanismos de cifra e autenticação.**

Conhecimentos	Aptidões	Atitudes
• Conceitos básicos de segurança dos sistemas de informação	• Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.	• Responsabilidade pelas suas ações e pelas de terceiros.
• Normas de segurança de informação ISSO 27001	• Interpretar os conceitos relacionados com segurança da informação.	• Autonomia no âmbito das suas funções.
• Organizações relacionadas com segurança da informação	• Identifica e avalia o nível de risco de ataques cibernéticos.	• Empenho e persistência na resolução de problemas.
• Políticas de Segurança	• Utilizar procedimentos técnicos para implementar políticas de segurança.	• Ética.
• Análise de Risco	• Configurar funcionalidades para garantir a confidencialidade, disponibilidade e integridade da informação na organização.	• Proatividade.
• Auditoria à Segurança	• Implementar protocolos seguros nas organizações.	• Sentido de organização.
• Criptografia Simétrica	• Efetuar uma auditoria à segurança de informação.	• Rigor
• Criptografia Assimétrica	• Executar procedimentos de resposta a incidentes.	• Respeito pelas regras e normas definidas.
• Tipos de criptografia.	• Aplicar normas e regulamentos.	
• Funções Hash e Autenticação		
• Infraestruturas de Chave Pública		
• Aplicações de diversas técnicas criptográficas		
• Normas e regulamentos aplicáveis.		

Critérios de Desempenho

Gerir a segurança da informação e criptografia

- Garantindo que os procedimentos de segurança e a criptografia estejam em conformidade com a legislação aplicável.
- Analisando o risco e implementando controlos de criptografia em conformidade.
- Monitorizando os sistemas para detetar possíveis vulnerabilidades.

Contexto (de uso de competência)

- Empresas do setor da informática e redes.

- Serviços de apoio técnico.
- Organismos da Função Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos tecnológicos com acesso à Internet.
- Servidor.
- Software de rede.

UC01489	Implementar procedimentos de recolha e análise forense digital
Pontos de crédito	4,5

Realizações

- **Planear a recolha e análise forense.**
- **Analisar um ataque ou incidente de um ponto de vista forense.**
- **Utilizar técnicas e procedimentos para preservar a prova.**

Conhecimentos

- Análise forense – fundamentos, metodologia e tipos de dados
- Legislação aplicável em termos de prova.
- Validade e admissibilidade da prova digital.
- Meios de prova.
- Meios de obtenção de prova.
- Etapas e respetivas ferramentas – recolha, preservação, análise e apresentação.
- Plataformas de análise forense digital.
- Análise forense de sistemas, sistemas Windows, Linux, Mac e sistemas móveis.

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Interpretar os fundamentos da análise forense.
- Interpretar os requisitos de validade e admissibilidade da prova digital.
- Utilizar orientações metodológicas para planear as etapas de recolha e analise forense.
- Interpretar os trâmites durante todo o processo de análise forense.
- Usar técnicas e as funcionalidades das aplicações para recolha e analise forense.
- Recolher, através de software de captura de dados, de discos, memórias e/ou pacotes de rede.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Proatividade.
- Sentido de organização.
- Rigor
- Respeito pelas regras e normas definidas.

Conhecimentos	Aptidões
• Análise forense de redes de comunicação, análise de dados da rede, análise dos sistemas de gestão ativos. • Análise forense em bases de dados e em ambientes cloud. • Análise forense em equipamentos móveis e IOT. • Normas e regulamentos aplicáveis.	• Utilizar procedimentos técnicos para identificação, recolha e aquisição de registos e informação. • Aplicar procedimentos para preservar a prova. • Produzir relatórios das diferentes fases da análise. • Aplicar normas e regulamentos.

Critérios de Desempenho

Implementar procedimentos de recolha e análise forense digital

- Cumprindo as diferentes etapas do processo de análise forense.
- Cumprindo as orientações e técnicas para preservar a prova.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Editor de texto.
- Software específico de captura de dados.
- Processador de texto.

UC01490	Executar técnicas de hacking ético
Pontos de crédito	2,25

Realizações

- **Planear e executar testes de invasão.**
- **Detetar riscos e vulnerabilidades em equipamentos, redes e sistemas.**

Realizações

- **Elaborar relatórios técnicos.**

Conhecimentos

- Hacking ético - conceitos.
- Código de ética dos hackers éticos.
- Diretrizes gerais para a criação do código de ética.
- Segurança da informação e proteção dos dados – normas nacionais e internacionais, legislação e regulamento geral de proteção de dados.
- Hackers éticos versus outros tipos de hackers.
- Funções do hacking ético – testes de penetração ou "pentestes", engenharia social, hacking web sites, hacking redes wireless, hacking smartphones, hacking DDoS e DOS.
- Arquitetuta de redes.
- Sistemas operativos.
- Testes de Penetração – ferramentas, metodologias e relatórios.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar regulamentos, normativos, manuais, guiões e tutoriais técnicos.
- Interpretar os conceitos relacionados com hacking ético
- Aplicar as diretrizes gerais para a criação do código de ética.
- Distinguir o hacking ilegal do hacking ético.
- Interpretar legislação relativa à segurança dos sistemas e proteção de dados.
- Usar procedimentos técnicos para avaliar as políticas e medidas de segurança.
- Executar testes em ciclos.
- Aplicar as normas éticas e legais do hacking ético.
- Analisar vulnerabilidades e aplicar medidas de mitigação.
- Aplicar estratégias durante os testes para superar obstáculos.
- Produzir relatórios com os resultados dos testes de invasão.

Atitudes

- Responsabilidade pelas suas ações e pelas de terceiros.
- Autonomia no âmbito das suas funções e atribuições.
- Cooperação com a equipa.
- Empenho e persistência na resolução de problemas.
- Ética.
- Rigor.
- Sentido crítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Executar técnicas de hacking ético

- Cumprindo as diretrizes gerais do código de ética.
- Cumprindo a legislação relativa à segurança da informação e proteção de dados.
- Reportando as vulnerabilidades encontradas, propondo soluções práticas e seguras.

Contexto (de uso de competência)

- Empresas do setor da informática e cibersegurança.
- Serviços de apoio técnico.
- Consultoria TI.

- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.

UC00627	Instalar e configurar servidores Web
Pontos de crédito	2,25

Realizações

- **Efetuar a instalação e configuração de um servidor Intranet e Internet em ambiente web.**
- **Efetuar a manutenção e atualização do servidor intranet e Internet em ambiente web.**

Conhecimentos

- Servidores web – conceitos.
- Domínio web.
- Alojamento web.
- Estrutura de servidor web.
- Serviços FTP, CHAT, entre outros serviços.
- Gestão de servidores locais e remotos.
- Gestão de utilizadores.
- Normas de segurança da gestão de informação.
- Segurança dos utilizadores.
- Regulamento geral de proteção de dados.
- Normas e regulamentos aplicáveis.

Aptidões

- Interpretar manuais, guiões e tutoriais técnicos.
- Utilizar metodologias de planeamento e desenho da estrutura de um servidor web.
- Configurar as funcionalidades e serviços FTP, CHAT, entre outros.
- Realizar a manutenção do servidor e serviços.
- Configurar ferramentas de gestão remota do servidor.
- Definir privilégios dos perfis dos utilizadores.
- Interpretar normas e procedimentos de gestão e segurança da informação.
- Aplicar procedimentos de segurança na configuração e manutenção de um servidor intranet e Internet em ambiente web.
- Aplicar normas e regulamentos.

Atitudes

- Responsabilidade pelas suas ações.
- Autonomia no âmbito das suas funções.
- Empenho e persistência na resolução de problemas.
- Iniciativa.
- Sentido analítico.
- Sentido de organização.
- Respeito pelas regras e normas definidas.

Critérios de Desempenho

Instalar e configurar servidores Web

- Seguindo as orientações técnicas na instalação e na seleção das opções para os serviços.
- Cumprindo os procedimentos de manuseamento e segurança.

Contexto (de uso de competência)

- Empresas do setor da informática.
- Empresas de consultoria de Informática/Tecnologias de Informação.
- Lojas de informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Manuais, guiões e tutoriais técnicos.
- Dispositivos eletrónicos com acesso à Internet.
- Domínio na web.
- Alojamento web.
- Software.

UC01491	Projetar e administrar sistemas de bases de dados
Pontos de crédito	4,5

Realizações

- **Planear a arquitetura de uma base de dados.**
- **Efetuar a programação.**
- **Executar tarefas de administração de base de dados.**

Conhecimentos	Aptidões	Atitudes
• Base de dados – arquitetura, ligações e técnicas de otimização	• Interpretar manuais, guiões e tutoriais técnicos.	• Responsabilidade pelas suas ações e pelas de terceiros.
• Estruturas em memória.	• Avaliar a arquitetura de uma base de dados.	• Autonomia no âmbito das suas funções e atribuições.
• Espaço em disco.	• Identificar os fatores que influenciam a performance da base de dados.	• Cooperação com a equipa.
• Controlo de acesso – perfis e privilégios dos utilizadores.	• Identificar os parâmetros que influenciam a segurança e desempenho da base de dados.	• Empenho e persistência na resolução de problemas.
• Monitorização do funcionamento da base de dados.		• Ética.

Conhecimentos	Aptidões	Atitudes
• Exportação e importação de dados.	• Aplicar técnicas para otimização do desempenho de uma base de dados.	• Rigor.
• Segurança da informação – normas de gestão e segurança da informação e proteção dos dados sensíveis, backups, atualizações.	• Configurar das ligações à base de dados.	• Sentido crítico.
• Normas e regulamentos aplicáveis.	• Analisar e configurar o funcionamento das estruturas em memória.	• Sentido de organização.
	• Gerir espaço em disco.	• Respeito pelas regras e normas definidas.
	• Gerir os privilégios de acesso para os perfis de utilizador.	
	• Analisar o funcionamento da base de dados.	
	• Aplicar técnicas para efetuar a importação ou exportação de uma base de dados.	
	• Interpretar e aplicar normas e procedimentos de gestão da segurança da informação e proteção de dados sensíveis.	
	• Planear e configurar a realização de backups dos dados.	
	• Aplicar técnicas para efetuar a reposição de uma base de dados.	
	• Atualizar e manter as aplicações.	
	• Aplicar normas e regulamentos.	

Critérios de Desempenho

Projetar e administrar sistemas de bases de dados

- Analisando eventuais falhas de segurança numa base de dados e corrigindo-a
- Efetuando testes de desempenho da base de dados
- Realizando backups de bases de dados existentes
- Efetuando a reposição de uma base de dados

Contexto (de uso de competência)

- Empresas do setor da informática.
- Serviços de apoio técnico.
- Organismos da Administração Pública.

Recursos

- Dispositivos tecnológicos com acesso à Internet.
- Ferramentas de programação de bases de dados