Ministério das Finanças
e do Fomento Empresarial
Unidade de Coordenação do
Sistema Nacional de Qualificações

SISTEMA NACIONAL DE QUALIFICAÇÕES

Qualificação Profissional

MONTAGEM E MANUTENÇÃO DE SISTEMAS INFORMÁTICOS

TIC003.A1_3

Família Profissional Tecnologias de Informação e Comunicação

Ficha Técnica

Unidade de Coordenação do Sistema Nacional de Qualificações (UC-SNQ)

Coordenador da UC-SNQ
Amílcar Alexandre Mendes

Família Profissional: Tecnologias de Informação e Comunicação

Coordenador(a) da Família Profissional

Agosto 2025

Apoio ao utilizador

Telefone: +238 333 70 55/76/61 | E-Mail: snqcv.uc@gmail.com | Website: www.snq.cv

Siglas e Acrónimos

TIC	Tecnologias de Informação e Comunicação
UC	Unidades de Competência
EC	Elementos de Competência
CD	Critérios de Desempenho
RAM	Random Access Memory
BIOS	Basic Input/Output System
UEFI	Unified Extensible Firmware Interface
SSD	Solid State Drive
USB	Universal Serial Bus
HDMI	High-Definition Multimedia Interface
VLAN	Virtual Local Area Network
ISO	International Organization for Standardization
EIA	Environmental Impact Assessment
IEEE	Institute of Electrical and Electronics Engineers
UPS	Uninterruptible Power Supply
IA	Inteligência Artificial

ÍNDICE

PERFIL PROFISSIONAL 5
UNIDADES DE COMPETÊNCIA (UC) 7
UC1: Realizar operações de montagem de sistemas informáticos. 7
UC2: Realizar operações de manutenção de sistemas informáticos. 10
UC3: Executar operações com ferramentas de escritório e IA. 0
UC4: Instalar, configurar e conectar equipamentos em redes locais. 4
UNIDADES FORMATIVAS TRANSVERSAIS 10
Unidade formativa : Inglês Técnico UF524 ? 10
MÓDULOS FORMATIVOS (MF) 13
MF1: Montagem e Configuração de Sistemas Informáticos 13
Unidade Formativa 1: Arquitetura de Computadores (UF492) 13
Unidade Formativa 2: Montagem e Manutenção de Sistemas Informáticos (UF493) 16
MF2: Operações de Manutenção de Sistemas Informáticos 20
MF3: Gestão de Informação e Documentação com Aplicações de Office e IA 24
Unidade Formativa 1: Manipulação de Informação com Ferramentas Office e IA (UF488) 24
Unidade Formativa 2: Produção e Edição de Conteúdos Multimédia (UF489) 29
MF4: Instalação de Redes de Área Local 32
Unidade Formativa 1: Principios das Redes de Área Local (UF257.1) 32
Unidade Formativa 2: Equipamentos de Interconexão (UF260.1) 34
MF5: MANUTENÇÃO DA SEGURANÇA NO SISTEMA INFORMÁTICO (MF176_3) 37
Unidade formativa 1: Procedimentos de Segurança no Sistema Informático UF261.1 37
MÓDULO FORMATIVO EM CONTEXTO REAL DE TRABALHO 42
MT_TIC003.A1 42

PERFIL PROFISSIONAL

TIC003.A1_3

MONTAGEM E MANUTENÇÃO DE SISTEMAS INFORMÁTICOS

<table>
<tr><th colspan="5">PERFIL PROFISSIONAL</th></tr>
<tr><td>Código</td><td>TIC003.A1_3</td><td>Denominação</td><td colspan="2">MONTAGEM E MANUTENÇÃO DE SISTEMAS INFORMÁTICOS</td></tr>
<tr><td>Nível</td><td>3</td><td>Família Profissional</td><td colspan="2">Tecnologias de Informação e Comunicação (TIC)</td></tr>
<tr><td colspan="2">COMPETÊNCIA GERAL</td><td colspan="3">Executar atividades de montagem e manutenção de sistemas informáticos, seguindo padrões de qualidade, segurança e sustentabilidade, em conformidade com normas e procedimentos técnicos predefinidos.</td></tr>
<tr><td colspan="2" rowspan="6">UNIDADES DE COMPETÊNCIA</td><td>N.º</td><td>Denominação</td><td>Código</td></tr>
<tr><td>1</td><td>Realizar operações de montagem de sistemas informáticos.</td><td>UC381_3</td></tr>
<tr><td>2</td><td>Realizar operações de manutenção de sistemas informáticos.</td><td>UC382_3</td></tr>
<tr><td>3</td><td>Executar operações com ferramentas de escritório e IA.</td><td>UC379_3</td></tr>
<tr><td>4</td><td>Instalar, configurar e conectar equipamentos em redes locais.</td><td>UC175.1_3</td></tr>
<tr><td>5</td><td>Manter a segurança de um sistema informático.</td><td>UC176.1_3</td></tr>
<tr><td colspan="2" rowspan="2">AMBIENTE PROFISSIONAL</td><td colspan="3">Âmbito profissional:

O profissional exerce funções na área de suporte técnico, integrado em empresas de Tecnologias de Informação e Comunicação (TIC), podendo tratar-se de entidades públicas ou privadas, de qualquer dimensão, com principal enfoque em serviços de informática. Pode desempenhar a sua atividade como trabalhador independente ou por conta de outrem, independentemente da forma jurídica da organização. No âmbito das suas tarefas, o profissional pode atuar sob orientação funcional ou hierárquica de um superior, sempre que tal se aplique. Adicionalmente, no desenvolvimento do seu trabalho, são respeitados e aplicados os princípios da acessibilidade universal, em estrita conformidade com as normas e regulamentações vigentes.</td></tr>
<tr><td colspan="3">Setores:

O profissional atua principalmente no setor dos serviços, em subsetores dedicados à montagem, manutenção, reparação e comercialização, de equipamentos e serviços de informática. Inclui-se também a assistência técnica em informática, a integração em redes de telecentros e a intervenção em setores que utilizam sistemas informáticos para gestão. A sua atividade estende-se a áreas como telecomunicações, finanças, educação e saúde, contribuindo para a otimização de processos e resolução de problemas técnicos. O profissional implementa soluções tecnológicas, apoia a utilização de ferramentas digitais e assegura o bom funcionamento dos sistemas, cumprindo normas de segurança, qualidade e sustentabilidade.</td></tr>
</table>

PERFIL PROFISSIONAL	
	Ocupações e postos de trabalho relacionados: CNP 2010: ● 3511 Técnico das tecnologias de informação e comunicação (TIC). ● 3512 Técnico de apoio aos utilizadores das TIC. Sugestões: ● Técnico de reparação de computadores. ● Técnico auxiliar na instalação de redes locais. ● Operador de sistemas informáticos.

UNIDADES DE COMPETÊNCIA (UC)

UC1: Realizar operações de montagem de sistemas informáticos.	
Código: UC381_3	Nível: 3

Elementos de Competência (EC) e Critérios de Desempenho (CD)

EC 1: Realizar tarefas de montagem e substituição de componentes de *hardware* de equipamentos informáticos, seguindo a documentação técnica do fabricante e as instruções recebidas para garantir o funcionamento do equipamento.

CD 1.1. Os componentes de hardware dos equipamentos informáticos são instalados ou substituídos utilizando ferramentas adequadas e elementos de proteção, conforme as especificações do fabricante, para garantir a fixação correta e a segurança do processo.

CD 1.2. As ligações dos componentes de hardware dos equipamentos informáticos são verificadas quanto à conexão com cabos de dados e energia, seguindo rigorosamente as instruções e boas práticas de manuseio e segurança, para assegurar a conformidade com as especificações dos guias de instalação.

CD 1.3. A compatibilidade entre os componentes de hardware é verificada, analisando especificações técnicas e requisitos do sistema para garantir uma montagem correta e funcional.

CD 1.4. Os procedimentos de aterramento e descarga eletrostática são aplicados, utilizando pulseiras antiestáticas e superfícies adequadas para evitar danos nos componentes eletrónicos.

CD 1.5. O funcionamento do equipamento deve ser testado após a montagem ou substituição de componentes, verificando o correto desempenho do sistema para assegurar que atende aos requisitos técnicos estabelecidos.

CD 1.6. Os resíduos e componentes descartáveis resultantes da substituição de hardware devem ser separados e geridos, sendo depositados nos locais designados pela organização, em conformidade com as normas ambientais e de gestão de resíduos aplicáveis, para garantir a sustentabilidade do processo.

EC 2: Executar operações de montagem, substituição e ligação de dispositivos externos a um sistema informático, seguindo as especificações técnicas recebidas, de modo a facilitar a utilização e a transmissão de informação com o sistema.

CD 2.1. Os dispositivos externos devem ser ligados utilizando os cabos e conectores indicados pelo fabricante, assegurando que as conexões sejam feitas de acordo com as especificações técnicas fornecidas, para garantir um funcionamento adequado.

CD 2.2. As tarefas realizadas e os incidentes detetados devem ser registados conforme os procedimentos internos da organização, utilizando modelos (templates), ferramentas de software ou outros métodos definidos, para garantir a rastreabilidade das atividades.

CD 2.3. Os dispositivos externos substituídos e os resíduos descartáveis devem ser eliminados ou reciclados, sendo depositados nos locais designados pela organização, em conformidade com as normas de gestão de resíduos e sustentabilidade, para minimizar o impacto ambiental.

CD 2.4. Os cabos de alimentação e dados são organizados e fixados, utilizando braçadeiras ou canais específicos para melhorar o fluxo de ar e facilitar futuras manutenções.

CD 2.5. Os sistemas de arrefecimento (ventoinhas, dissipadores, pasta térmica) são instalados corretamente, garantindo a dissipação térmica eficiente para evitar sobreaquecimento dos componentes.

CD 2.6. Os módulos de memória RAM são inseridos corretamente, respeitando os encaixes e

verificando a ativação de canais duplos ou outras tecnologias para otimizar o desempenho.

EC 3: Executar tarefas de monitorização utilizando programas de diagnóstico, seguindo guias e instruções detalhadas recebidas, com o objetivo de verificar o correto funcionamento dos equipamentos e dos dispositivos externos.

CD 3.1. A funcionalidade dos componentes de hardware e dispositivos externos é verificada utilizando ferramentas de diagnóstico de hardware ou software, confirmando se os valores obtidos estão de acordo com as especificações indicadas, para garantir a integridade do equipamento.

CD 3.2. O sistema informático completo é testado realizando os testes recomendados pelo fabricante para verificar a sua funcionalidade global, assegurando que os resultados obtidos estão dentro dos parâmetros esperados, para garantir o correto desempenho do sistema.

CD 3.3. Os parâmetros de desempenho dos componentes de hardware ou dispositivos externos são avaliados utilizando ferramentas de software de monitorização específicas, confirmando se estão em conformidade com os valores de referência estabelecidos, para garantir a eficiência operacional.

CD 3.4. As atualizações de firmware e drivers dos equipamentos são verificadas e aplicadas conforme necessário, utilizando software apropriado, para garantir que os sistemas operam com as versões mais recentes recomendadas pelos fabricantes.

CD 3.5. Os dispositivos externos (impressoras, scanners, discos externos) são configurados e testados, para garantir a sua funcionalidade antes da entrega ao utilizador final.

CD 3.6. Os alertas ou erros gerados pelos sistemas de diagnóstico são analisados e solucionados aplicando procedimentos corretivos adequados e reportando falhas críticas conforme os protocolos estabelecidos, para garantir a estabilidade e funcionalidade dos equipamentos.

EC 4: Validar e testar a montagem do sistema, assegurando a sua funcionalidade antes da entrega ao utilizador final.

CD 4.1. A integridade física dos componentes montados é verificada para assegurar que todas as conexões estão devidamente encaixadas e fixadas conforme as especificações do fabricante.

CD 4.2. Os testes de inicialização do sistema são efetuados, para garantir que o hardware é corretamente reconhecido pela BIOS/UEFI e que não existem mensagens de erro críticas.

CD 4.3. Os diagnósticos básicos de hardware e software são executados utilizando ferramentas apropriadas para identificar eventuais falhas nos componentes instalados.

CD 4.4. A funcionalidade dos dispositivos periféricos conectados é testada em elementos como teclado, rato, monitor, armazenamento externo e interfaces de comunicação.

CD 4.5. A ventilação e refrigeração do sistema é verificada monitorizando a temperatura e o funcionamento das ventoinhas para evitar sobreaquecimento.

CD 4.6. A conformidade do sistema montado é assegurada pelo cumprimento das especificações definidas, comparando os resultados dos testes com os requisitos técnicos do equipamento.

Contexto Profissional

Meios de produção

Os equipamentos de informática incluem elementos de proteção e segurança, como óculos, luvas e dispositivos antiestáticos, bem como ferramentas e equipamentos comuns utilizados na montagem de equipamentos e periféricos. Entre os componentes internos do computador destacam-se processadores, módulos de memória e placas-mãe (motherboards), além de adaptadores de rede, vídeo e comunicações, dispositivos de armazenamento (discos rígidos, SSD) e dispositivos de ligação à rede, como repetidores, switches e routers. Interfaces físicas (portas USB, HDMI), periféricos de entrada (teclados, ratos), saída (monitores, impressoras) e entrada/saída (ecrãs tácteis) complementam o sistema. Ferramentas de teste de hardware e software, fontes de alimentação ininterruptas (UPS) e cablagem

estruturada são essenciais para garantir o funcionamento, a segurança e a eficiência dos sistemas informáticos.

Produtos e resultados

Equipamento informático instalado e operacional. Dispositivos externos devidamente instalados e ligados ao computador. Equipamento informático e os respetivos dispositivos externos verificados e confirmados como funcionais.

Informação utilizada ou gerada

Manuais e guias para a montagem de componentes em equipamentos informáticos, bem como para a ligação de periféricos a esses sistemas. Informações técnicas detalhadas sobre o equipamento, catálogos de produtos de *hardware*, listas de fornecedores e preços. Plano de qualidade organizacional e documentação sobre regulamentos aplicáveis em matéria de saúde, segurança e prevenção de riscos ocupacionais. Registo das operações de montagem, verificação e ligação de periféricos. Normas sobre prevenção de riscos profissionais e normas de proteção ambiental, especialmente as relacionadas com a produção e gestão de resíduos e solos contaminados.

UC2: Realizar operações de manutenção de sistemas informáticos.	
Código: UC382_3	Nível: 3

Elementos de Competência (EC) e Critérios de Desempenho (CD)

EC 1: Aplicar procedimentos de rotina para verificar o funcionamento e a limpeza de equipamentos e dispositivos de informática, utilizando ferramentas específicas, como escovas, sopradores de ar e outros acessórios adequados, de modo a assegurar a sua utilização contínua e eficiente.

CD 1.1. Os dispositivos de impressão são limpos utilizando ferramentas específicas, como escovas, sopradores de ar ou produtos de limpeza adequados, para assegurar o correto desempenho dos equipamentos e prevenir falhas operacionais.

CD 1.2. Os componentes internos do sistema, como ventiladores ou ranhuras de cartões, são limpos utilizando ar comprimido, escovas ou aspiradores, para remover poeiras e evitar sobreaquecimento ou mau funcionamento.

CD 1.3. Os dispositivos externos (rato, teclado, microfone, câmaras, etc.) são limpos com o auxílio de escovas, aspiradores, produtos específicos ou outros equipamentos apropriados, para assegurar a sua higienização e bom estado.

CD 1.4. As temperaturas e o desempenho dos componentes são monitorizados utilizando ferramentas de diagnóstico para prevenir sobreaquecimentos e falhas de hardware.

CD 1.5. A integridade dos discos rígidos e SSD é verificada recorrendo a utilitários de verificação de setores defeituosos e status de saúde, para evitar perda de dados e melhorar a longevidade dos dispositivos de armazenamento.

CD 1.6. Os registos de eventos do sistema operativo são analisados, identificando avisos e erros, para antecipar falhas e otimizar a manutenção preventiva.

EC 2: Resolver incidentes relacionados com *hardware* em equipamentos e dispositivos informáticos, verificando sinais luminosos, códigos de erro e outras indicações, de modo a assegurar o correto funcionamento dos sistemas.

CD 2.1. O funcionamento anormal do equipamento é verificado conferindo as conexões dos cabos, consultando sinais luminosos e códigos de erro na documentação técnica e, se o problema persistir, deve ser reportado a nível superior.

CD 2.2. Os cabos de alimentação e de dados são inspecionados e, se necessário, substituídos, com referência ao tipo de conector e compatibilidade com o dispositivo, para restaurar a funcionalidade do sistema.

CD 2.3. A limpeza física dos componentes internos é realizada, removendo poeira e resíduos, para garantir o correto funcionamento do sistema e evitar superaquecimento.

CD 2.4. Os cabos e conexões internas e externas são verificados e organizados, para assegurar a correta ligação e prevenir falhas de comunicação entre dispositivos.

CD 2.5. As atualizações de firmware da BIOS/UEFI e outros dispositivos são verificadas e aplicadas, conforme necessário, para melhorar a compatibilidade e estabilidade do sistema.

CD 2.6. As tarefas executadas e os incidentes detetados são registados detalhando o estado do dispositivo e as ações realizadas, utilizando suportes físicos ou digitais indicados pela entidade responsável.

EC 3: Executar a receção, embalagem e movimentação de equipamentos e materiais, utilizando ferramentas e máquinas adequadas, para facilitar a armazenagem, garantir a segurança e gerir o inventário.

CD 3.1. Os novos equipamentos informáticos são identificados através do registo no inventário e aplicação de etiquetas de identificação, de acordo com os procedimentos da organização.

CD 3.2. Os equipamentos informáticos, dispositivos e materiais de consumo são movimentados até

ao local designado pela organização, utilizando veículos, máquinas para cargas pesadas, elevadores ou outros meios, cumprindo as normas de segurança e prevenção de riscos profissionais.

CD 3.3. As opções de recuperação do sistema operativo são utilizadas, recorrendo a pontos de restauro, reparação de arranque ou recuperação do sistema, para restaurar o funcionamento do computador em caso de falha crítica.

CD 3.4. A substituição de componentes defeituosos é realizada, assegurando a compatibilidade com o sistema e testando o novo hardware, para confirmar a resolução do problema.

CD 3.5. A remoção de drivers incompatíveis ou obsoletos é efetuada, instalando versões atualizadas, para corrigir erros e melhorar o desempenho do hardware.

CD 3.6. As tarefas realizadas e incidências detetadas durante a embalagem, desembalagem e transferência de equipamentos são registadas em suportes físicos ou digitais indicados, para garantir a documentação adequada.

Contexto Profissional

Meios de produção

Equipamentos de informática. Ferramentas de limpeza para componentes de *hardware*. Dispositivos de armazenamento, como discos rígidos e SSD. Dispositivos de rede, incluindo repetidores, *switches*, *routers* e outros. Interfaces físicas, como portas USB, HDMI e outras. Periféricos de entrada (teclados, ratos), saída (monitores, impressoras) e entrada/saída (ecrãs tácteis). Artigos consumíveis para equipamentos e dispositivos informáticos, como toner e cartuchos de tinta. Cabos de ligação de rede, cabos de energia e cabos de dados. Material de embalagem para equipamentos informáticos e consumíveis, como caixas, plástico bolha e proteções antiestáticas. Ferramentas de etiquetagem para identificação de equipamentos e dispositivos.

Produtos e resultados

Equipamentos e dispositivos informáticos devidamente limpos e conservados. Problemas de *hardware* resolvidos e comunicados ao responsável. Equipamento informático catalogado, embalado, etiquetado e transportado de acordo com as normas estabelecidas.

Informação utilizada ou gerada

Documentação e manuais de utilização e instalação de equipamentos e dispositivos informáticos. Guias do fabricante para a manutenção de dispositivos informáticos. Manuais e guias detalhados para a substituição de consumíveis, como toner e cartuchos. Catálogos de produtos consumíveis. Rótulos de produtos de *hardware* e *software*. Regulamentações ambientais aplicáveis ao tratamento de resíduos. Registo das operações de manutenção realizadas. Notas de entrega de componentes. Normas sobre prevenção de riscos profissionais. Normas de proteção ambiental, especialmente as relacionadas com a produção e gestão de resíduos e solos contaminados.

UC3: Executar operações com ferramentas de escritório e IA.	
Código: UC379_3	Nível: 3

Elementos de Competência (EC) e Critérios de Desempenho (CD)

EC 1: Gerir as ferramentas do ambiente do utilizador no sistema operativo, configurando os parâmetros conforme as necessidades e seguindo instruções para organizar o ambiente de trabalho e otimizar a gestão da informação.

CD 1.1. As mensagens de arranque do sistema operativo e as ligações aos dispositivos conectados são verificadas, comparando com os padrões esperados e corrigindo eventuais falhas, para garantir o carregamento correto do sistema e evitar erros de funcionamento.

CD 1.2. A ferramenta de gestão de ficheiros é utilizada para criar, eliminar e renomear pastas e ficheiros, organizando a informação de forma a facilitar a sua utilização e acesso.

CD 1.3. O ambiente gráfico do sistema operativo é configurado, ajustando elementos, como fundo do ecrã, resolução, barras de ferramentas e ícones, para melhorar a usabilidade e a adaptação às necessidades do utilizador.

CD 1.4. As ferramentas de gestão de dispositivos, como impressoras e digitalizadores, são utilizadas para modificar preferências de impressão, digitalizar documentos e realizar outras tarefas relacionadas com periféricos.

CD 1.5. As atualizações do sistema operativo e das aplicações são verificadas e instaladas, utilizando ferramentas de atualização automática ou manual, para garantir a segurança e o desempenho adequado do sistema.

CD 1.6. As permissões de utilizador e a gestão de contas são configuradas, ajustando privilégios e acessos, para assegurar a proteção dos dados e a correta utilização do sistema.

EC 2: Gerir dispositivos e aplicações multimédia, utilizando os recursos e ferramentas disponíveis, seguindo as instruções recebidas para editar e organizar a informação nelas contida.

CD 2.1. O software multimédia incluído no sistema operativo ou fornecido com o dispositivo é utilizado, explorando funções de ajuste, edição e organização dos conteúdos, para assegurar a correta gestão e manipulação dos ficheiros multimédia.

CD 2.2. O software multimédia incluído no sistema operativo ou fornecido com o dispositivo (visualizadores de fotografias, reprodutores de música, etc.) é utilizado para realizar ajustes, aceder, copiar e apagar a informação contida no dispositivo.

CD 2.3. As informações são editadas e conteúdos simples de vídeo, imagem ou som são criados utilizando aplicações multimédia, seguindo as instruções recebidas para garantir a organização e a qualidade do conteúdo produzido.

CD 2.4. Os formatos de ficheiros multimédia são verificados e convertidos, recorrendo a software específico, para garantir compatibilidade com diferentes dispositivos e aplicações.

CD 2.5. Os conteúdos multimédia são armazenados e organizados em diretórios específicos, seguindo critérios definidos, para facilitar a sua recuperação e assegurar a sua integridade.

CD 2.6. As aplicações de captura e edição de áudio são utilizadas, ajustando volume, cortes e efeitos, para melhorar a qualidade dos ficheiros de som.

EC 3: Criar documentos utilizando um processador de texto e aplicar-lhes formatação (tipos de letra, tabulações, alinhamentos, etc.), de modo a tornar a informação neles contida mais atrativa e de fácil compreensão, seguindo as instruções recebidas.

CD 3.1. As funcionalidades do processador de texto são utilizadas para criar, armazenar, imprimir e visualizar documentos, acedendo ao conteúdo, visualizando, imprimindo ou guardando os ficheiros de acordo com as necessidades de utilização.

CD 3.2. A formatação é aplicada ao texto utilizando opções como negrito, itálico, sublinhado, tamanho e tipo de letra, numeração, marcadores, tabulações e alinhamento de parágrafos, para melhorar a apresentação e a legibilidade do documento.

CD 3.3. Os elementos gráficos como imagens, tabelas e gráficos são inseridos e formatados,

ajustando tamanho, alinhamento e legendas, para melhorar a apresentação visual e tornar o documento mais compreensível.

CD 3.4. A formatação das páginas é definida inserindo cabeçalhos, rodapés, ajustando a orientação, o tamanho das margens e outras configurações de layout, utilizando as ferramentas disponíveis no processador de texto.

CD 3.5. A ortografia e a gramática do documento são verificadas e corrigidas, utilizando as ferramentas de revisão do processador de texto, para garantir clareza e correção linguística.

CD 3.6. As opções de tabelas e listas são aplicadas visando organizar e categorizar dados no documento, utilizando os recursos do processador de texto, para garantir uma apresentação clara e eficaz da informação.

CD 3.7. Os documentos são exportados para diferentes formatos (PDF, DOCX, ODT, etc.), ajustando configurações de compatibilidade, para garantir a correta visualização e partilha da informação.

EC 4: Utilizar aplicações de escritório (bases de dados, apresentações, folhas de cálculo, entre outras), para manipular informação, recorrendo a projetos existentes e seguindo as instruções recebidas.

CD 4.1. As folhas de cálculo já preparadas são abertas e manipuladas executando a aplicação de escritório correspondente, inserindo, visualizando e imprimindo dados, de acordo com as instruções fornecidas.

CD 4.2. As bases de dados já criadas são abertas e manipuladas, inserindo e apresentando dados através de formulários e relatórios predefinidos, para facilitar a extração e análise da informação.

CD 4.3. As fórmulas e funções específicas de cálculo são aplicadas corretamente nas folhas de cálculo para processar e analisar dados, seguindo as instruções fornecidas e garantindo a precisão dos resultados.

CD 4.4. A formatação de células e campos em folhas de cálculo e bases de dados é ajustada, aplicando cores, alinhamento e estilos de apresentação, para melhorar a legibilidade e organização da informação.

CD 4.5. Os macros e automação de tarefas são utilizadas em folhas de cálculo, recorrendo a funções específicas, para otimizar processos repetitivos e aumentar a produtividade.

CD 4.6. As tabelas dinâmicas são criadas e configuradas, selecionando intervalos de dados e aplicando filtros, para facilitar a análise e interpretação da informação.

EC 5: Utilizar a Internet, gerindo browsers e seguindo instruções, para pesquisar e obter informações na rede interna e externa.

CD 5.1. O navegador é utilizado para aceder a páginas web indicadas e navegar pelos links disponíveis, seguindo as instruções recebidas para localizar informações específicas.

CD 5.2. Os motores de pesquisa são utilizados, aplicando critérios avançados e filtros de busca, para otimizar a obtenção de informações relevantes e confiáveis.

CD 5.3. A pesquisa é realizada de forma eficiente e dentro dos prazos estabelecidos, utilizando palavras-chave apropriadas e ajustando os parâmetros de pesquisa, para otimizar os resultados.

CD 5.4. As informações obtidas são analisadas e validadas, comparando fontes e verificando a credibilidade, para assegurar a qualidade e fiabilidade dos dados.

CD 5.5. As informações encontradas são organizadas e apresentadas de forma clara e estruturada, utilizando ferramentas de gestão de documentos ou anotações, para facilitar a consulta futura.

CD 5.6. As ferramentas de segurança online são utilizadas, configurando bloqueadores de anúncios, firewalls e antivírus, para reduzir riscos de ataques cibernéticos e proteger dados pessoais.

EC 6: Gerir aplicações de e-mail e videoconferência para trocar informações e comunicar, seguindo as instruções recebidas.

CD 6.1. As aplicações de correio eletrónico são utilizadas para enviar e receber mensagens, anexar e descarregar ficheiros, e organizar as mensagens em pastas, seguindo as instruções recebidas.

CD 6.2. Os fóruns de notícias e blogues são utilizados para consultar informações, deixar opiniões, colocar e responder a questões sobre temas específicos, de acordo com as necessidades de utilização.

CD 6.3. As plataformas de formação virtual são acedidas para consultar conteúdos fornecidos pelo tutor, enviar informações solicitadas e utilizar recursos como chat para troca de mensagens e informações.

CD 6.4. As ferramentas de videoconferência são utilizadas, configurando áudio, vídeo e partilha de ecrã, para facilitar a comunicação eficiente e a troca de informações em reuniões virtuais.

CD 6.5. As ferramentas de compressão e descompressão são utilizadas para aceder a ficheiros compactados e criar novos ficheiros reduzidos, conforme necessário.

CD 6.6. As configurações de privacidade e segurança são ajustadas, aplicando definições adequadas, para proteger os dados e garantir comunicações seguras.

EC 7: Utilizar ferramentas de Inteligência Artificial (IA), concretamente Chats de IA, para pesquisa, suporte e auxílio na operação de manutenção e resolução de incidentes técnicos.

CD 7.1. Utilizar Chats de IA para pesquisa e obtenção de informações técnicas, formulando perguntas adequadas e analisando as respostas fornecidas.

CD 7.2. Aplicar informações obtidas por meio da IA para auxiliar na resolução de incidentes técnicos, garantindo a veracidade dos dados.

CD 7.3. Utilizar IA como suporte para aprendizado contínuo, explorando novas funcionalidades e tendências tecnológicas.

CD 7.4. Verificar a confiabilidade das respostas geradas por IA, validando-as com fontes oficiais e especialistas técnicos.

CD 7.5. Integrar chats de IA ao fluxo de trabalho, utilizando-os de forma ética e responsável para otimizar a produtividade.

Contexto Profissional

Meios de produção

Equipamentos de informática. Sistemas operativos. Dispositivos de impressão. Rede local. Ligação à Internet. Ferramentas da Internet: browser, correio eletrónico. Software multimédia. Dispositivos multimédia. Ferramentas e aplicações de escritório. Dispositivos de mobilidade, como tablets e smartphones. Ferramentas de compressão de ficheiros. Plataformas de formação virtual. Ferramentas de videoconferência e mensagens instantâneas. Ferramentas de Inteligência Artificial para suporte técnico e pesquisa.

Produtos e resultados

Ambiente de trabalho personalizado e informação organizada. Conteúdos audiovisuais editados. Documentos de texto criados, formatados, armazenados e impressos. Informação manipulada através de uma base de dados, folha de cálculo e aplicação de apresentações. Informação pesquisada na Internet e armazenada no sistema informático. Troca de informação realizada através de ferramentas de correio eletrónico, videoconferência ou plataformas colaborativas. Informações obtidas e verificadas por meio de Inteligência Artificial para suporte técnico e resolução de incidentes

Informação utilizada ou gerada

Manuais para dispositivos multimédia e respetivas aplicações. Manuais de aplicações de escritório. Manuais do utilizador do sistema operativo. Guias do utilizador de ferramentas da Internet. Documentos preparados, verificados ortograficamente e apresentados com formatação aplicada. Normas sobre prevenção de riscos profissionais. Normas de proteção ambiental, especialmente as relacionadas com a produção e gestão de resíduos e solos contaminados.

UC4: Instalar, configurar e conectar equipamentos em redes locais.	
Código: UC175.1_3	Nível: 3

Elementos de Competência (EC) e Critérios de Desempenho (CD)

EC 1: Instalar os meios de interconexão de rede conforme o projeto da organização, cumprindo as normas de prevenção dos riscos laborais.

CD 1.1. Os componentes passivos e ativos, como tomadas, cabos e hubs, são diferenciados e identificados pelas suas características.

CD 1.2. O projeto de instalação das infraestruturas de rede de comunicações é interpretado e os componentes são identificados e localizados.

CD 1.3. As tomadas de rede são instaladas nos locais definidos no projeto, utilizando ferramentas específicas.

CD 1.4. As antenas e componentes sem fio são instalados e alinhados para assegurar a conectividade.

CD 1.5. Os testes da instalação são realizados utilizando instrumentos de medição apropriados, para validar a integridade, a continuidade e o desempenho da infraestrutura de rede, conforme o projeto.

CD 1.6. As conexões de rede são avaliadas, aplicando ferramentas de diagnóstico, para garantir a estabilidade, a velocidade e a conformidade com os padrões técnicos definidos.

CD 1.7. As proteções contra interferências eletromagnéticas são aplicadas, seguindo as normas técnicas e utilizando materiais adequados, para evitar degradação do sinal e assegurar a qualidade da comunicação.

EC 2: Montar os equipamentos de interconexão de redes, garantindo o funcionamento seguro e cumprindo as normas de prevenção de riscos laborais.

CD 2.1. Os requisitos de implementação do dispositivo e das linhas de comunicação são verificados quanto à compatibilidade, conforme a documentação técnica.

CD 2.2. As interfaces e módulos de adaptação das linhas de comunicação são instalados e verificados, para ligação posterior, conforme os requisitos de implementação do dispositivo de comunicação.

CD 2.3. As conexões entre as linhas de comunicação e o dispositivo são estabelecidas, seguindo as especificações técnicas, para assegurar a comunicação eficiente e segura entre redes públicas e privadas.

CD 2.4. O equipamento de interconexão de redes é testado após a instalação, utilizando ferramentas de diagnóstico, para verificar a operação correta e a conformidade com os requisitos técnicos.

CD 2.5. O trabalho de instalação é documentado para satisfazer as necessidades técnicas e administrativas da organização, seguindo os protocolos especificados.

CD 2.6. Os equipamentos ativos de rede são atualizados com firmware e patches mais recentes, conforme as diretrizes do fabricante, para garantir a segurança e a estabilidade da comunicação.

EC 3: Instalar e configurar os protocolos de comunicação de rede para garantir a conectividade necessária, conforme as especificações da organização.

CD 3.1. Os equipamentos ativos de comunicação são configurados e, se necessário, modificados, para permitir a coexistência e/ou interconexão de redes locais virtuais por meio de circuitos alugados.

CD 3.2. A configuração física e lógica dos encaminhadores de ligação com redes externas é realizada, utilizando as ferramentas adequadas e seguindo os procedimentos estabelecidos.

CD 3.3. O software de encriptação é instalado e parametrizado, conforme as diretrizes da organização, para proteger a integridade e a confidencialidade das comunicações de

rede.

CD 3.4. Os parâmetros de segurança dos protocolos de comunicação são configurados e verificados para garantir a proteção da rede contra acessos não autorizados e ataques cibernéticos.

CD 3.5. As VLAN e segmentações de rede são configuradas, conforme as políticas da organização, para otimizar o tráfego, melhorar a segurança e reduzir a propagação de falhas.

CD 3.6. As políticas de acesso à rede são implementadas e verificadas, aplicando listas de controlo de acesso e autenticação, para restringir o acesso não autorizado e reforçar a segurança da infraestrutura.

EC 4: Monitorizar o tráfego da rede e gerir incidências nos equipamentos, conforme os procedimentos definidos.

CD 4.1. Os sistemas de notificação de incidências são instalados e configurados, conforme os procedimentos internos, para fornecer alertas e informações à plataforma de gestão centralizada.

CD 4.2. A origem da incidência é localizada, interpretando os dados do sistema de monitorização e a documentação técnica, para isolar e diagnosticar a causa do problema.

CD 4.3. A incidência detetada é corrigida, utilizando ferramentas adequadas e seguindo os protocolos internos, para restaurar a operação normal dos serviços de rede.

CD 4.4. O processo de resolução da incidência é documentado, registando ações tomadas e notificando os utilizadores afetados, para garantir a rastreabilidade e a melhoria contínua da operação da rede.

CD 4.5. As métricas de desempenho da rede são analisadas regularmente, utilizando ferramentas de monitorização, para otimizar a eficiência do tráfego e garantir a estabilidade dos equipamentos, conforme os requisitos operacionais

CD 4.6. As cópias de segurança das configurações dos equipamentos de rede são realizadas e armazenadas periodicamente, para garantir a rápida recuperação em caso de falhas ou ataques, conforme as políticas da organização.

CD 4.7. A capacidade e utilização da rede são analisadas regularmente, identificando possíveis gargalos, para planear futuras expansões e otimizar o desempenho da infraestrutura.

Contexto Profissional

Meios de produção

Equipamentos informáticos e periféricos. Ferramentas de inventário. Ferramentas informáticas de escritório. Elementos de proteção individual (EPI). Elementos de proteção de equipamentos. Ferramentas e utensílios para a manutenção elétrica e eletrónica. Ferramenta específica de medida e diagnóstico para montagem. Elementos de interconexão de redes.

Produtos e resultados

Equipamentos de rede instalados ou reparados. Conectividade estabelecida. Relatórios sobre incidências no processo de instalação ou entrada em exploração. Infraestrutura de rede em exploração configurada fisicamente. Incidências na rede resolvidas e geridas.

Informação utilizada ou gerada

Normas e padronização do equipamento (ISO, EIA, IEEE). Normas internas da organização. Normas de prevenção dos riscos laborais. Norma para a proteção contra descargas eletrostáticas. Regras sobre garantias. Documentação para calibração de equipamentos de medição. Provas e controlo de testes. Manuais de instalação e informações técnicas do equipamento e/ou componentes. Recomendações de montagem dos fabricantes. Suporte técnico do fabricante. Documentação para instalação e arranque de equipamentos de interconexão de redes. Documentação técnica e de prestação dos equipamentos. Partes de incidentes e históricos de incidentes da montagem. Relatórios de incidência de montagem. Dicionário técnico.

UC4: Manter a segurança de um sistema informático	
Código: UC176.1_3	Nível: 3

Elementos de Competência (EC) e Critérios de Desempenho (CD)

EC 1: Gerir e manter atualizados os inventários de software e componentes lógicos do sistema informático

CD 1.1. Os inventários de software e demais componentes lógicos do sistema são automaticamente gerados e atualizados com o apoio de ferramentas de gestão de ativos, assegurando a sua conformidade com os procedimentos e periodicidades definidos pela organização.

CD 1.2. Alterações detetadas em versões, configurações ou estados dos componentes lógicos são imediatamente registadas e documentadas para garantir a integridade do inventário.

CD 1.3. As licenças de software são geridas através de sistemas de Software Asset Management (SAM), assegurando o controlo dos direitos de propriedade intelectual e conformidade com a legislação em vigor.

CD 1.4. Incidentes relacionados com mau funcionamento, alterações de configuração não autorizadas, instalação de software não autorizado ou uso indevido são registados automaticamente e comunicados ao responsável hierárquico, de acordo com os procedimentos**.** definidos.

CD 1.5. Dashboards de monitorização e alertas automáticos são utilizados para facilitar a supervisão contínua e proativa do inventário lógico.

EC 2: Auditar e gerir os acessos ao sistema informático, assegurando a conformidade com o plano de segurança

CD 2.1. Ferramentas de monitorização e análise de logs, incluindo soluções SIEM, são utilizadas para garantir a eficácia da supervisão dos acessos e das atividades no sistema.

CD 2.2. Os logs de conexões e atividades dos utilizadores são analisados regularmente para identificar comportamentos anómalos ou acessos não autorizados.

CD 2.3. Alterações na configuração de controlo de acessos são documentadas de forma estruturada e integradas com sistemas de alerta em tempo real.

CD 2.4. Auditorias periódicas são realizadas aos perfis de utilizadores para garantir que apenas os acessos necessários estão ativos, seguindo o princípio do menor privilégio.

CD 2.5. O uso de mecanismos como a autenticação multifator (MFA) é verificado em todos os sistemas críticos.

CD 2.6. As tarefas realizadas e os incidentes detetados são documentados conforme os procedimentos internos, sendo comunicados aos responsáveis sempre que necessário.

EC 3: Monitorizar e validar os mecanismos de segurança do sistema informático

CD 3.1. As permissões de acesso dos utilizadores são validadas regularmente, assegurando que estão em conformidade com o plano de segurança e o perfil de risco.

CD 3.2. A aplicação das políticas de segurança, nomeadamente aquelas associadas ao utilizador, é verificada com ferramentas automatizadas para garantir a sua eficácia e atualidade.

CD 3.3. Os sistemas de proteção antivírus e anti-malware são avaliados continuamente quanto à sua configuração, atualização e resposta a ameaças.

CD 3.4. As configurações de firewall, tanto a nível de desktop como de rede, são revistas regularmente e comparadas com os parâmetros definidos no plano de segurança.

CD 3.5. São realizados testes periódicos de segurança (ex: pentests, simulações de ataques) para comprovar a resiliência do sistema.

CD 3.6. As ações realizadas, resultados das verificações e incidentes são sistematicamente

documentados e comunicados aos responsáveis designados.

EC 4: Implementar e verificar políticas de cópias de segurança para garantir a integridade e recuperação dos dados

CD 4.1. As cópias de segurança são realizadas automaticamente de acordo com a periodicidade, condições e procedimentos definidos no plano de segurança, com notificações em caso de falha.

CD 4.2. A integridade das cópias de segurança é verificada através de testes regulares de restauração, garantindo que os dados podem ser efetivamente recuperados.

CD 4.3. O armazenamento dos backups cumpre os requisitos de segurança física e lógica descritos no plano de segurança e segue as recomendações dos fabricantes dos suportes.

CD 4.4. As cópias de segurança são armazenadas, sempre que possível, em local distinto ou na nuvem, como parte de uma estratégia de continuidade de negócio e recuperação de desastres.

CD 4.5. As operações realizadas e os incidentes detetados são registados nos sistemas de gestão documental, sendo os responsáveis informados quando necessário.

Contexto profissional:

Meios de produção

Equipamentos informáticos e periféricos; Software de aplicações informáticas; Software antivírus; Atualizações e correções de software de sistema e aplicações; Drivers de dispositivos; Ferramentas software de segurança; Monitores de rendimento; Ferramentas de inventariado; Ferramentas informáticas de oficina; Ferramentas de gestão e realização de cópias de segurança.

Produtos e resultados

Sistema operacional e aplicações configurados e parametrizados conforme as necessidades da organização; Inventários de software e de configuração das aplicações do sistema atualizado; Cópias de segurança corretamente etiquetadas e armazenadas; Documentação de instalação, configuração e informação de incidências do software do sistema atualizado; Documentação de instalação, configuração e informação de incidências do software de aplicação atualizada; Sistema informático assegurado mediante acessos e atividades não autorizadas.

Informação utilizada ou gerada

Normas de procedimento da organização; Normas e recomendações ambientais de segurança; Plano de segurança informática da organização; Assistência técnica online; Informação de instalação e configuração de sistema e aplicações; Documentação de ferramentas de backup; Legislação sobre proteção de dados e propriedade intelectual; Relatórios de incidências de acessos ao sistema; Relatórios de incidências nos mecanismos de segurança do sistema; Relatórios de incidências nas cópias de segurança; Dicionário técnico; Planos de contingência.

PROGRAMA FORMATIVO ASSOCIADO AO PERFIL PROFISSIONAL

TIC003.A1_3

MONTAGEM E MANUTENÇÃO DE SISTEMAS INFORMÁTICOS

PROGRAMA FORMATIVO DA QUALIFICAÇÃO PROFISSIONAL			
Código: TIC003.A1_3	Denominação	Montagem e Manutenção de Sistemas Informáticos	
Nível: 3	Família Profissional	Tecnologias de Informação e Comunicação (TIC)	
Duração indicativa	950 Horas		

Unidades de Competência	N.º	Denominação	Código
	1	Realizar operações de montagem de sistemas informáticos.	UC381_3
	2	Realizar operações de manutenção de sistemas informáticos.	UC382_3
	3	Executar operações com ferramentas de escritório e IA	UC379_3
	4	Instalar, configurar e conectar equipamentos em redes locais.	UC175.1_3
	5	Manter a segurança de um sistema informático.	UC176.1_3

UNIDADES FORMATIVAS (UF) Básicas desta Qualificação Profissional				
Denominação			Duração	Código
Inglês Técnico			60 horas	UF468
MÓDULOS FORMATIVOS			UNIDADES FORMATIVAS	
N.º	Denominação	Código	Denominação	Código
1	Montagem e Configuração de Sistemas Informáticos (120 h)	MF381_3	Arquitetura de Computadores (60 horas)	UF492
			Montagem e Manutenção de Sistemas Informáticos (60 horas)	UF493
2	Operações de Manutenção de Sistemas Informáticos (60 horas)	MF382_3	-	-
3	Gestão de Informação e Documentação com Aplicações de Office e IA (150 horas)	MF379_3	Manipulação de Informação com Ferramentas Office e IA (90 horas)	UF488
			Produção e Edição de Conteúdos Multimédia (60 horas)	UF489
4	Instalação de Redes de Área Local. (120h)	MF175.1_3	Princípios das Redes de Área Local (70 horas).	UF257.1
			Equipamentos de Interconexão (50 horas).	UF260.1
5	Manutenção da segurança no	MF176.1_3	Procedimentos de segurança no sistema informático (80 horas).	UF261.1

	sistema informático. (80 h)			
MT_TIC003.A1		Módulo Formativo em Contexto Real de Trabalho (360 horas)		

UNIDADES FORMATIVAS TRANSVERSAIS

Unidade formativa : Inglês Técnico UF468

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Compreender mensagens orais e escritas no contexto profissional.

- **CA 1.1.** Interpretar mensagens orais e escritas gerais e específicas com correção, utilizando técnicas de dedução pelo contexto e identificação da ideia principal.
- **CA 1.2.** Reconhecer a terminologia e expressões específicas do sector em discursos, documentos e mensagens diversas.
- **CA 1.3.** Localizar informação relevante em textos técnicos aplicando estratégias de leitura rápida e leitura orientada.
- **CA 1.4.** Responder a questões orais e escritas com base em documentos técnicos e mensagens profissionais, demonstrando compreensão da informação essencial.
- **CA 1.5.** Relacionar vocabulário técnico com situações práticas do contexto profissional, através de exercícios de correspondência, preenchimento de lacunas ou produção de frases contextualizadas.

RA2: Produzir mensagens orais e escritas adequadas a diferentes contextos profissionais.

- **CA 2.1.** Produzir mensagens orais e escritas com estrutura clara, coerência e terminologia específica, ajustadas ao registo e interlocutor.
- **CA 2.2.** Elaborar documentos profissionais aplicando normas de cortesia e formalidade adequadas ao contexto.
- **CA 2.3.** Transmitir instruções e informações profissionais utilizando recursos linguísticos habituais e palavras-chave relevantes.
- **CA 2.4.** Participar em situações profissionais (ex: reuniões, conferência e apresentações etc.), utilizando expressões funcionais adequadas e linguagem específica do setor.
- **CA 2.5.** Redigir e-mails, memorandos ou relatórios simples em inglês técnico, respeitando convenções de formatação e utilizando vocabulário apropriado ao objetivo e ao destinatário.

RA3: Identificar normas de protocolo e regras de comunicação formal e informal em contexto profissional.

- **CA 3.1.** Identificar regras de comunicação formal e informal em diferentes contextos e suportes de comunicação.
- **CA 3.2.** Descrever procedimentos de protocolo e etiqueta profissional em eventos, reuniões e comunicações empresariais.
- **CA 3.3.** Distinguir características de discursos formais e informais com exemplos adequados ao meio profissional.
- **CA 3.4.** Demonstrar a aplicação prática de normas de etiqueta em ambientes profissionais, como ao participar em reuniões, eventos e videoconferências, respeitando o protocolo de comunicação e comportamento esperado.

RA4: Aplicar estratégias de comunicação eficaz na gestão de reclamações e resolução de conflitos.

CA 4.1. Aplicar técnicas de comunicação assertiva na gestão de situações de conflito e reclamação em contexto profissional.

CA 4.2. Utilizar vocabulário adequado e tom de voz apropriado em situações de tensão, respeitando o protocolo empresarial.

CA 4.3. Redigir respostas a reclamações seguindo normas de cortesia e estruturas formais específicas.

CA 4.4. Analisar situações comunicativas profissionais, identificando comportamentos adequados e inadequados segundo normas de etiqueta e protocolo.

CA 4.5. Demonstrar a utilização de técnicas de escuta ativa e feedback construtivo para compreender e resolver reclamações de forma eficaz, mantendo a calma e o profissionalismo.

CA 4.6. Redigir e-mails ou cartas de resposta a reclamações, utilizando uma abordagem clara, cortês e focada na resolução do problema, de acordo com as normas de comunicação formal e protocolos empresariais.

RA5: Demonstrar uma atitude proativa e adequada na comunicação em ambiente profissional.

CA 5.1. Adotar normas de relação e protocolo respeitando a formalidade e a cortesia em interações presenciais, telefónicas e escritas.

CA 5.2. Solicitar esclarecimentos e confirmar mensagens de forma educada e assertiva, promovendo a compreensão mútua.

CA 5.3. Responder a reclamações e queixas com atitude profissional e respeitosa, mantendo a fluidez e o respeito na comunicação.

CA 5.4. Manter uma postura ativa e positiva durante as interações profissionais, demonstrando interesse e comprometimento nas respostas e na solução de problemas.

CA 5.5. Utilizar expressões e gestos apropriados para garantir uma comunicação respeitosa e profissional, seja em ambientes presenciais, por telefone ou por escrito.

Conteúdos

1. Compreensão Oral e Escrita em Contexto Profissional

1.1. Técnicas de compreensão de mensagens orais e escritas:

1.1.1. Dedução pelo contexto e identificação da ideia principal e secundária.

1.1.2. Localização rápida de informações específicas (scanning e skimming).

1.2. Terminologia e expressões técnicas do sector:

1.2.1. Vocabulário habitual em ambiente profissional.

1.2.2. Palavras-chave e expressões mais utilizadas em discursos, documentos e mensagens.

1.3. Tipos de mensagens e discursos profissionais:

1.3.1. Mensagens diretas, telefónicas, gravadas, radiofónicas e televisivas.

1.3.2. Instruções sobre operações e tarefas do posto de trabalho.

1.3.3. Solicitação de informações gerais e específicas.

2. Produção Oral e Escrita em Ambiente Profissional

2.1. Estruturação e clareza na produção de mensagens:

2.1.1. Estratégias para manter a fluidez na conversação (exemplos e perguntas de confirmação).

2.1.2. Estratégias de clarificação do discurso.

2.2. Elaboração de mensagens profissionais:

2.2.1. Redação de instruções de trabalho e comunicações internas.

2.2.2. Comunicação de mau funcionamento de equipamentos ou aplicações.

2.2.3. Produção de mensagens telefónicas, presenciais ou gravadas, com registo e terminologia apropriados.

2.3. Resposta a reclamações e resolução de problemas:

2.3.1. Utilização de expressões adequadas para gerir queixas.

2.3.2. Estruturas formais e corteses para comunicação de resposta.

3. Normas de Protocolo e Comunicação Formal e Informal

3.1. Normas de comunicação profissional: Normas de cortesia e formalidade em diferentes contextos e suportes (presencial, telefónico, escrito).

3.2. Protocolo em ambiente profissional:

3.2.1. Normas de saudação, recepção e despedida.

3.2.2. Procedimentos de etiqueta em reuniões, eventos e comunicações empresariais.

3.3. Características dos discursos formais e informais: Exemplos práticos aplicados ao contexto profissional.

4. Gestão de Reclamações e Resolução de Conflitos

4.1. Comunicação assertiva em situações de conflito: Técnicas de gestão de reclamações com foco na assertividade.

4.2. Adaptação do tom de voz e vocabulário: Aplicação de vocabulário adequado e utilização do tom apropriado em situações de tensão.

4.3. Redação de respostas a reclamações: Estrutura formal, normas de cortesia e resolução clara.

5. Atitudes e Comportamentos na Comunicação Profissional

5.1. Normas de relação interpessoal e protocolo empresarial: Comportamento adequado em interações presenciais, telefónicas e escritas.

5.2. Técnicas para promover a compreensão mútua: Solicitação de esclarecimentos e confirmação de mensagens de forma educada e assertiva.

5.3. Gestão respeitosa de reclamações: Resposta a queixas com atitude profissional, respeitosa e fluída.

MÓDULOS FORMATIVOS (MF)

MF1: Montagem e Configuração de Sistemas Informáticos		
Código: MF381_3	Nível: 3	Duração Mínima: 120 Horas
Associado à UC381_3: Realizar operações de montagem de sistemas informáticos		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
■ Unidade Formativa 1:	Arquitetura de Computadores	UF492
■ Unidade Formativa 2:	Montagem e Manutenção de Sistemas Informáticos	UF493

Unidade Formativa 1: Arquitetura de Computadores (UF492)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar os princípios fundamentais da arquitetura de computadores, identificando os seus componentes e funcionamento interno.

CA 1.1. Explicar a estrutura básica de um computador, identificando os seus principais componentes (CPU, memória, barramentos, dispositivos de entrada e saída, entre outros).

CA 1.2. Identificar os diferentes tipos de arquiteturas de computadores (Von Neumann, Harvard, RISC, CISC), descrevendo suas características e aplicações.

CA 1.3. Explicar o funcionamento da Unidade Central de Processamento (CPU), detalhando o ciclo de instrução (busca, decodificação, execução e escrita).

CA 1.4. Relacionar os conceitos de barramento de dados, barramento de endereços e barramento de controle com o funcionamento da comunicação interna no computador.

RA2: Analisar os diferentes tipos de memória de um computador e sua hierarquia no sistema.

CA 2.1. Identificar e diferenciar os principais tipos de memória (RAM, ROM, cache, registradores, memória virtual, entre outros), explicando suas funções e características.

CA 2.2. Explicar o conceito de hierarquia de memória e sua importância para o desempenho do sistema computacional.

CA 2.3. Analisar o funcionamento da memória cache e sua relação com a CPU, detalhando os níveis L1, L2 e L3.

CA 2.4. Interpretar tabelas e especificações técnicas de módulos de memória (DDR, LPDDR, GDDR, entre outros), comparando suas velocidades e capacidades.

RA3: Analisar e interpretar as especificações técnicas dos componentes de hardware, avaliando a sua compatibilidade e desempenho.

CA 3.1. Comparar as especificações técnicas de diferentes componentes de hardware, identificando as suas características e limitações, com base em documentação técnica.

CA 3.2. Avaliar a compatibilidade entre processador, memória RAM, armazenamento e placa-mãe, garantindo a integridade e o funcionamento correto do sistema.

CA 3.3. Interpretar benchmarks e testes de desempenho de hardware, utilizando ferramentas especializadas para analisar a eficiência dos componentes.

CA 3.4. Justificar a escolha de componentes de hardware para diferentes cenários de utilização, considerando critérios como desempenho, eficiência energética e custo-benefício.

CA 3.5. Analisar as especificações técnicas dos componentes de hardware, identificando a sua compatibilidade e desempenho com base em manuais técnicos e ferramentas de benchmarking.

CA 3.6. Interpretar relatórios de testes de desempenho de hardware, comparando os resultados com padrões de referência para justificar a adequação dos componentes ao sistema.

RA4: Adotar boas práticas de organização, segurança e descarte de resíduos eletrônicos, garantindo a sustentabilidade e a conformidade com normas ambientais.

CA 4.1. Organizar os componentes de hardware, ferramentas e materiais de trabalho, mantendo o ambiente limpo e seguro, conforme as boas práticas de manuseio e normas internas.

CA 4.2. Utilizar equipamentos de proteção individual (EPIs) e aplicar procedimentos de segurança, evitando riscos elétricos e danos aos componentes, de acordo com as normas de segurança do trabalho.

CA 4.3. Separar e descartar corretamente resíduos eletrônicos e materiais recicláveis, seguindo as diretrizes ambientais e locais designados pela organização, para minimizar impactos ambientais.

CA 4.4. Demonstrar responsabilidade e comprometimento com a sustentabilidade, promovendo a utilização consciente de materiais e recursos, alinhado às práticas recomendadas na área de TI.

CA 4.5. Incentivar colegas e demais profissionais a adotarem práticas sustentáveis, compartilhando orientações sobre organização, segurança e descarte adequado de resíduos eletrônicos, promovendo um ambiente de trabalho mais responsável e ecologicamente correto.

Conteúdos

1. **Introdução à arquitetura de computadores**
   - **1.1.** Conceitos fundamentais.
   - **1.2.** Componentes essenciais de um computador.
   - **1.3.** Tipos de computadores e aplicações.
   - **1.4.** Tendências em arquitetura de computadores.
2. **Arquitetura e componentes internos de um sistema de computador**
   - **2.1.** Unidade Central de Processamento (CPU).
   - **2.2.** Carcaças e fontes de alimentação.
   - **2.3.** Placa-mãe (Motherboard).
   - **2.4.** Memórias RAM e armazenamento.
   - **2.5.** Placas de expansão e conectores internos.
3. **Conectividade e interação entre dispositivos internos e externos**
   - **3.1.** Conectores e barramentos externos.
   - **3.2.** Dispositivos externos de entrada e saída.
   - **3.3.** Dispositivos de armazenamento e transferência de dados.
   - **3.4.** Infraestrutura de rede e conectividade.
   - **3.5.** Técnicas de diagnóstico e troubleshooting de conectividade.
4. **Tópicos avançados e tendências em arquitetura de computadores**
   - **4.1.** Processadores e arquiteturas modernas.
   - **4.2.** Avanços em armazenamento e memória
   - **4.3.** Computação paralela e GPUs.
   - **4.4.** Segurança e proteção de hardware.

4.5. Métodos de monitorização e diagnóstico de hardware.

Outras Capacidades Associadas à Unidade Formativa

- Analisar o impacto da arquitetura do processador no desempenho computacional.
- Compreender os conceitos de barramentos e sua influência na comunicação entre componentes internos do computador.
- Explicar a evolução das arquiteturas computacionais e suas aplicações específicas.
- Interpretar especificações técnicas de hardware e realizar benchmarks para avaliar o desempenho de sistemas computacionais.

Unidade Formativa 2: Montagem e Manutenção de Sistemas Informáticos (UF493)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar procedimentos para montar, substituir e/ou ligar dispositivos internos de um sistema de computador para expandir ou manter a funcionalidade do sistema, seguindo guias detalhados.

CA 1.1. Interpretar os guias técnicos de instalação e ligação de componentes de hardware de um sistema de computador, identificando fisicamente as ferramentas de montagem, conectores, cabos, portas, entre outros.

CA 1.2. Identificar os blocos funcionais de um sistema de computador pela sua localização em motherboards de diferentes fabricantes, tendo em conta as características específicas do equipamento.

CA 1.3. Os dispositivos de impressão e os componentes internos do sistema, como ventoinhas e ranhuras de cartões, são limpos com ferramentas específicas, como escovas, sopradores de ar, ar comprimido, aspiradores ou produtos de limpeza adequados, garantindo o correto funcionamento, prevenindo falhas operacionais e evitando sobreaquecimento.

CA 1.4. Identificar os componentes de hardware de um sistema de computador, distinguindo as suas características, funcionalidades e elementos que o compõem.

CA 1.5. Reconhecer os tipos de portas, compartimentos internos, tomadas e cabos de ligação (dados e/ou alimentação) existentes num sistema de computador, descrevendo as suas características e função.

CA 1.6. Refira as ferramentas para montar, substituir ou ligar componentes de hardware de um sistema de computador, indicando a sua funcionalidade, utilização e medidas de segurança para as manusear.

CA 1.7. Num caso prático, de montagem de componentes de "hardware" num sistema de computador, de acordo com as instruções recebidas.

- Selecionar as ferramentas de montagem (alicates, chaves de fendas, entre outros) e os elementos de segurança pessoal (pulseira antiestática, luvas, entre outros), específicos para a montagem dos componentes de “hardware” a instalar.
- Selecionar os componentes de hardware a instalar, verificando se as suas características estão de acordo com as indicadas.
- Montar os componentes de hardware (memória, processador, placa gráfica, bateria, entre outros) na motherboard do sistema computador, ligando os que necessitam de cabos de ligação para a sua integração no sistema computador seguindo as instruções recebidas e utilizando as ferramentas indicadas na documentação técnica fornecida pelo fabricante.
- Recolher as ferramentas (chaves de fendas, alicates, etc.) e os resíduos para eliminação ou reciclagem após a conclusão do trabalho de acordo com o guia de trabalho.
- Documentar as operações realizadas utilizando os formatos estabelecidos pela organização (templates, ferramentas de software, entre outros).

RA2. Compreender a arquitetura de um sistema informático, identificando os principais componentes de hardware e as interações entre eles para garantir a funcionalidade do sistema.

CA 2.1. Explicar os principais componentes de um computador, incluindo CPU, memória, placa-mãe, unidades de armazenamento, e dispositivos periféricos, de acordo com especificações técnicas e diagramas do fabricante.

CA 2.2. Descrever as interações entre os componentes de hardware de um sistema informático, identificando a função de cada um dentro da arquitetura do sistema.

CA 2.3. Identificar as funções de cada componente de hardware num sistema informático, explicando como contribuem para o desempenho global do sistema, com base nas especificações técnicas fornecidas pelo fabricante.

CA 2.4. Comparar diferentes tipos de processadores (ex. Intel vs. AMD) e suas características, como arquitetura, desempenho e compatibilidade, de acordo com as necessidades do sistema e especificações técnicas.

CA 2.5. Explicar o papel e a importância dos dispositivos de entrada e saída (ex. teclado, monitor, impressora) dentro da arquitetura de um sistema, identificando como eles se comunicam com os componentes principais para garantir a operação do sistema.

CA 2.6. Identificar as portas externas de um computador para ligar dispositivos de computação externos, utilizando esboços e diagramas gráficos.

RA3: Aplicar procedimentos de monitorização de sistemas de computadores, utilizando ferramentas de diagnóstico de *software* e *hardware* para verificar a montagem, substituição e ligação de dispositivos informáticos externos ao sistema e seus componentes internos, seguindo especificações fornecidas.

CA 3.1. Classificar o software de diagnóstico e as ferramentas de hardware e os procedimentos de monitorização com base no componente de hardware (memória, processador, etc.) ou dispositivo de computador externo (impressora, webcam, etc.) a ser instalado, substituído ou ligado, seguindo as especificações fornecidas.

CA 3.2. Descrever as operações de carregamento do sistema operativo e as possíveis falhas que podem ocorrer durante a fase de arranque do computador, tendo em conta as especificações técnicas do equipamento.

CA 3.3. Aplicar ferramentas de diagnóstico de software e hardware para verificar a montagem e a substituição de componentes de hardware internos, como memória, disco rígido e processador, garantindo que o sistema reconheça corretamente os novos componentes, conforme as especificações do fabricante.

CA 3.4. Realizar testes de funcionamento de dispositivos externos conectados ao computador, como impressoras, teclados e monitores, utilizando ferramentas de diagnóstico apropriadas, assegurando que a comunicação entre o sistema e os dispositivos externos esteja em conformidade com as especificações fornecidas.

CA 3.5. Registar os resultados obtidos durante os testes de diagnóstico, incluindo qualquer falha detetada nos componentes ou dispositivos conectados, e relatar as ações corretivas realizadas, de acordo com os procedimentos internos estabelecidos pela organização.

RA4: Adotar boas práticas de segurança e sustentabilidade durante a montagem e manutenção de sistemas informáticos, respeitando as normas ambientais e de segurança do trabalho.

CA 4.1. Utilizar ferramentas e equipamentos de proteção adequados, como pulseiras antiestáticas e luvas, durante a montagem e manutenção, seguindo as normas de segurança estabelecidas pela organização.

CA 4.2. Gerir corretamente os resíduos de componentes substituídos, separando-os para reciclagem ou descarte adequado, conforme as políticas ambientais e de gestão de resíduos da organização.

CA 4.3. Garantir a manutenção de um ambiente de trabalho organizado e seguro, seguindo as normas de ergonomia e segurança no manuseio de ferramentas e componentes.

CA 4.4. Seguir procedimentos de segurança para evitar danos aos componentes eletrônicos e ao ambiente, utilizando superfícies antiestéticas e evitando a exposição a descargas eletrostáticas durante a montagem e manutenção de sistemas informáticos.

CA 4.5. Assegurar que todos os equipamentos e ferramentas estejam devidamente armazenados após a utilização, mantendo a área de trabalho limpa e sem obstruções, de acordo com as diretrizes de segurança e organização da empresa.

CA 4.6. Cumprir com as regulamentações de saúde e segurança durante a execução das atividades, como a ventilação adequada da área de trabalho e a utilização de equipamentos de proteção individual (EPIs), para garantir a segurança própria e de outros colaboradores no ambiente de trabalho.

RA5: Resolver incidentes relacionados com hardware em equipamentos e dispositivos informáticos, verificando sinais luminosos, códigos de erro e outras indicações, de modo a garantir o correto funcionamento dos sistemas.

CD 5.1. O funcionamento anómalo do equipamento é investigado através da verificação das conexões dos cabos, análise de sinais luminosos e consulta de códigos de erro na documentação técnica. Caso o problema persista, deve ser reportado ao nível superior.

CD 5.2. Os cabos de alimentação e de dados são inspecionados e, se necessário, substituídos, considerando o tipo de conector e a compatibilidade com o dispositivo para restaurar a funcionalidade do sistema.

CD 5.3. A limpeza física dos componentes internos é realizada, removendo poeiras e resíduos, para assegurar o funcionamento adequado do sistema e evitar superaquecimento.

CD 5.4. Os cabos e conexões internas e externas são verificados e organizados, garantindo ligações corretas e prevenindo falhas de comunicação entre dispositivos.

CD 5.5. As atualizações de firmware da BIOS/UEFI e de outros dispositivos são verificadas e aplicadas conforme necessário, melhorando a compatibilidade e estabilidade do sistema.

CD 5.6. As tarefas executadas e os incidentes detetados são registados detalhadamente, documentando o estado do dispositivo e as ações realizadas, utilizando suportes físicos ou digitais definidos pela entidade responsável.

Conteúdos

1. **Montagem e substituição de componentes de hardware**
   - **1.1.** Fundamentos da montagem de computadores.
   - **1.2.** Componentes de hardware interno.
   - **1.3.** Montagem física do computador.
   - **1.4.** Dispositivos externos e periféricos.
   - **1.5.** Normas de segurança elétrica e ESD (Electrostatic Discharge)
2. **Manutenção, testes e segurança**
   - **2.1.** Diagnóstico e testes de hardware.
   - **2.2.** Segurança na montagem e manutenção.
   - **2.3.** Normas ambientais e sustentabilidade.
   - **2.4.** Procedimentos preventivos e de manutenção.
   - **2.5.** Segurança na manutenção e diagnóstico de hardware.
3. **Solução de problemas e manutenção preventiva**
   - **3.1.** Identificação e resolução de problemas comuns.
   - **3.2.** Técnicas de manutenção preventiva.
   - **3.3.** Documentação e registo de intervenções técnicas.
4. **Configuração e otimização de sistemas informáticos**
   - **4.1.** Instalação e configuração do sistema operacional.
   - **4.2.** Personalização e otimização de sistema.
   - **4.3.** Configuração e otimização de hardware.
   - **4.4.** Soluções de backup e recuperação de dados.
   - **4.5.** Monitorização de desempenho e ferramentas de diagnóstico.

Outras Capacidades Associadas à Unidade Formativa

- Capacidade de diagnóstico e resolução de problemas técnicos.
- Capacidade de gestão de inventário e peças de reposição.
- Capacidade de adaptação a novas tecnologias e ferramentas.

Requisitos Básicos do Contexto Formativo do Módulo

Espaços:

Os espaços onde deve decorrer o contexto formativo devem preencher os requisitos básicos estipulados pelo Sistema de Acreditação das Entidades Formadoras. (cf. Decreto-Lei nº6/2013, de 11 de fevereiro; Boletim Oficial nº9; I Série).

Professor(a) / Formador(a):

- O(A) professor(a) ou formador(a) deve possuir um Certificado de Aptidão Profissional que prove que o mesmo é detentor de formação pedagógica na abordagem por competências, segundo a lei.
- O(A) professor(a) ou formador(a) deve ter a formação técnica relacionada com os conteúdos do Módulo Formativo.
- O(A) professor(a) ou formador(a) deve ter experiência profissional, mínima de 3 anos, comprovada nas competências incluídas na Unidade de Competência associada ao Módulo Formativo.

Requisitos de Acesso ao Módulo Formativo

As condições de acesso ao módulo formativo constam no BO nº 20, I Série, Portaria Conjunta nº 09/2020 de 20 de fevereiro - Estrutura e Organização do Catálogo Nacional de Qualificações e Portaria Conjunta nº 10/2020 de 20 de fevereiro - Quadro Nacional de Qualificações.

MF2: Operações de Manutenção de Sistemas Informáticos		
Código MF382_3	Nível: 3	Duração: 60 Horas
Associado à UC382_3: Executar tarefas de apoio na manutenção de sistemas informáticos.		

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar técnicas de limpeza em equipamentos e dispositivos informáticos, verificando o seu funcionamento.

CA 1.1. Descrever as técnicas de limpeza de equipamentos e dispositivos de informática, detalhando as ações a realizar e as ferramentas a utilizar.

CA 1.2. Aplicar técnicas de limpeza de dispositivos de impressão, utilizando ferramentas específicas como escovas, sopradores, produtos específicos para dispositivos, entre outros, para assegurar o seu bom funcionamento.

CA 1.3. Aplicar técnicas de limpeza em dispositivos externos do sistema informático como rato, teclado, microfone, câmaras, entre outros, utilizando escovas, aspiradores, dispositivos e produtos específicos, garantindo a sua higienização e funcionalidade.

CA 1.4. Aplicar técnicas de limpeza em ventoinhas e outros componentes internos do sistema informático, utilizando ar comprimido nas ranhuras dos cartões e ferramentas como escovas e aspiradores, para evitar sobreaquecimento e garantir o bom funcionamento do sistema.

CA 1.5. Aplicar técnicas de verificação do estado e funcionamento dos dispositivos do sistema computador, detetando possíveis anomalias no seu funcionamento, para garantir a operação adequada dos equipamentos.

CA 1.6. Descrever os procedimentos para a gestão (separação, armazenamento, etc.) de resíduos e artigos descartáveis provenientes da limpeza de equipamentos e dispositivos de computador, para cumprir com as normas de produção e gestão de resíduos.

Executar a limpeza de um computador e dos seus dispositivos ligados, utilizando ferramentas específicas (aspiradores, escovas, entre outros), seguindo as condições:

CA 1.7. Identificar os componentes de hardware do equipamento informático e os seus dispositivos ligados a limpar, descrevendo os procedimentos de limpeza e as ferramentas a utilizar.

- Limpar os componentes de hardware e os dispositivos ligados, utilizando ferramentas adequadas.
- Seguir as recomendações de segurança indicadas no manual do fabricante para o manuseamento de componentes eletrónicos durante o processo de limpeza, utilizando luvas, pulseira antiestática, entre outros, para garantir a segurança.
- Gerir a recolha, separação e armazenamento de resíduos e descartáveis provenientes do processo de limpeza para posterior intervenção, cumprindo as normas de gestão de resíduos.
- Verificar o estado dos equipamentos ou dispositivos informáticos limpos, para garantir que mantêm a sua funcionalidade.
- Registar as operações realizadas utilizando os modelos ou formulários indicados, para garantir a documentação adequada.

RA2: Executar a manutenção preventiva e corretiva em sistemas informáticos, identificando falhas e implementando soluções adequadas.

CA 2.1. Identificar os procedimentos técnicos de manutenção preventiva e corretiva, detalhando cada etapa e sua importância para o bom funcionamento dos dispositivos de informática, em conformidade com as normas estabelecidas pela organização.

CA 2.2. Explicar as causas comuns de falhas em equipamentos informáticos, distinguindo entre problemas de hardware e software, e descrevendo métodos para prevenir falhas recorrentes.

CA 2.3. Verificar o funcionamento anormal de um computador ou computador, examinando quais os cabos de alimentação e de dados que estão ligados e ajustados, analisando o significado dos sinais luminosos e os possíveis códigos ou mensagens de erro.

CA 2.4. Substituir os cabos de alimentação e de dados nos equipamentos e dispositivos do sistema de computador, desligando o cabo antigo e ligando o novo no seu lugar, verificando se a funcionalidade e a ligação do sistema do computador foram restabelecidas.

CA 2.5. Substituir componentes de hardware de um computador, desligando o componente antigo e ligando o novo no seu lugar, seguindo as medidas de segurança para o manuseamento de componentes eletrónicos, utilizando ferramentas específicas (chave de fendas, alicates, entre outras) e verificando se a funcionalidade do equipamento foi reposta.

CA 2.6. Registar as tarefas executadas, bem como os incidentes de hardware detetados, detalhando o estado do dispositivo computacional e a ação realizada, utilizando o suporte físico ou computacional indicado.

CA 2.7. Selecionar os resíduos e descartáveis resultantes das operações realizadas para a sua gestão ou reciclagem, classificando-os de acordo com a sua tipologia.

RA3: Demonstrar responsabilidade e compromisso ao realizar operações de manutenção e manuseio de equipamentos informáticos, assegurando a qualidade do trabalho e a segurança durante as atividades.

CA 3.1. Cumprir as normas de segurança durante o manuseio de equipamentos e materiais, garantindo a integridade física dos dispositivos e a segurança do ambiente de trabalho, conforme as normativas de segurança estabelecidas.

CA 3.2. Manter uma atitude proativa, identificando necessidades de manutenção preventiva e sugerindo melhorias para otimizar o desempenho dos sistemas, cumprindo prazos e padrões de qualidade, de acordo com as especificações dos dispositivos.

CA 3.3. Cumprir os procedimentos de registo e documentação das atividades de manutenção, incluindo incidentes, ações corretivas e status dos equipamentos, garantindo a rastreabilidade e a transparência no processo, conforme as diretrizes de controle de qualidade.

CA 3.4. Demonstrar capacidade de comunicação clara e eficaz com a equipe e superiores, reportando incidentes e sugerindo melhorias para as operações de manutenção, conforme as necessidades do ambiente de trabalho e a dinâmica da equipe.

CA 3.5. Adotar uma abordagem detalhada e cuidadosa ao manusear dispositivos e componentes sensíveis, assegurando que todas as operações de manutenção sejam realizadas sem causar danos aos equipamentos, respeitando as especificações do fabricante e as normas de segurança.

CA 3.6. Garantir a utilização correta de ferramentas e equipamentos de proteção individual (EPIs), assegurando a segurança pessoal e a de terceiros durante a execução de tarefas de manutenção, conforme as normas de segurança e saúde no trabalho.

RA4: Aplicar operações de etiquetagem, embalagem, armazenamento e transferência de equipamentos e dispositivos informáticos, consumíveis, entre outros, utilizando ferramentas (de etiquetagem e embalagem, por exemplo), materiais de embalagem, entre outros.

CA4.1 Descrever as condições de manuseamento, transporte e armazenamento de equipamentos de hardware e componentes de um sistema de informática, indicando o procedimento a seguir, materiais a utilizar e medidas de segurança aplicáveis.

CA4.2 Identificar os tipos de embalagens adequadas para equipamentos e dispositivos informáticos, consumíveis e outros, descrevendo suas características, medidas e as diretrizes para a sua gestão como resíduo.

CA4.3 Identificar as ferramentas necessárias para a etiquetagem e acondicionamento de equipamentos e dispositivos informáticos, consumíveis, descrevendo as suas funções e as medidas de segurança a serem adotadas durante a sua utilização.

CA4.4 Detalhar as técnicas de etiquetagem de equipamentos e dispositivos informáticos, consumíveis e outros, descrevendo os tipos de etiquetas, informações nelas contidas e o processo de aplicação.

CA4.5 Executar a embalagem de equipamentos e dispositivos informáticos num caso prático, utilizando as ferramentas e materiais fornecidos, incluindo: selecionar a embalagem e ferramentas adequadas ao tipo de dispositivo, preparar o equipamento para acondicionamento, embalá-lo e etiquetar a embalagem, separando e classificando os resíduos para posterior gestão.

Conteúdos

1. **Técnicas auxiliares para a manutenção de sistemas computadores**
   - **1.1.** Manutenção de sistemas informáticos:
   - **1.2.** Níveis de manutenção.
   - **1.3.** Técnicas de limpeza e conservação de equipamentos:
   - **1.4.** Ferramentas de diagnóstico.
2. **Elementos consumíveis dos sistemas de computadores**
   - **2.1.** Tipos e característica.
   - **2.2.** Medidas de conservação e gestão de resíduos.
   - **2.3.** Técnicas de etiquetagem, embalagem, armazenamento e transporte.
   - **2.4.** Procedimentos de rotulagem.
   - **2.5.** Embalagem de componentes.
   - **2.6.** Normas de segurança na movimentação.
   - **2.7.** Gestão de resíduos eletrónicos.
3. **Boas práticas de segurança para evitar danos físicos e elétricos**
   - **3.1.** Medidas de segurança no manuseio de equipamentos eletrônicos.
   - **3.2.** Prevenção de choques elétricos e curto-circuitos.
   - **3.3.** Manuseio seguro de baterias e fontes de alimentação.
   - **3.4.** Recomendações para ambientes de manutenção.
4. **Legislação ambiental e boas práticas para o descarte de resíduos eletrônicos**
   - **4.1.** Impacto ambiental dos resíduos eletrónicos.
   - **4.2.** Normas e regulamentações para o descarte de lixo eletrónico.
   - **4.3.** Procedimentos de separação e armazenamento de resíduos eletrónicos.
   - **4.4.** Boas práticas na reciclagem e reaproveitamento de componentes.

Outras Capacidades Associadas ao Módulo

- Responsabilidade Ambiental e Sustentabilidade.
- Organização e Gestão do Espaço de Trabalho.
- Comunicação e Trabalho em Equipe.
- Ética e Profissionalismo.

Requisitos Básicos do Contexto Formativo do Módulo

Espaços:

Os espaços onde deve decorrer o contexto formativo devem preencher os requisitos básicos estipulados pelo Sistema de Acreditação das Entidades Formadoras. (cf. Decreto-Lei nº6/2013, de 11 de fevereiro; Boletim Oficial nº9; I Série).

Professor(a) / Formador(a):

- O(A) professor(a) ou formador(a) deve possuir um Certificado de Aptidão Profissional que prove que o mesmo é detentor de formação pedagógica na abordagem por competências, segundo a lei.

- O(A) professor(a) ou formador(a) deve ter a formação técnica relacionada com os conteúdos do Módulo Formativo.
- O(A) professor(a) ou formador(a) deve ter experiência profissional, mínima de 3 anos, comprovada nas competências incluídas na Unidade de Competência associada ao Módulo Formativo.

Requisitos de Acesso ao Módulo Formativo

As condições de acesso ao módulo formativo constam no BO nº 20, I Série, Portaria Conjunta nº 09/2020 de 20 de fevereiro - Estrutura e Organização do Catálogo Nacional de Qualificações e Portaria Conjunta nº 10/2020 de 20 de fevereiro - Quadro Nacional de Qualificações.

MF3: Gestão de Informação e Documentação com Aplicações de Office e IA		
Código: MF379_3	Nível: 3	Duração: 150 Horas
Associado à UC379_3 Executar operações com ferramentas de escritório e IA,		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
▪ Unidade Formativa 1:	Manipulação de Informação com Ferramentas Office e IA.	UF488
▪ Unidade Formativa 2:	Produção e Edição de Conteúdos Multimédia	UF489

Unidade Formativa 1: Manipulação de Informação com Ferramentas Office e IA (UF488)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Utilizar corretamente ferramentas de processamento de texto para criação e formatação de documentos.

- **CA 1.1.** Criar documentos de texto aplicando formatação adequada (tipo e tamanho de letra, estilos, espaçamentos e alinhamentos).
- **CA 1.2.** Inserir e formatar tabelas, imagens, cabeçalhos, rodapés e numeração de páginas.
- **CA 1.3.** Aplicar funções de revisão e colaboração, incluindo comentários e controle de alterações.
- **CA 1.4.** Exportar e converter documentos para diferentes formatos (PDF, DOCX, entre outros).
- **CA 1.5.** Utilizar recursos avançados como mala direta e referências cruzadas para automação de documentos.
- **CA 1.6.** Configurar permissões e restrições para proteger o conteúdo dos documentos.

RA2: Aplicar os princípios fundamentais da organização e gestão da informação utilizando ferramentas Office.

- **CA 2.1.** Identificar as principais funcionalidades dos processadores de texto, folhas de cálculo, bases de dados e apresentações, relacionando-as com suas aplicações práticas.
- **CA 2.2.** Explicar os conceitos de formatação, organização e estruturação de documentos, destacando boas práticas na manipulação da informação digital.
- **CA 2.3.** Descrever as regras básicas de segurança e proteção de dados ao trabalhar com aplicações Office, garantindo a integridade da informação.

RA3: Criar e gerir apresentações multimédia para comunicação eficaz

- **CA 3.1.** Criar uma apresentação multimédia estruturada, aplicando princípios de comunicação visual, utilizando software de apresentações.
- **CA 3.1.** Integrar texto, imagens, gráficos e vídeos numa apresentação, respeitando critérios de clareza e coerência, utilizando ferramentas de edição.
- **CA 3.2.** Aplicar transições e animações moderadas numa apresentação, garantindo a fluidez da comunicação, de acordo com boas práticas profissionais.
- **CA 3.3.** Adequar o conteúdo e o design da apresentação ao público-alvo e ao objetivo da comunicação, demonstrando intencionalidade na escolha dos elementos visuais e textuais.
- **CA 3.4.** Apresentar a produção multimédia utilizando recursos técnicos de apoio e demonstrando competências de comunicação oral.

RA4. Gerir folhas de cálculo para tratamento e análise de informação em contextos profissionais.

- **CA 4.1.** Criar uma folha de cálculo com fórmulas básicas e funções, assegurando a correção dos cálculos, em software de folhas de cálculo.

CA 4.2. Criar fórmulas automáticas personalizadas, utilizando operadores e referências relativas e absolutas, para resolver problemas específicos de cálculo em folhas de cálculo.

CA 4.3. Gerar gráficos a partir de dados numéricos, garantindo a clareza e a precisão da informação, utilizando software de folhas de cálculo.

CA 4.4. Organizar dados em tabelas com formatação adequada (títulos, filtros, formatação condicional), facilitando a leitura, a análise e a interpretação da informação.

CA 4.5. Aplicar funções de análise de dados demonstrando a capacidade de extrair conclusões relevantes a partir dos dados tratados.

CA 4.6. Produzir um relatório de análise de dados, a partir de folhas de cálculo, respeitando os requisitos definidos para o contexto profissional.

RA4: Demonstrar autonomia e responsabilidade na manipulação e gestão de documentos digitais.

CA 4.1. Aplicar metodologias eficazes na organização e armazenamento de documentos digitais, garantindo fácil acesso e recuperação da informação.

CA 4.2. Utilizar corretamente normas e padrões para a criação e partilha de documentos, respeitando princípios éticos e de confidencialidade.

CA 4.3. Adotar boas práticas de segurança e manutenção da informação ao utilizar ferramentas Office, garantindo a preservação dos dados e a minimização de riscos.

CA 4.4. Utilizar serviços de armazenamento na nuvem para compartilhamento e colaboração.

CA 4.5. Aplicar medidas básicas de segurança na gestão de informação digital (senhas, permissões de acesso e cópias de segurança).

CA 4.6. Automatizar tarefas com macros ou modelos predefinidos para otimizar a produtividade.

CA 4.7. Utilizar ferramentas de pesquisa e indexação para localização rápida de documentos.

CA 4.8. Implementar políticas de backup e recuperação de dados para evitar perda de informação.

RA5: Pesquisar informação técnica sobre utilização do sistema informático.

CA 5.1. Identificar os diferentes tipos de browsers;

CA 5.2. Reconhecer os motores de busca de informação e suas funcionalidades;

CA 5.3. Identificar os factores que devem ser levados em consideração durante a pesquisa;

CA 5.4. Numa situação prática de pesquisa:

- Pesquisar informações online;
- Localizar informações na nuvem;
- Organizar e armazenar a informação reconhecida;
- Transferir as informações pesquisadas para nuvem.

RA6: Integrar ferramentas de Inteligência Artificial (como ChatGPT, Copilot, Google Bard, etc.) na recolha, produção e tratamento de informação relevante.

CA 6.1. Selecionar ferramentas de IA adequadas às necessidades de recolha, produção ou tratamento de informação, de forma autónoma e justificada.

CA 6.2. Recolher informação relevante com ferramentas de IA, a partir de fontes digitais diversas e com foco na fiabilidade e atualidade dos dados.

CA 6.3. Produzir conteúdos informativos (textos, relatórios, apresentações) com apoio de IA, garantindo coerência, clareza e adequação ao público-alvo e ao contexto.

CA 6.4. Organizar e resumir informação digital com ferramentas de IA, respeitando princípios de ética, privacidade e integridade dos dados.

CA 6.5. Comparar resultados obtidos com diferentes ferramentas de IA, em função da qualidade, precisão e utilidade da informação gerada.

Conteúdos

1. Ferramentas de escritório e práticas profissionais

1.1. Conceitos fundamentais de aplicações de escritório;

1.2. Principais categorias de software de escritório;

1.3. Aplicações de escritório e organização da informação;

1.4. Comparação de diferentes softwares: vantagens e limitações;

2. Processador de texto

2.1. A janela do processador de texto;

2.2. Manipulação de documentos;

2.3. Cópia, transferência e eliminação de blocos de texto;

2.4. Nomear, gravar e encerrar sessão de trabalho;

2.5. Localização e substituição de texto;

2.6. Marcas e numeração;

2.7. Formatação e espaçamento de caracteres;

2.8. Letras maiúsculas e minúsculas;

2.9. Formatação de parágrafos e configuração de tabulações.

2.10. Inserção de quebras de página;

2.11. Formatação de colunas;

2.12. Copiar formato;

2.13. Capitulares maiúsculas;

2.14. Limites e sombreados;

2.15. Numeração de páginas;

2.16. Configuração de página cabeçalhos e rodapés;

2.17. Nota de rodapé e símbolos;

2.18. Inserção de tabelas, imagens, gráficos e objetos;

2.19. Aplicação e gestão de estilos predefinidos;

2.20. Revisão e utilização de ferramentas de verificação ortográfica e gramatical;

2.21. Índice automático;

2.22. Configuração e impressão de um documento.

3. Pesquisa e organização de informação

3.1. Utilização de motores de busca e bases de dados;

3.2. Técnicas de pesquisa de Informações;

3.3. Critérios de validação de fontes: relevância, atualidade e fiabilidade;

3.4. Resumo e organização da informação em fichas técnicas;

3.5. Elaboração de relatórios de validação de fontes;

3.6. Download de arquivos;

3.7. Correio eletrónico;

3.8. Grupos/listas de discussão;

3.9. Boas práticas de comportamento na internet.

4. Responsabilidade e colaboração em ambiente digital

4.1. Planeamento de tarefas e cumprimento de prazos;

4.2. Normas de organização e segurança informática;

4.3. Ferramentas de colaboração online (ex.: Google Docs, Microsoft 365);

4.4. Comunicação clara e adequada em ambiente de trabalho digital;

4.5. Apresentação de trabalhos segundo normas de formatação e partilha.

5. Apresentações multimédia

5.1. Introdução a aplicação;

5.1.1. Interface da aplicação;

5.1.2. Modos de visualização;

5.1.3. Criar, abrir e guardar apresentações;

5.1.4. Estruturação de Apresentações

5.1.5. Planeamento de uma apresentação eficaz (objetivo, público-alvo, tempo);

5.1.6. Criação de um guião lógico de diapositivos;

5.1.7. Boas práticas de design e legibilidade;

5.1.8. Utilização de esquemas e modelos base;

5.2. Criação e Formatação de diapositivos.

5.2.1. Inserção de texto imagens e ícones;

5.2.2. Inserção e organização de slides;

5.2.3. Aplicação e personalização de layouts;

5.2.4. Formatação de texto e listas;

5.2.5. Utilização de formas e SmartArt;

5.3. Elementos Visuais e Multimédia.

5.3.1. Inserção de gráficos e tabelas;

5.3.2. Inserção de vídeos e áudios;

5.3.3. Edição de imagens (corte, efeitos, redimensionamento);

5.4. Aplicação de transições e animações moderadas;

5.4.1. Diferença entre transições e animações;

5.4.2. Utilizar transição de slides, efeitos e animação.

5.4.3. Aplicação de efeitos de entrada, ênfase e saída;

5.4.4. Ordem e tempo das animações;

5.4.5. Criação de apresentações automatizadas.

5.5. Princípios de comunicação visual em apresentações;

5.6. Boas práticas de fluidez na comunicação multimédia;

5.7. Modos de apresentação e exportação.

6. Folhas de cálculo

6.1. Inserção, cópia, e eliminação de folhas;

6.2. Alteração do nome das folhas;

6.3. Mover folhas dentro do livro;

6.4. Alteração da largura de colunas e altura de linhas;

6.5. Inserção e eliminação de células, colunas, linhas e folhas;

6.6. Seleção de folhas, células, linhas, colunas adjacentes e não adjacentes;

6.7. Transferência, cópia e eliminação de blocos de células;

6.8. Ocultar e mostrar linhas e colunas;

6.9. Ocultar e mostrar folhas;

6.10. Criação de séries de dados;

6.11. Anulação e repetição de comandos;

6.12. Fixação de paineis;

6.13. Formatação

6.13.1. Tipo, tamanho, efeitos e cor da letra;

6.13.2. Cor da letra;

6.13.3. Preenchimento das células;

6.13.4. Unir células;

6.13.5. Alinhamento horizontal e vertical;

6.13.6. Orientação do texto;

6.13.7. Moldar texto;

6.13.8. Formato numérico das células;

6.13.9. Formatar limite e sombreado;

6.13.10. Criar e editar tabelas;

6.13.11. Ordenação de dados;

6.13.12. Formatação automática;

6.13.13. Cópia de formatação;

6.13.14. Formatação condicional;

6.13.15. Fórmulas: Operadores; Precedências; Referências Relativa, Absoluta e Mista;

6.14. Principais funções de estatísticas, data e hora, matemática e lógica.

6.15. Criação de gráficos: tipos e personalização;

6.16. Utilização de filtros e ordenação de dados;

6.17. Análise de dados e produção de relatórios;

6.18. Configuração da Impressão;

6.18.1. Configuração da área de impressão;

6.18.2. Definição das opções de impressão, e configuração da página;

6.18.3. Visualizar e configurar a impressão;

6.18.4. Definir títulos de Impressão;

6.18.5. Inserção de Cabeçalhos e Rodapés.

4.Organizar e armazenar documentos digitais

4.1. Estruturar arquivos e pastas de forma eficiente.

4.2. Utilizar armazenamento em nuvem para compartilhamento.

4.3. Aplicar técnicas de recuperação de documentos.

4.4. Implementar medidas de segurança e recuperação.

4.5. Aplicar permissões de acesso e políticas de backup.

4.6. Automatizar tarefas para otimização da produtividade.

4.7. Garantir a conformidade com normas e regulamentações.

4.8. Utilizar macros no Excel para automatizar tarefas repetitivas.

4.9. Aplicar medidas de segurança digital.

5. Utilizar Ferramentas de Inteligência Artificial (IA)

5.1. Selecionar ferramentas de IA adequadas.

5.2. Recolher dados técnicos com IA.

5.3. Analisar respostas de IA.

5.4. Aplicar soluções de IA na resolução de incidentes técnicos.

5.5. Organizar dados de forma ética com IA.

5.6. Validar as respostas da IA.

5.7. Explorar novas funcionalidades de IA para aprendizagem contínuo.

Unidade Formativa 2: Produção e Edição de Conteúdos Multimédia (UF489)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Criar, editar e otimizar conteúdos multimédia (imagens e vídeos) para diferentes aplicações

- **CA 1.1.** Selecionar e utilizar ferramentas adequadas para edição de imagens e vídeos.
- **CA 1.2.** Aplicar técnicas de retoque e correção de cores para aprimorar imagens e vídeos.
- **CA 1.3.** Criar composições visuais utilizando camadas, máscaras e filtros em imagens.
- **CA 1.4.** Gravar e importar vídeos com configurações adequadas de resolução e taxa de quadros.
- **CA 1.5.** Aplicar cortes, transições e efeitos visuais para aprimorar a narrativa em vídeos.
- **CA 1.6.** Inserir e sincronizar elementos audiovisuais, como trilha sonora e legendas.
- **CA 1.7.** Exportar imagens e vídeos em formatos adequados para diferentes mídias digitais.
- **CA 1.8.** Utilizar técnicas de compressão para otimizar o tamanho de imagens e vídeos sem perda significativa de qualidade.
- **CA 1.9.** Otimizar conteúdos multimédia para utilização na web e redes sociais, garantindo qualidade e leveza do arquivo.

RA2: Aplicar os princípios básicos da produção multimédia, incluindo formatos de ficheiros, resolução, compressão e compatibilidade entre dispositivos.

- **CA 1.1.** Identificar os principais formatos de ficheiros multimédia, explicando as suas características e aplicabilidade em diferentes contextos, com base em documentação técnica.
- **CA 1.2.** Descrever as principais funcionalidades das ferramentas de edição de imagem, explicando os conceitos de brilho, contraste, saturação e aplicação de filtros para melhoria da qualidade visual.
- **CA 1.3.** Explicar as técnicas de edição de vídeo, incluindo cortes, transições e legendagem, e identificar softwares profissionais utilizados na área.
- **CA 1.4.** Identificar os princípios básicos da gravação e edição de áudio, explicando técnicas como ajuste de volume, aplicação de filtros e remoção de ruídos indesejados.
- **CA 1.5.** Explicar os procedimentos de exportação de conteúdos multimédia para diferentes formatos (JPEG, PNG, MP4, WAV, etc.), detalhando a importância da configuração de parâmetros como resolução, taxa de compressão e codec para garantir compatibilidade e qualidade.
- **CA 1.6.** Analisar os princípios de design e composição visual na produção de conteúdos multimédia, destacando a importância da criatividade e adequação ao público-alvo.

RA3: Produzir conteúdos multimédia adaptados a diferentes plataformas digitais

- **CA 3.1.** Adaptar formatos e resoluções para diferentes dispositivos e plataformas.
- **CA 3.2.** Utilizar ferramentas de edição para otimizar a experiência do utilizador.
- **CA 3.3.** Criar conteúdos que atendam a normas de acessibilidade digital.
- **CA 3.4.** Testar e validar a compatibilidade dos conteúdos multimédia em diversos ambientes.

CA 3.5. Publicar e distribuir conteúdos multimédia garantindo integração com redes sociais, sites e aplicações móveis.

RA4: Utilizar software de edição de imagem, vídeo e áudio para criar e modificar conteúdos multimédia de acordo com os requisitos definidos.

CA 4.1. Utilizar software de edição de imagem para ajustar brilho, contraste, saturação e aplicar filtros, garantindo a melhoria da qualidade visual de acordo com as especificações do projeto.

CA 4.2. Criar e editar vídeos aplicando cortes, transições e legendas, assegurando a coesão e atratividade do conteúdo final conforme os requisitos definidos.

CA 4.3. Gravar e editar áudio ajustando volume, aplicando filtros e removendo ruídos, garantindo qualidade sonora adequada para os diferentes meios de distribuição especificados.

CA 4.4. Exportar conteúdos multimédia para diferentes formatos (JPEG, PNG, MP4, WAV, etc.), configurando corretamente os parâmetros de resolução, taxa de compressão e codec, assegurando compatibilidade e qualidade.

CA 4.5. Aplicar princípios de design e composição visual na produção de conteúdos multimédia, garantindo criatividade e alinhamento com os objetivos do projeto e o público-alvo.

Conteúdos

1. **Introdução à edição de imagens digitais**

1.6. Técnicas de manipulação de imagens.

1.7. Composição visual e design gráfico.

1.8. Otimização de imagens para web.

1.9. Otimização de imagens para web e dispositivos móveis.

2. **Fundamentos da produção de vídeo**

2.6. Edição de vídeo.

2.7. Edição de áudio e sincronização.

2.8. Exportação e compressão de vídeos.

2.9. Exportação e compressão de vídeos para diferentes plataformas e dispositivos.

3. **Introdução à animação digital**

3.4. Criação de animações 2D.

3.5. Gráficos interativos e animação em interfaces digitais.

3.6. Exportação e aplicação de animações em diferentes media.

3.7. Exportação e aplicação de animações em diferentes media.

5. Adaptação de conteúdos para diferentes dispositivos

4.6. Normas de acessibilidade digital.

4.7. Testes de compatibilidade em múltiplas plataformas.

4.8. Distribuição e publicação de conteúdos multimédia.

4.9. Aplicação das normas de acessibilidade em vídeos, imagens e animações digitais.

4.10. Publicação e otimização de conteúdos para redes sociais e plataformas de vídeo.

Outras Capacidades Associadas ao Módulo

- Capacidade de trabalhar com software multimédia profissional.
- Capacidade de desenvolver conteúdos multimédia responsivos.
- Capacidade de utilizar técnicas de animação e efeitos visuais.

- Capacidade de lidar com diferentes formatos de media.
- Capacidade de implementar soluções multimédia interativas.
- Capacidade de analisar e interpretar feedback sobre conteúdos multimédia.

Requisitos Básicos do Contexto Formativo do Módulo

Espaços:

Os espaços onde deve decorrer o contexto formativo devem preencher os requisitos básicos estipulados pelo Sistema de Acreditação das Entidades Formadoras. (cf. Decreto-Lei nº6/2013, de 11 de fevereiro; Boletim Oficial nº9; I Série).

Professor(a) / Formador(a):

- O(A) professor(a) ou formador(a) deve possuir um Certificado de Aptidão Profissional que prove que o mesmo é detentor de formação pedagógica na abordagem por competências, segundo a lei.
- O(A) professor(a) ou formador(a) deve ter a formação técnica relacionada com os conteúdos do Módulo Formativo.
- O(A) professor(a) ou formador(a) deve ter experiência profissional, mínima de 3 anos, comprovada nas competências incluídas na Unidade de Competência associada ao Módulo Formativo.

Requisitos de Acesso ao Módulo Formativo

As condições de acesso ao módulo formativo constam no BO nº 20, I Série, Portaria Conjunta nº 09/2020 de 20 de fevereiro - Estrutura e Organização do Catálogo Nacional de Qualificações e Portaria Conjunta nº 10/2020 de 20 de fevereiro - Quadro Nacional de Qualificações.

MF4: Instalação de Redes de Área Local		
Código: MF175.1_3	Nível: 3	Duração: 120 Horas
Associado à UC175.1_3: Instalar, configurar e conectar equipamentos em redes locais.		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
▪ Unidade Formativa 1:	Princípios das Redes de Área Local	UF257.1
▪ Unidade Formativa 2:	Equipamentos de Interconexão	UF260.1

Unidade Formativa 1: Principios das Redes de Área Local (UF257.1)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar os conceitos fundamentais das Redes de Área Local (LAN)

- **CA 1.5.** Identificar corretamente os componentes principais de uma rede LAN, incluindo dispositivos de rede, protocolos e topologias.
- **CA 1.6.** Explicar a função de cada componente dentro da rede LAN, como switches, roteadores e pontos de acesso.
- **CA 1.7.** Relacionar os diferentes tipos de LANs (por exemplo, Ethernet, Wi-Fi) com suas vantagens e limitações.
- **CA 1.8.** Descrever as especificações técnicas dos cabos e conectores utilizados em LANs.
- **CA 1.9.** Demonstrar entendimento sobre o funcionamento e a operação dos protocolos básicos de rede, como TCP/IP.

RA2: Planear a estrutura e a topologia de uma Rede de Área Local

- **CA 2.1.** Escolher a topologia mais adequada (estrela, barramento, anel, etc.) para um determinado cenário de rede.
- **CA 2.2.** Projetar o layout físico e lógico da rede LAN, considerando a área a ser coberta, o número de dispositivos e a largura de banda necessária.
- **CA 2.3.** Selecionar os equipamentos necessários (switches, hubs, roteadores, etc.) com base no planeamento da rede.
- **CA 2.4.** Garantir a escalabilidade e a flexibilidade da rede projetada para futuras expansões.
- **CA 2.5.** Apresentar soluções para garantir a segurança e a integridade da rede, como segmentação e isolamento de tráfego.

RA3: Instalar os dispositivos e componentes necessários para configurar uma rede LAN

- **CA 3.1.** Realizar a instalação física de dispositivos de rede como switches, roteadores e pontos de acesso em conformidade com as boas práticas de cabeamento.
- **CA 3.2.** Conectar os dispositivos da rede utilizando os cabos e conectores apropriados, seguindo as normas técnicas de instalação.
- **CA 3.3.** Realizar a instalação física e a configuração inicial dos dispositivos de interconexão de acordo com as especificações técnicas e boas práticas.
- **CA 3.4.** Testar a conectividade entre os dispositivos da rede e diagnosticar problemas de instalação (por exemplo, falhas de conectividade).
- **CA 3.5.** Documentar o processo de instalação, incluindo a configuração de dispositivos e a topologia da rede para futuras manutenções.
- **CA 3.6.** Configurar VLANs (Redes Locais Virtuais) para segmentação do tráfego de rede, garantindo maior segurança e eficiência.

CA 3.7. Realizar testes de desempenho da rede, como análise de largura de banda e latência, para validar a configuração da rede LAN.

CA 3.8. Elaborar a documentação do processo de instalação, incluindo diagramas de rede, configurações aplicadas e justificativas técnicas, de forma detalhada e conforme normas estabelecidas

RA4: Configurar os parâmetros básicos da Rede de Área Local

CA 4.1. Configurar endereços IP estáticos ou dinâmicos para os dispositivos da rede, conforme necessário.

CA 4.2. Implementar a configuração de DHCP (Protocolo de Configuração Dinâmica de Host) para facilitar a atribuição de endereços IP.

CA 4.3. Verificar a comunicação entre os dispositivos da LAN utilizando ferramentas como ping e tracert para garantir a conectividade.

CA 4.4. Configurar VLANs e outros parâmetros de segmentação de rede, garantindo a segurança, o isolamento adequado e a otimização do tráfego.

CA 4.5. Realizar testes de desempenho da rede, como análise de largura de banda e latência, para validar a configuração da rede LAN.

CA 4.6. Utilizar ferramentas de diagnóstico de rede, como Wireshark e iPerf, para analisar a performance da rede, identificar gargalos e verificar a conformidade com os requisitos de projeto.

RA5: Seguir as normas e regulamentos técnicos para garantir a segurança e a integridade da rede LAN

CA 4.1. Identificar corretamente as normas e regulamentos técnicos aplicáveis à instalação e manutenção da rede LAN, garantindo conformidade com padrões nacionais e internacionais.

CA 4.2. Utilizar adequadamente os equipamentos de proteção individual (EPI) e coletiva (EPC) para assegurar a segurança pessoal e do ambiente de trabalho durante a instalação e manutenção da rede LAN.

CA 4.3. Aplicar procedimentos de aterramento e proteção contra surtos elétricos para garantir a integridade dos equipamentos e a continuidade do serviço, seguindo normas técnicas e recomendações dos fabricantes.

CA 4.4. Implementar medidas de proteção contra interferências eletromagnéticas para minimizar impactos no desempenho da rede, utilizando materiais adequados e boas práticas de cabeamento estruturado.

CA 4.5. Realizar a instalação e configuração da rede LAN assegurando a confidencialidade, integridade e disponibilidade dos dados, conforme as diretrizes de segurança da informação.

CA 4.6. Documentar corretamente as práticas adotadas na instalação e manutenção da rede LAN para garantir rastreabilidade e conformidade com os padrões técnicos, utilizando relatórios e registos padronizados.

CA 4.7. Seguir protocolos de desligamento e energização segura ao realizar intervenções na rede, prevenindo danos aos equipamentos e riscos de acidentes, conforme os procedimentos operacionais estabelecidos.

CA 4.8. Produzir e manter a documentação de conformidade da rede, incluindo políticas de segurança aplicadas, configurações de dispositivos e evidências de testes de vulnerabilidades, conforme normas técnicas e regulatórias.

Conteúdos

1.Introdução aos conceitos de redes LAN

1.1. Topologias de LAN.

1.2. Funcionamento e protocolos de LAN.

1.3. Função dos dispositivos: Switches, Roteadores, Pontos de Acesso Wi-Fi:

1.4. Protocolos básicos: TCP/IP, Ethernet.

2. Planeamento da rede LAN

2.1 Seleção da topologia.
2.2 Escolha de equipamentos.

2.3 Cálculo da capacidade da rede.

2.4 Considerações técnicas para a topologia e escalabilidade.

2.5 Cálculo de alcance e cobertura.

2.6 Segurança e isolamento de tráfego.

3.Instalação dos equipamentos de rede

3.1 Instalação física.

3.2 Conexão de dispositivos.

3.3Testes e diagnóstico de problemas de instalação

3.4 Verificação de cabos e conexões

3.5 Diagnóstico de falhas de conexão

4. Configuração Inicial da rede LAN

4.1 Atribuição de endereços IP

4.2 Configuração de segurança básica

4.3 Criação de VLANs

4.5 Verificação de desempenho da rede

4.6 Teste de conectividade

Outras Capacidades Associadas à Unidade Formativa

- Capacidade de análise e resolução de problemas de rede;
- Capacidade de implementação de protocolos de comunicação de redes;
- Capacidade de configuração e manutenção de dispositivos de rede;
- Capacidade de implementação de políticas de segurança em redes LAN.

Unidade Formativa 2: Equipamentos de Interconexão (UF260.1)

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar os Equipamentos de Interconexão em Redes LAN

CA 4.1. Identificar os diferentes tipos de equipamentos de interconexão (switches, hubs, roteadores, bridges, etc.) e suas funções dentro de uma rede LAN.

CA 4.2. Explicar a funcionalidade dos equipamentos de interconexão e como eles afetam o desempenho da rede, como através de redução de colisões ou segmentação de tráfego.

CA 4.3. Descrever as diferenças entre equipamentos de camada 2 e camada 3, como switches e roteadores, e quando usar cada um deles.

CA 4.4. Discutir a importância de uma boa escolha de equipamento de interconexão, levando em consideração fatores como velocidade de transmissão, capacidade de portas e tipos de protocolos suportados.

CA 4.5. Elaborar uma configuração básica de uma rede utilizando diferentes equipamentos de interconexão, explicando o papel de cada um no tráfego de dados

RA2. Instalar e configurar equipamentos de interconexão

CA 2.1. Instalar fisicamente equipamentos de interconexão, como switches e roteadores, em um ambiente de rede local.

CA 2.2. Configurar parâmetros básicos dos dispositivos de interconexão, como endereçamento IP, VLANs e parâmetros de segurança.

CA 2.3. Verificar o correto funcionamento do equipamento após a instalação e configuração, utilizando ferramentas de diagnóstico de rede.

CA 2.4. Aplicar técnicas para otimização do tráfego de dados por meio da configuração de equipamentos de interconexão (como QoS e Spanning Tree Protocol).

CA 2.5. Identificar e corrigir erros comuns de configuração durante a instalação e manutenção de equipamentos de interconexão.

RA3: Interconexão Trabalhar de forma colaborativa e ética na implementação e manutenção dos equipamentos de interconexão, promovendo um ambiente profissional eficiente e seguro.

CA 3.1. Cumprir as normas técnicas e de segurança na instalação e configuração dos equipamentos de interconexão, garantindo a proteção da infraestrutura e a integridade da rede, de acordo com os padrões estabelecidos.

CA 3.2. Manter a documentação técnica atualizada e organizada, registando configurações e alterações realizadas nos equipamentos de interconexão, de acordo com os procedimentos internos da organização.

CA 3.3. Respeitar as diretrizes de segurança e privacidade na configuração dos equipamentos, implementando práticas adequadas de controle de acesso e encriptação, conforme as políticas da organização.

CA 3.4. Adotar uma postura proativa na identificação e resolução de problemas de interconexão, utilizando ferramentas de diagnóstico adequadas e propondo soluções eficazes, seguindo as melhores práticas da área.

CA 3.5. Demonstrar colaboração e ética no trabalho em equipa, comunicando-se de forma clara e respeitosa com colegas e superiores, de modo a garantir a eficiência na instalação e manutenção dos equipamentos.

RA4: Diagnosticar e resolver problemas de interconexão

CA 4.1. Diagnosticar falhas de conectividade em redes locais causadas por equipamentos de interconexão, como switches e roteadores.

CA 4.2. Utilizar ferramentas de diagnóstico de rede (como ping, tracert, e diagnósticos integrados nos próprios dispositivos) para identificar problemas relacionados à interconexão.

CA 4.3. Aplicar soluções para problemas comuns de interconexão, como loops de rede, colisões e falhas de roteamento.

CA 4.4. Verificar as configurações de VLAN e protocolos de roteamento em equipamentos de interconexão para garantir a comunicação eficiente entre os dispositivos.

CA 4.5. Reparar e substituir equipamentos de interconexão com falhas, seguindo procedimentos corretos de substituição e manutenção.

CA 4.6. Avaliar os riscos de segurança associados a diferentes tipos de equipamentos de interconexão e aplicar práticas recomendadas para mitigação desses riscos.

CA 4.7. Documentar e manter registos de configurações de segurança dos equipamentos, incluindo logs de acesso e alterações

Conteúdos

1. Introdução aos equipamentos de interconexão

1.1. Definição de equipamentos de interconexão.
1.2. Função dos equipamentos de interconexão na rede.
1.3. Topologias de redes e a influência dos equipamentos.
1.4. Tipos de equipamentos de interconexão.
1.5. Instalação e configuração de equipamentos de interconexão.
1.6. Configuração de equipamentos: switches, roteadores.

2. Gestão de segurança de equipamentos de interconexão

2.1. Introdução à segurança de redes.
2.2. Ameaças e vulnerabilidades.

2.3. Medidas de segurança.
2.4. Monitoramento e manutenção.

3. Diagnóstico e resolução de problemas.

3.1. Introdução ao diagnóstico de redes.
3.2. Identificação de problemas de conectividade.
3.3. Resolução de problemas comuns.

4. Testes e Validação da Rede

4.1. Importância dos testes e validação.
4.2. Testando a rede.
4.3. Validação de segurança.
4.4. Documentação.

Outras Capacidades Associadas à Unidade Formativa

- Análise e diagnóstico de redes.
- Aplicação de protocolos de rede.
- Segurança de redes.
- Gestão e monitoramento de redes.

Requisitos Básicos do Contexto Formativo do Módulo

Espaços:

Os espaços onde deve decorrer o contexto formativo devem preencher os requisitos básicos estipulados pelo Sistema de Acreditação das Entidades Formadoras. (cf. Decreto-Lei nº6/2013, de 11 de fevereiro; Boletim Oficial nº9; I Série).

Professor(a) / Formador(a):

- O(A) professor(a) ou formador(a) deve possuir um Certificado de Aptidão Profissional que prove que o mesmo é detentor de formação pedagógica na abordagem por competências, segundo a lei.
- O(A) professor(a) ou formador(a) deve ter a formação técnica relacionada com os conteúdos do Módulo Formativo.
- O(A) professor(a) ou formador(a) deve ter experiência profissional, mínima de 3 anos, comprovada nas competências incluídas na Unidade de Competência associada ao Módulo Formativo.

Requisitos de Acesso ao Módulo Formativo

As condições de acesso ao módulo formativo constam no BO nº 20, I Série, Portaria Conjunta nº 09/2020 de 20 de fevereiro - Estrutura e Organização do Catálogo Nacional de Qualificações e Portaria Conjunta nº 10/2020 de 20 de fevereiro - Quadro Nacional de Qualificações.

MF5: MANUTENÇÃO DA SEGURANÇA NO SISTEMA INFORMÁTICO		
Código: MF176.1_3	Nível: 3	Duração: 80 Horas
Associado à UC176.1_3: Manter a segurança num sistema informático.		

Unidade formativa 1: Procedimentos de Segurança no Sistema Informático UF261.1

Resultados de Aprendizagem (RA) e critérios de avaliação (CA)

RA1: Analisar as condições de risco dos equipamentos informáticos com base em fatores de segurança física e lógica

CA 1.1. Identifica e descreve corretamente os principais fatores de risco físico (temperatura, humidade, poeiras, vibração, intrusão física) e lógico (acessos indevidos, malware, falhas de software) associados a equipamentos informáticos.

CA 1.2. Avalia o impacto das condições ambientais e operacionais sobre a integridade e desempenho dos sistemas, com base em cenários reais.

CA 1.3. Reconhece situações de risco iminente para os equipamentos, propondo medidas de mitigação preventiva baseadas em boas práticas (ex: ISO/IEC 27002).

CA 1.4. Utiliza listas de verificação (checklists) e/ou ferramentas digitais para a inspeção e monitorização das condições ambientais.

CA 1.5. Distinguir as condições dos equipamentos que sejam suscetíveis de produzir falhas ou gerar riscos de segurança.

CA 1.6. Numa situação pratica:

- Distinguir avisos de segurança gerados por sistemas de monitorização ou inspeção de arquivos de log.
- Propor ações de melhoria das condições de risco detetadas.
- Realizar as ações que devem ser realizadas conforme os planos de contingência.

RA2: Interpretar avisos de segurança e propor medidas de melhoria em resposta a incidentes ou riscos identificados

CA 2.1. Interpreta corretamente alertas e mensagens geradas por ferramentas de monitorização de segurança (SIEM, antivírus, firewalls, logs do sistema).

CA 2.2. Identifica padrões de comportamento suspeito com base na análise de registos e correlação de eventos.

CA 2.3. Propõe ações corretivas e preventivas de acordo com o plano de segurança da organização e os princípios de gestão de risco.

CA 2.4. Colabora na atualização dos planos de contingência e resposta a incidentes, incorporando as lições aprendidas.

CA 2.5. Numa situação prática:

- Aplicar procedimentos de cópia e restauração de dados seguindo as especificações recebidas.
- Classificar, etiquetar e arquivar os suportes de cópia de segurança.
- Registar as tarefas desenvolvidas nos formulários previstos para tal efeito.

RA3: Aplicar procedimentos de cópia de segurança e de recuperação de dados, garantindo a sua integridade e disponibilidade

CA 3.1. Executa corretamente os procedimentos de cópia e restauração de dados e aplicações conforme as instruções técnicas e o plano de segurança.

CA 3.2. Identifica e seleciona os meios de armazenamento (físicos e digitais) mais adequados às necessidades e requisitos da organização, considerando critérios de custo, desempenho e segurança.

CA 3.3. Distingue diferentes tipos de backup (completo, incremental, diferencial) e suas vantagens e limitações.

CA 3.4. Utiliza ferramentas de backup profissionais (ex: Veeam, Acronis, Bacula) e demonstra domínio das suas funcionalidades essenciais.

CA 3.5. Regista e organiza adequadamente os suportes de cópia de segurança, aplicando boas práticas de etiquetagem, versionamento e arquivo.

CA 3.6. Descreve os riscos associados ao armazenamento inseguro de cópias de segurança e propõe soluções de mitigação (ex: encriptação, offsite/cloud backup).

CA 3.7. Descrever os riscos de segurança associados a mudanças no software instalado.

RA4: Gerir o processo de inventário e controlo do software instalado, com foco na segurança do sistema.

CA 4.1. Verifica regularmente o sistema de inventário de software, utilizando ferramentas específicas de auditoria e gestão de ativos (ex: OCS Inventory, GLPI, Lansweeper).

CA 4.2. Identifica discrepâncias entre o software instalado e o software registado no inventário, avaliando os riscos de segurança associados.

CA 4.3. Distingue entre software autorizado, não autorizado e potencialmente perigoso.

CA 4.4. Documenta e reporta as anomalias encontradas com clareza e precisão, utilizando formulários normalizados ou sistemas de ticketing.

CA 4.5. Produz relatórios de auditoria e inventário com qualidade e rigor, apoiando a tomada de decisão por parte dos responsáveis de segurança.

CA 4.6. Aplica boas práticas de escalonamento de incidentes e comunicação com a equipa de segurança ou superiores hierárquicos.

RA5: Demonstrar comportamentos responsáveis, colaborativos e éticos na implementação e manutenção da segurança do sistema informático.

CA 5.5. Cumpre rigorosamente os procedimentos definidos no plano de segurança, respeitando normas e políticas internas da organização.

CA 5.6. Comunica de forma clara, precisa e atempada as incidências de segurança aos responsáveis, utilizando os canais estabelecidos.

CA 5.7. Colabora eficazmente com colegas na resolução de problemas e na implementação de medidas corretivas ou preventivas.

CA 5.8. Demonstra proatividade na identificação de riscos, propondo melhorias nos procedimentos e ferramentas de segurança.

CA 5.9. Mantém uma postura ética no tratamento de informação sensível ou confidencial, respeitando os princípios da privacidade e proteção de dados.

CA 5.10. Regista de forma meticulosa as tarefas realizadas, mantendo a rastreabilidade das ações, conforme boas práticas profissionais.

Conteúdos:

1. Fundamentos de segurança informática

1.1. Conceitos essenciais

1.1.1. Confidencialidade, integridade e disponibilidade (CIA).

1.1.2. Princípios de segurança: defesa em profundidade, privilégio mínimo, confiança zero

1.1.3. Tipos de ameaças: físicas, lógicas, internas e externas

1.1.4. Tipos de ataques: Phishing, Ransomware, DDoS, engenharia social

1.2. Segurança física e lógica

1.2.1. Proteção de infraestruturas: controlo de acesso físico, videovigilância, sensores ambientais

1.2.2. Segurança lógica: antivírus, firewalls, gestão de identidades e acessos (IAM)

2. Gestão de risco e políticas de segurança

2.1. Análise e gestão de risco

2.1.1. Identificação de ativos críticos

2.1.2. Avaliação de ameaças e vulnerabilidades

2.1.3. Cálculo do impacto e priorização dos riscos

2.1.4. Metodologias: ISO/IEC 27005, OCTAVE, NIST RMF Xxx;

2.2. Políticas e planos de segurança

2.2.1. Desenvolvimento e estrutura de políticas de segurança

2.2.2. Plano de segurança organizacional: objetivos, recursos, medidas e ações

2.2.3. Gestão da continuidade e planos de contingência

3. Controlo de acessos e autenticação

3.1. Gestão de Utilizadores e Permissões

3.1.1. Controlo de acessos baseado em funções (RBAC) e atributos (ABAC)

3.1.2. Ferramentas de diretório (LDAP, Active Directory)

3.1.3. Gestão de contas privilegiadas (PAM)

3.2. Autenticação e autorização

3.2.1. Autenticação forte: 2FA/MFA, biometria

3.2.2. Protocolos de autenticação: Kerberos, RADIUS, TACACS+

4. Monitorização, deteção e resposta a incidentes

4.1. Monitorização e logs

4.1.1. Recolha e análise de logs: sistema operativo, firewall, antivírus, IDS/IPS

4.1.2. Ferramentas SIEM (ex: Splunk, Graylog, Wazuh)

4.1.3. Indicadores de compromisso (IoCs)

4.2. Gestão de Incidentes

4.2.1. Fases de resposta: deteção, análise, contenção, erradicação, recuperação

4.2.2. Planos de resposta a incidentes e documentação

4.2.3. Comunicação e escalonamento interno

5. Segurança do ambiente físico e condições operacionais

5.1. Instalações e infraestruturas

5.1.1. Fatores ambientais: temperatura, humidade, poeiras, vibração

5.1.2. Proteção contra sinistros: incêndio, inundações, falhas elétricas

5.1.3. Sistemas UPS e geradores

5.2. Riscos operacionais

5.2.1. Interferência eletromagnética, eletricidade estática

5.2.2. Ergonomia e segurança no posto de trabalho

5.2.3. Prevenção contra intrusão física

6. Cópias de segurança e recuperação de dados

6.1. Tipos e estratégias de backup

6.1.1. Backup completo, incremental, diferencial

6.1.2. Políticas de backup: frequência, retenção, versão

6.1.3. Backup local vs. backup na cloud

6.2. Ferramentas e procedimentos

6.2.1. Softwares profissionais: Veeam, Bacula, Acronis, Clonezilla

6.2.2. Testes de restauração e integridade dos dados

6.2.3. Encriptação e armazenamento offsite

7. **Inventário e gestão de software**

7.1. Inventariação e Auditoria

7.1.1. Ferramentas de inventário: OCS Inventory, GLPI, Lansweeper

7.1.2. Verificação de conformidade com licenças

7.1.3. Atualizações e correções de segurança (patch management)

7.2. Análise de risco aplicacional

7.2.1. Identificação de software não autorizado

7.2.2. Análise de vulnerabilidades (ex: CVEs, scanners de vulnerabilidades)

7.2.3. Riscos associados a aplicações obsoletas ou descontinuadas

8. Boas práticas, ética e comportamento profissional

8.1. Postura profissional

8.1.1. Comunicação eficaz e registo de atividades

8.1.2. Colaboração e resolução de problemas em equipa

8.1.3. Cumprimento de normas e políticas internas

8.2. Ética e privacidade

8.2.1. Tratamento responsável de dados pessoais e sensíveis

8.2.2. Regulamentos e leis aplicáveis (ex: GDPR, RGPD)

8.2.3. Ética profissional na segurança da informação.

Requisitos básicos do contexto formativo do Módulo

Espaços:

Os espaços onde deve decorrer o contexto formativo devem preencher os requisitos básicos estipulados pelo Sistema de Acreditação das Entidades Formadoras. (cf. Decreto-Regulamentar nº2/2011, de 24 de Janeiro; Boletim Oficial nº4; I Série).

- Sala com um mínimo de 30 m^2.
- Condições sanitárias adequadas.
- Climatização.
- Condições de segurança.
- Um computador por aluno.
- Vídeo – projector.
- Quadros.
- Acesso a Internet.
- Ambiente de trabalho e ferramentas *software* e *hardware* adequadas ao módulo formativo.

Professor / Formador:

- O Professor ou formador deve possuir um Certificado de Aptidão Profissional que prove que o mesmo é detentor de formação pedagógica na abordagem por competências, segundo a lei.
- O professor ou formador deve ter a formação técnica relacionada com os conteúdos do Módulo Formativo.
- O professor ou formador deve ter experiência profissional mínima de 3 anos, comprovada nas competências incluídas na Unidade de Competência associada ao Módulo Formativo.

Requisitos de acesso ao módulo formativo:

As condições de acesso ao módulo formativo constam no Artigo 15º, 16º, 17º 18º e 19º do Decreto-Lei nº 66/2010, de 27 de Dezembro (Cf. Boletim Oficial nº 50/2010; I Série, de 27 de Dezembro).

MÓDULO FORMATIVO EM CONTEXTO REAL DE TRABALHO	MT_TIC003.A1
Nível: 3	Duração indicativa: 360 Horas
Associado a todas as Unidades de Competência	

Resultados de Aprendizagem (RA) e Critérios de Avaliação (CA)

RA1: Aplicar os princípios fundamentais da arquitetura de computadores

CA 1.1. Identificar os componentes principais de um computador (CPU, memória, barramentos, dispositivos de entrada e saída), explicando suas funções e interações.

CA 1.2. Descrever os diferentes tipos de arquiteturas de computadores (Von Neumann, Harvard, RISC, CISC), destacando suas características e aplicabilidades.

CA 1.3. Explicar o conceito de ciclo de instrução e como ele é executado num processador, abordando a busca, decodificação e execução de instruções

CA 1.4. Analisar o impacto das tecnologias de armazenamento e cache na performance de sistemas computacionais, considerando aspetos como latência e largura de banda.

RA2: Saber planear, implementar e gerir projetos dentro do contexto real de trabalho, utilizando metodologias profissionais.

CA 2.1. Aplicar as metodologias de gestão de projetos para a organização e execução de atividades dentro do prazo e orçamento estabelecido.

CA 2.2. Identificar os stakeholders do projeto, analisar riscos e elaborar planos de mitigação para garantir o sucesso do projeto.

CA 2.3. Gerir o tempo e os recursos de forma eficiente, priorizando tarefas conforme a importância e impacto no projeto.

CA 2.4. Utilizar ferramentas de gestão de projetos (como Microsoft Project, Trello, ou Asana) para monitorizar o progresso, alocar tarefas e garantir a conformidade com o plano de execução.

CA 2.5. Avaliar a eficácia da comunicação no projeto, assegurando uma troca de informações clara e eficiente entre a equipa, stakeholders e clientes.

RA3: Analisar e interpretar as especificações técnicas dos componentes de hardware

CA 3.1. Comparar especificações técnicas e avaliar a compatibilidade entre os componentes de hardware (processador, memória RAM, armazenamento, etc.).

CA 3.2. Interpretar relatórios de testes de desempenho e justificar a escolha de componentes para diferentes cenários de utilização.

CA 3.3. Avaliar as especificações de sistemas de refrigeração e fontes de alimentação, considerando os requisitos de consumo energético e dissipação térmica dos componentes de hardware.

CA 3.4. Analisar as especificações de dispositivos de armazenamento (HDD, SSD, NVMe), comparando desempenho, capacidade e durabilidade para diferentes necessidades e orçamentos.

CA 3.5. Examinar as características de placas gráficas e adaptadores de vídeo, avaliando a sua compatibilidade com diferentes tipos de software e necessidades de processamento gráfico.

CA 3.6. Identificar e interpretar as especificações de dispositivos de conectividade (placas-mãe, portas USB, interfaces de rede), avaliando a compatibilidade com as tecnologias de comunicação e redes atuais.

RA4: Adotar boas práticas de organização e segurança

CA 4.1. Planear o ambiente de trabalho de forma segura e eficiente, mantendo os componentes e ferramentas organizados.

CA 4.2. Utilizar equipamentos de proteção pessoal, seguindo as normas de segurança estabelecidas.

CA 4.3. Descartar corretamente resíduos eletrónicos, seguindo as diretrizes ambientais da organização.

CA 4.4. Implementar medidas de segurança para prevenir danos a equipamentos e componentes, como a utilização de dispositivos de proteção contra surtos de energia e aterramento adequado.

CA 4.5. Garantir a proteção física e lógica dos dados sensíveis, aplicando técnicas de criptografia e controle de acesso adequado durante o manuseio e armazenamento de dispositivos.

CA 4.6. Seguir as diretrizes de segurança cibernética, mantendo softwares atualizados e protegidos contra vírus e malwares, além de garantir a integridade da rede e dos dispositivos conectados.

RA5: Aplicar procedimentos para montar, substituir e/ou ligar dispositivos internos de um sistema de computador

CA 5.1. Identificar as ferramentas e componentes necessários para a montagem, substituição ou ligação de componentes, seguindo as instruções recebidas.

CA 5.2. Selecionar e utilizar as ferramentas corretas (chaves de fenda, alicates, etc.) e as medidas de segurança (pulseira antiestática, luvas, etc.) durante o processo de montagem.

CA 5.3. Montar componentes de hardware (memória, processador, placa gráfica, etc.) na motherboard, ligando-os corretamente, conforme as especificações.

CA 5.4. Realizar testes de funcionamento dos componentes montados, assegurando que todos estão corretamente conectados e operando dentro dos parâmetros especificados.

CA 5.5. Diagnosticar e resolver problemas de montagem, substituição ou ligação de dispositivos internos, utilizando técnicas de troubleshooting e ferramentas adequadas.

RA6: Adaptar-se ao ambiente organizacional, compreendendo a cultura da empresa e interagindo de forma adequada com diferentes contextos profissionais.

CA 6.1. Compreender e respeitar a hierarquia e as normas da organização.

CA 6.2. Demonstrar flexibilidade no trabalho, adaptando-se a diferentes exigências e circunstâncias dentro da organização.

CA 6.3. Contribuir para a melhoria contínua da cultura organizacional, identificando oportunidades de desenvolvimento para si e para a empresa.

CA 6.4. Estabelecer relações profissionais de confiança e colaborar de forma eficaz com colegas e superiores, respeitando as diferenças e as competências de cada um.

CA 6.5. Demonstrar capacidade de comunicação eficaz em diferentes contextos organizacionais, ajustando a abordagem conforme a audiência e a situação.

RA7: Adotar boas práticas de segurança e sustentabilidade

CA 7.1. Utilizar os equipamentos de proteção adequados (luvas, pulseiras antiestáticas) durante a montagem e manutenção de sistemas informáticos.

CA 7.2. Garantir que todos os resíduos e materiais descartáveis sejam corretamente geridos e reciclados, conforme as políticas ambientais da organização. Manter a área de trabalho limpa e segura, conforme as normas de segurança e ergonomia estabelecidas pela empresa.

CA 7.3. Seguir procedimentos de segurança durante o manuseio de ferramentas e dispositivos, minimizando riscos de acidentes e danos aos equipamentos.

CA 7.4. Aplicar práticas de sustentabilidade na escolha de materiais e componentes, priorizando opções ecológicas e de baixo impacto ambiental sempre que possível.

CA 7.5. Participar ativamente de programas de sensibilização e treinamento sobre segurança e sustentabilidade, promovendo a conscientização entre os colegas de trabalho.

RA8: Aplicar corretamente os conhecimentos adquiridos em ambientes controlados para o desempenho das funções no contexto real de trabalho.

CA 8.1. Demonstrar a capacidade de aplicar os conceitos técnicos adquiridos na formação ao realizar as tarefas diárias no ambiente de trabalho.

CA 8.2. Adaptar-se às ferramentas e sistemas utilizados pela empresa, cumprindo prazos e requisitos estabelecidos.

CA 8.3. Implementar soluções práticas para problemas do dia a dia no ambiente de trabalho, utilizando as competências adquiridas.

RA9: Saber identificar as necessidades e as áreas de melhoria dentro do processo de trabalho real e sugerir melhorias com base nas competências adquiridas.

CA 9.1. Identificar áreas críticas no processo de trabalho que podem ser aprimoradas utilizando novas ferramentas ou processos.

CA 9.2 Propor e implementar melhorias ou sugestões que visem a otimização do fluxo de trabalho ou a resolução de problemas identificados.

CA 9.3. Trabalhar em colaboração com outros membros da equipe para analisar e melhorar processos existentes.

CA 9. 4. Avaliar continuamente a eficácia das soluções implementadas e fazer ajustes quando necessário, com base nos resultados e feedback recebidos.

CA 9.5. Colaborar com a equipa para resolver problemas complexos, utilizando o conhecimento técnico adquirido durante a formação e as melhores práticas do setor.

RA10: Aplicar, em contexto real, medidas de segurança física e lógica na proteção de equipamentos e infraestruturas informáticas.

CA 10.1. Identificar os fatores de risco físico e lógico no local de trabalho e propor medidas de mitigação adequadas, utilizando ferramentas e procedimentos recomendados.

CA 10.2. Executar rotinas de verificação e monitorização ambiental (temperatura, humidade, poeiras, acessos indevidos), utilizando ferramentas apropriadas e/ou checklists, conforme os procedimentos estabelecidos pela organização.

CA 10.3. Implementar procedimentos de controlo de acessos, proteção antivírus/firewall e configuração segura dos sistemas, conforme as melhores práticas de segurança e requisitos organizacionais.

CA 10.4. Aplicar boas práticas reconhecidas (ex: ISO/IEC 27002) no controlo de riscos operacionais, registando as ações realizadas de forma clara e estruturada, de acordo com os padrões estabelecidos pela organização.

RA11: Colaborar na implementação e documentação de medidas corretivas e preventivas em resposta a incidentes de segurança.

CA 11.1. Analisar alertas e eventos de segurança em tempo real (logs, antivírus, firewalls, SIEM) e relatar anomalias ou comportamentos suspeitos aos responsáveis, garantindo que a análise esteja de acordo com o plano de segurança.

CA 11.2. Executar tarefas de backup e restauração de dados, assegurando a integridade dos dados, conforme os procedimentos definidos pela organização e planos de segurança.

CA 11.3. Preencher corretamente formulários de registo de incidentes, backups e ações tomadas, garantindo rastreabilidade e conformidade com as normas internas da organização.

CA 11.4. Demonstrar iniciativa e responsabilidade na aplicação de medidas corretivas, comunicar com clareza e colaborar eficazmente com os colegas de equipa, de acordo com as políticas da organização.


SNQ