Ministério da Promoção de Investimentos e Fomento Empresarial

Unidade de Coordenação do Sistema Nacional de Qualificações

SISTEMA NACIONAL DE QUALIFICAÇÕES

Qualificação Profissional

INSTALAÇÃO, MONITORIZAÇÃO E SEGURANÇA DE REDES LOCAIS

TIC006_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
VPN	Virtual Private Network
GDPR	General Data Protection Regulation
SIEM	Security Information and Event Management
DoS	Denial of Service
WIDS	Wireless Intrusion Detection System
NIST	National Institute of Standards and Technology
TLS	Transport Layer Security
SSL	Secure Sockets Layer
IPSec	Internet Protocol Security
AES	Advanced Encryption Standard
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SNMP	Simple Network Management Protocol
SSH	Secure Shell
WIPS	Wireless Intrusion Prevention System

ÍNDICE

PERFIL PROFISSIONAL 5

UNIDADES DE COMPETÊNCIA (UC) 6

UC1: INSTALAR E CONFIGURAR DISPOSITIVOS DE COMUNICAÇÃO EM REDES LOCAIS 6

UC2: REALIZAR A MANUTENÇÃO PREVENTIVA E CORRETIVA EM REDES LOCAIS, OTIMIZANDO O DESEMPENHO, A CONFIABILIDADE E A SEGURANÇA DOS DISPOSITIVOS E SERVIÇOS DE COMUNICAÇÃO. 9

UC3: IMPLEMENTAR SOLUÇÕES DE INTERLIGAÇÃO ENTRE REDES PRIVADAS E PÚBLICAS DE FORMA EFICIENTE. 0

UC4: MONITORIZAR E DIAGNOSTICAR REDES LOCAIS PARA GARANTIA DE DESEMPENHO E CONTINUIDADE DO SERVIÇO 3

UNIDADES FORMATIVAS TRANSVERSAIS 7

UNIDADE FORMATIVA : Inglês Técnico (468) 7

UNIDADE FORMATIVA – Ferramentas Informáticas de Escritório**Erro! Marcador não definido.**

MÓDULOS FORMATIVOS (MF) 14

MF1: Instalação e Configuração de Redes Locais (MF000_0) 14

Unidade Formativa 1: Instalação e Configuração de Dispositivos de Comunicação em Redes Locais (UF470)..... **Erro! Marcador não definido.**

Unidade Formativa 2: Configuração e Diagnóstico de Equipamentos e Protocolos em Redes Locais (UF471)..... **Erro! Marcador não definido.**

MF2: Manutenção, Monitorização e Segurança de Redes Locais (MF369_3) 20

Unidade Formativa 1: Monitorização e Manutenção de Redes Locais (UF472)**Erro! Marcador não definido.**

Unidade Formativa 2: Segurança Física e Lógica em Redes Locais (UF473)**Erro! Marcador não definido.**

MF3: Instalação, Monitorização e Gestão de Interligações de Redes Locais e Públicas 26

Unidade Formativa 1: Gestão de Desempenho e Solução de Incidentes em Redes. (UF474) ..... **Erro! Marcador não definido.**

Unidade Formativa 2: Instalação e Configuração de Dispositivos de Interligação entre redes locais e públicas (UF475)..... **Erro! Marcador não definido.**

MF4: Gestão Avançada e Otimização de Redes Locais 32

MÓDULO FORMATIVO EM CONTEXTO REAL DE TRABALHO 36

PERFIL PROFISSIONAL

TIC006_3

INSTALAÇÃO, MONITORIZAÇÃO E SEGURANÇA DE REDES LOCAIS

<table>
<tr><th colspan="5">PERFIL PROFISSIONAL</th></tr>
<tr><td>Código</td><td>TIC006_3</td><td>Denominação</td><td colspan="2">INSTALAÇÃO, MONITORIZAÇÃO E SEGURANÇA DE REDES LOCAIS</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">Instalar e manter redes locais, assegurando a conectividade interna e externa, o acesso aos recursos da rede, a segurança informática e o cumprimento das normas ambientais, de proteção de dados e de propriedade intelectual e industrial.</td></tr>
<tr><td colspan="2" rowspan="5">UNIDADES DE COMPETÊNCIA</td><td>N.º</td><td>Denominação</td><td>Código</td></tr>
<tr><td>1</td><td>Instalar e configurar dispositivos de comunicação em redes locais</td><td>UC368_3</td></tr>
<tr><td>2</td><td>Realizar a manutenção preventiva e corretiva em redes locais, otimizando o desempenho, a confiabilidade e a segurança dos dispositivos e serviços de comunicação.</td><td>UC369_3</td></tr>
<tr><td>3</td><td>Implementar soluções de interligação entre redes privadas e públicas de forma eficiente.</td><td>UC370_3</td></tr>
<tr><td>4</td><td>Monitorizar e diagnosticar redes locais para garantia de desempenho e continuidade do serviço.</td><td>UC371_3</td></tr>
<tr><td colspan="2" rowspan="3">AMBIENTE PROFISSIONAL</td><td colspan="3">Âmbito Profissional:

O profissional exerce a sua atividade profissional no departamento de informática, com foco na operação e gestão de redes, em entidades públicas ou privadas, assim como em empresas de média ou grande dimensão. Pode desempenhar funções por conta própria ou por conta de outrem, independentemente da forma jurídica da organização. O profissional atua, quando aplicável, sob supervisão funcional e/ou hierárquica de um superior direto. Poderá também coordenar equipas de colaboradores, de forma ocasional, sazonal ou permanente. No desenvolvimento da sua atividade são adotados os princípios da acessibilidade universal e do design universal (ou design para todos), assegurando o cumprimento das normas e regulamentações aplicáveis.</td></tr>
<tr><td colspan="3">Setores:

O profissional atua maioritariamente no setor dos serviços, especificamente no subsetor de instalação e manutenção de redes informáticas, bem como em outros setores produtivos que, pela sua dimensão e organização, requeiram a implementação e gestão de redes.</td></tr>
<tr><td colspan="3">Ocupações e postos de trabalho relacionados:

CNP 2010:
● 3513 Técnico em redes e sistema de computadores.
● 7422 Instalador e reparador de tecnologias de informação e comunicação.
● 3512 Técnico de apoio aos utilizadores das tecnologias de informação e comunicação (TIC).

Sugestões:
● Técnico de sistemas informáticos.
● Técnico de redes locais.
● Instalador de equipamentos de comunicações.</td></tr>
</table>

UC1: INSTALAR E CONFIGURAR DISPOSITIVOS DE COMUNICAÇÃO EM REDES LOCAIS	
Código: UC368_3	Nível: 3

UNIDADES DE COMPETÊNCIA (UC)

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

EC 1: Instalar e configurar dispositivos de comunicação em redes locais, garantindo a compatibilidade e conectividade eficiente.

CD 1.1. A rede física é configurada de acordo com o meio de transmissão utilizado, a topologia da rede e a documentação técnica do fabricante, para garantir a correta instalação dos dispositivos e a funcionalidade da rede.

CD 1.2. O dispositivo é instalado no bastidor seguindo as instruções do fabricante e verificando parâmetros como alimentação elétrica, fixação mecânica, ligação à terra, temperatura e humidade, para assegurar condições adequadas de funcionamento.

CD 1.3. Os dispositivos de rede são conectados e configurados, utilizando ferramentas de monitorização para validar a conectividade e assegurar sua gestão remota conforme as especificações da organização.

CD 1.4. A ordem de serviço ou relatório técnico de instalação é preenchido utilizando modelos ou aplicações informáticas estabelecidas, registando detalhes como interligações efetuadas, data e hora da instalação e dados do técnico, para garantir a rastreabilidade dos processos.

CD 1.5. A configuração dos serviços de comunicação é realizada de acordo com os requisitos da rede e as especificações técnicas, garantindo a acessibilidade e funcionalidade tanto para utilizadores locais como remotos.

CD 1.6. As medidas de segurança são implementadas na configuração dos nós da rede, incluindo autenticação, encriptação e segmentação, para proteger a infraestrutura contra acessos não autorizados e ataques cibernéticos.

CD 1.7. Auditoria básica e documentação técnica são aplicadas na instalação de redes locais para garantir a conformidade com normas e boas práticas.

EC 2: Configurar dispositivos de rede, assegurando a sua funcionalidade tanto no arranque como na gestão posterior, de acordo com os requisitos e especificações operacionais definidos pela entidade responsável pela instalação.

CD 2.1. O funcionamento dos protocolos de gestão (como SNMP e SSH) é verificado após a ativação, para garantir a gestão remota eficaz dos dispositivos de comunicação.

CD 2.2. O software de encriptação é configurado nos nós de rede, criando redes privadas virtuais (VPN) através da interface específica, após a instalação, para garantir a segurança e a privacidade das comunicações.

CD 2.3. O nó da rede é incluído nos sistemas de monitorização, recolhendo parâmetros operacionais como frames geridos, largura de banda utilizada e erros/colisões, para garantir a gestão eficiente da infraestrutura.

CD 2.4. Os processos de configuração e testes são documentados, registando valores dos parâmetros, dados técnicos e outras informações relevantes, utilizando modelos ou aplicações informáticas estabelecidas pela entidade responsável, para garantir a rastreabilidade das atividades realizadas.

CD 2.5. As atualizações de firmware e patches de segurança são aplicadas regularmente nos dispositivos configurados, seguindo as recomendações do fabricante, para garantir a estabilidade e a proteção contra vulnerabilidades.

CD 2.6. Os acessos administrativos aos dispositivos de rede são configurados com autenticação segura e perfis de utilizador diferenciados, garantindo que apenas pessoal autorizado pode efetuar alterações na configuração.

CD 2.7. Metodologias estruturadas de troubleshooting, são implementadas utilizando abordagens como top-down, bottom-up e "divide and conquer", para identificar e resolver falhas de configuração de forma eficiente.

EC 3: **Corrigir falhas na instalação de dispositivos de rede, diagnosticando e aplicando soluções ou reportando-as conforme os planos de contingência, para assegurar a continuidade dos serviços de comunicação.**

CD 3.1. Os sistemas de notificação de incidentes são periodicamente revistos, assegurando resposta eficaz a falhas.

CD 3.2. A identificação de falhas é feita por meio de logs, sistemas de alarme e consulta à documentação técnica, permitindo diagnósticos precisos e ágeis.

CD 3.3. O problema é identificado e classificado, permitindo a aplicação rápida de soluções para restabelecimento dos serviços.

CD 3.4. Os incidentes não resolvidos são reportados ao nível superior conforme procedimentos estabelecidos.

CD 3.5. As ferramentas especializadas são utilizadas para corrigir falhas, garantindo conformidade com os protocolos da organização e recomendações dos fabricantes.

CD 3.6. Os incidentes são todos documentados, garantindo rastreabilidade e melhoria contínua do processo de resolução de problemas.

EC 4**: Implementar políticas de segurança e boas práticas na configuração e manutenção de redes locais, assegurando proteção contra vulnerabilidades e acessos não autorizados.**

CD 4.1. As configurações de segurança dos dispositivos de rede são realizadas conforme normas internacionais (ISO/IEC 27001, NIST) e políticas internas da organização, minimizando riscos de ataques cibernéticos.

CD 4.2. Os acessos administrativos são geridos com autenticação multifator (MFA), segregação de funções e permissões baseadas em perfis de utilizador, garantindo que apenas pessoal autorizado possa alterar configurações críticas.

CD 4.3. Os firewalls e sistemas de prevenção de intrusões são configurados e testados para bloquear tráfego malicioso e ataques direcionados, assegurando a integridade da rede.

CD 4.4. As auditorias periódicas são realizadas nas configurações da rede para identificar vulnerabilidades e assegurar conformidade com as melhores práticas de segurança.

CD 4.5. As políticas de backup e recuperação de desastres são implementadas para assegurar a continuidade dos serviços e a proteção dos dados críticos em caso de falha ou ataque.

CD 4.6. Os registos de logs e eventos de segurança são analisados e armazenados de acordo com regulamentos aplicáveis, permitindo a deteção precoce de ameaças e facilitando investigações forenses.

EC 5: **Implementar medidas de segurança para proteger a infraestrutura da rede local contra acessos não autorizados, garantindo a confidencialidade, integridade e disponibilidade dos dados.**

CD 5.1. As políticas de segurança da rede local são configuradas de acordo com as especificações da organização, utilizando firewalls atualizados, sistemas de deteção de intrusões e sistemas de prevenção de intrusões, para proteger a infraestrutura contra acessos não autorizados.

CD 5.2. A configuração de autenticação e controle de acesso é realizada utilizando sistemas como autenticação multifatorial, VPN e listas de controle de acesso, para garantir que apenas utilizadores autorizados tenham acesso à rede.

CD 5.3. O tráfego de dados na rede é monitorizado em tempo real, utilizando ferramentas de análise de pacotes como Wireshark, e logs de rede, para identificar e bloquear comportamentos anómalos que possam indicar tentativas de ataque, como negação de serviço ou vulnerabilidades.

CD 5.4. As políticas de encriptação de dados para proteger informações sensíveis em trânsito e em

repouso são implementadas, utilizando protocolos como TLS, SSL, AES (256 bits), e VPN de alta segurança, garantindo a confidencialidade e integridade dos dados.

EC 6: **Atualizar e manter as políticas de segurança de forma proativa, garantindo que as vulnerabilidades sejam identificadas e corrigidas rapidamente.**

CD 6.1. As políticas de segurança e proteção de dados são revistas regularmente e atualizadas conforme as mudanças nas ameaças de segurança e nas exigências legais, garantindo que a rede local esteja sempre protegida contra as novas vulnerabilidades.

CD 6.2. As atualizações de segurança de software e hardware são implementadas de forma regular e em conformidade com as recomendações do fabricante e as melhores práticas da indústria, para corrigir falhas de segurança.

CD 6.3. Os sistemas de monitorização contínua são configurados, utilizando ferramentas de gestão de vulnerabilidades como Nessus ou Qualys, para identificar e corrigir falhas de segurança na rede, tais como falhas no sistema operativo, em aplicações críticas ou em equipamentos de rede.

CD 6.4. As auditorias de segurança são realizadas internamente e por terceiros para avaliar a eficácia das medidas de segurança implementadas, identificar pontos fracos e recomendar melhorias, com base em frameworks como o NIST ou ISO/IEC 27001.

Meios de produção

Ferramentas de *software* para testes de conectividade. Ferramentas de *software* para controle de inventário de elementos de rede. Analisadores de redes. Certificadores de cablagem. Ferramentas manuais para trabalhos elétricos e mecânicos Computadores, impressoras e periféricos. Sistemas operativos. *Switches*, *routers*. Placas de rede. Cabos e conectores. Ferramentas de escritório. Mapas de rede. *Software* de gestão de rede. *Software* proprietário para dispositivos de rede.

Produtos e resultados

Nós de rede local instalados e operacionais. Dispositivos configurados e funcionais. Problemas detetados em dispositivos de rede resolvidos e reportados conforme necessário.

Informação utilizada ou gerada

Mapa de rede. Inventário de *hardware* da organização. Normas de proteção ambiental aplicáveis. Regulamentação relativa à propriedade industrial. Regulamentos de proteção de dados aplicáveis. Normas para o planeamento de ações preventivas. Manual de qualidade, incluindo padrões e critérios de qualidade. Ordens de serviço e peças. Documentação de rede. Plano de segurança. Plano de manutenção. Manuais de instalação de dispositivos. Manuais de configuração de dispositivos.

UC2: REALIZAR A MANUTENÇÃO PREVENTIVA E CORRETIVA EM REDES LOCAIS, OTIMIZANDO O DESEMPENHO, A CONFIABILIDADE E A SEGURANÇA DOS DISPOSITIVOS E SERVIÇOS DE COMUNICAÇÃO.	
Código: UC369_3	Nível: 3

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

EC 1: Monitorizar a rede local para detetar, resolver ou reportar avarias, assegurando o desempenho, evitando congestionamentos, garantindo o acesso aos servidores e seguindo os procedimentos da entidade responsável.

CD 1.1. A ferramenta de monitorização escolhida pelo administrador de rede é instalada e configurada, incluindo o servidor e a sonda local com os sensores necessários, garantindo a monitorização completa da rede local e a criação de uma plataforma de gestão unificada.

CD 1.2. Os ficheiros de registo de atividades dos serviços são recolhidos e analisados, assegurando a visibilidade, acessibilidade, integração e escalabilidade dos recursos de armazenamento e gestão, para identificar e resolver erros e conflitos.

CD 1.3. A interface da ferramenta de gestão de rede e os filtros de seleção de alarmes e alertas são configurados e personalizados, otimizando os processos de notificação e gestão de incidentes, conforme as necessidades específicas da rede e os padrões operacionais da organização.

CD 1.4. As auditorias periódicas à infraestrutura da rede são realizadas para validar a conformidade com os padrões de segurança e identificar possíveis vulnerabilidades ou melhorias necessárias.

CD 1.5. Os mecanismos de redundância e recuperação são implementados para minimizar o impacto de falhas na rede, assegurando a continuidade do serviço e a resiliência dos sistemas.

CD 1.6. Os mecanismos de automação para diagnosticar e resolver incidentes na rede são utilizados recorrendo a plataformas de automação como Ansible, Puppet e ferramentas avançadas de monitorização, agilizando a resposta a falhas e minimizando a intervenção manual.

EC 2: Manter os dispositivos da rede local através de revisões periódicas, verificação de alarmes e resolução de incidentes, garantindo os serviços de comunicação dentro dos requisitos definidos e seguindo os procedimentos do administrador da rede e os padrões do plano de manutenção preventiva.

CD 2.1. O mapa de rede é atualizado através de tarefas de descoberta realizadas na plataforma de gestão, garantindo uma visão atualizada dos dispositivos conectados conforme as especificações do administrador de rede.

CD 2.2. A conectividade dos dispositivos de rede (ativos e passivos) é verificada utilizando sinais acústicos-luminosos, comandos de rede específicos e análise de estatísticas de tráfego, com o objetivo de avaliar possíveis deteriorações ou alterações físicas e lógicas.

CD 2.3. As causas de comportamentos anómalos nos dispositivos de rede são identificadas através da metodologia de diagnóstico do plano de manutenção, utilizando ferramentas de diagnóstico de hardware e software e consultando a documentação técnica para localizar a origem dos erros.

CD 2.4. Os incidentes detetados, seja por inspeção ou por ferramentas de monitorização, são corrigidos por meio de diagnósticos e da implementação de medidas de resolução, como reset, atualização ou substituição de dispositivos, cablagem ou outras ações necessárias, realizadas de forma remota ou presencial.

CD 2.5. A segurança e configuração da rede são verificadas por meio de testes e utilizando ferramentas de segurança específicas, garantindo o cumprimento das políticas e normas estabelecidas pela organização, e gerando alertas em caso de anomalias.

CD 2.6. As ferramentas de diagnóstico avançado, como Wireshark e SolarWinds, são utilizadas para monitorização e análise de tráfego em tempo real, identificando e corrigindo problemas de desempenho.

EC 3: Atualizar hardware e firmware dos dispositivos de comunicação da rede local com os meios do fabricante, seguindo as especificações do administrador de rede e a documentação técnica para garantir eficiência e compatibilidade.

CD 3.1. O hardware dos equipamentos de comunicação é atualizado, parcial ou totalmente, utilizando os meios disponibilizados pelo fabricante, garantindo a adaptação a novas funcionalidades e requisitos tecnológicos, sem comprometer a compatibilidade com os sistemas existentes.

CD 3.2. O firmware atual dos equipamentos de comunicação é protegido por meio da criação de uma cópia de segurança da versão instalada, permitindo a sua restauração em caso de falha durante o processo de atualização.

CD 3.3. O firmware dos equipamentos de comunicação é atualizado através do site oficial do fabricante ou pela opção de pesquisa de atualizações no sistema operativo, garantindo a adaptação às novas funcionalidades e a verificação da autenticidade da fonte antes da instalação.

CD 3.4. As configurações dos equipamentos de comunicação são modificadas, incluindo a parametrização especificada pelo administrador de rede, para ajustar a sua funcionalidade ou integrá-los com novos equipamentos introduzidos na rede.

CD 3.5. A compatibilidade entre os novos componentes de hardware e firmware e os sistemas existentes é validada por meio de testes em ambiente controlado antes da implementação definitiva, assegurando a integração sem impactos negativos na rede local.

CD 3.6. As ações realizadas são documentadas utilizando o modelo ou a aplicação informática estabelecida pelo administrador de rede, registando detalhes como as referências dos dispositivos e a versão do firmware atualizado, garantindo a rastreabilidade dos processos.

EC 4: Verificar a segurança lógica e física dos dispositivos de rede local, assegurando a proteção dos dados e o acesso físico conforme as normas definidas.

CD 4.1. As notificações de alertas de segurança são atendidas através dos canais de comunicação das ferramentas de monitorização, utilizando as opções disponíveis nessas ferramentas para corrigir os incidentes reportados.

CD 4.2. Os ficheiros de auditoria dos dispositivos de comunicação são analisados para detetar acessos não autorizados, garantindo a confidencialidade e a integridade dos dados, conforme os procedimentos de segurança definidos pelo administrador de rede.

CD 4.3. Os dispositivos de comunicação são revistos, garantindo que o acesso físico e lógico seja controlado de acordo com os critérios de autenticação definidos pelo administrador de rede, garantindo a segurança dos sistemas.

CD 4.4. A rastreabilidade dos dados na rede é verificada, validando o cumprimento das normas legais relativas ao tratamento de dados, incluindo GDPR e outras regulamentações aplicáveis, utilizando ferramentas de rastreio específicas indicadas pelo administrador de rede.

CD 4.5. As ações realizadas são documentadas utilizando o modelo ou a aplicação informática estabelecida pelo administrador de rede, registando as atividades realizadas e garantindo a rastreabilidade dos sistemas e processos de segurança.

Contexto Profissional

Meios de produção

Ferramentas manuais para trabalhos elétricos e mecânicos. Analisadores de rede (sniffers). Certificadores de cablagem. Software proprietário para dispositivos de rede. Ferramentas de escritório. Ferramentas de auditoria. Ferramentas de diagnóstico. Aplicações de software para testes de conectividade. Ferramentas de software de inventário de equipamentos de rede. Computadores, impressoras e periféricos. Sistemas operativos. Switches e routers. Placas de rede. Cabos e conectores. Software cliente de rede. Software de gestão de rede. Sistemas de deteção e prevenção de intrusão sem fios (WIDS/WIPS). Software de monitorização de rede. Sondas de monitorização remota. Mapa de rede. Ferramentas de monitorização de cobertura de rede sem fios.

Produtos e resultados

Manutenção de dispositivos de rede local realizada de acordo com os padrões estabelecidos. Rede local monitorizada e otimizada. Segurança lógica e física comprovada e garantida, assegurando a integridade, confidencialidade e disponibilidade dos sistemas. Componentes de hardware e firmware dos dispositivos de comunicação de rede local devidamente atualizados.

Informação utilizada ou gerada

Inventário de hardware e configuração de rede detalhados. Normas de proteção de dados aplicáveis. Regulamentação aplicável sobre proteção ambiental, planeamento de ações preventivas e propriedade industrial. Mapas de rede atualizados. Peças de trabalho e ordens de serviço. Histórico de incidentes e avarias documentado. Documentação de rede completa. Especificações operacionais da organização. Manual de qualidade com padrões e critérios definidos. Manual de ferramentas de monitorização e gestão de rede. Plano de manutenção preventiva e corretiva. Plano de segurança abrangente. Manuais de instalação e configuração de dispositivos.

UC3: IMPLEMENTAR SOLUÇÕES DE INTERLIGAÇÃO ENTRE REDES PRIVADAS E PÚBLICAS DE FORMA EFICIENTE.	
Código: UC370_3	Nível: 3

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

EC 1: Instalar os nós de interligação entre redes, verificando os parâmetros técnicos e assegurando uma comunicação eficiente, em conformidade com as especificações da entidade responsável, a documentação do fabricante e um planeamento preventivo para garantir qualidade e segurança.

CD 1.1. Os requisitos de implementação do dispositivo são verificados, incluindo as linhas de comunicação e suas interfaces correspondentes, garantindo o cumprimento das condições de compatibilidade, conforme as especificações recebidas e a documentação técnica do fabricante.

CD 1.2. O dispositivo é instalado, verificando parâmetros como alimentação elétrica, fixação mecânica e ligação à terra, entre outros, para assegurar condições adequadas de funcionamento e segurança.

CD 1.3. As interfaces e módulos de adaptação das linhas de comunicação são instalados, verificando e garantindo a sua funcionalidade, e procedendo à sua ligação conforme os requisitos de implementação do dispositivo de comunicação.

CD 1.4. As linhas de comunicação e os dispositivos são ligados, verificando se a ligação está habilitada e funcional, garantindo a comunicação eficiente entre a rede pública e privada e a prestação do serviço de comunicações, com ênfase na estabilidade e redundância do enlace.

CD 1.5. O relatório técnico da instalação é elaborado utilizando o modelo ou a aplicação estabelecida pela entidade responsável, documentando detalhes como data da instalação, dispositivos, módulos e ligações, garantindo a rastreabilidade dos processos.

CD 1.6. As práticas de gestão de riscos são aplicadas para identificar pontos vulneráveis durante a instalação e integração dos dispositivos, e medidas preventivas são implementadas para mitigar falhas ou vulnerabilidades de segurança.

EC 2: Configurar os protocolos de comunicação nos dispositivos de interligação, garantindo conectividade eficiente entre redes, em conformidade com os parâmetros funcionais, requisitos operacionais e especificações técnicas da entidade responsável, assegurando interoperabilidade e desempenho adequado.

CD 2.1. Os equipamentos de comunicações ativas são configurados, utilizando a interface específica de cada dispositivo, ativando os parâmetros funcionais necessários para permitir a coexistência e/ou interligação de redes locais através de redes públicas, conforme as especificações técnicas.

CD 2.2. Os protocolos de roteamento (como OSPF, BGP) são configurados e otimizados nos dispositivos de interligação de rede, garantindo a seleção eficiente dos melhores caminhos para a transmissão de dados e assegurando a continuidade da comunicação entre redes privadas e públicas.

CD 2.3. As interfaces externas dos routers são configuradas utilizando ferramentas de gestão e software do fabricante, habilitando a sua funcionalidade e garantindo conectividade com redes externas, conforme os requisitos do operador de comunicações.

CD 2.4. As medidas de segurança nas comunicações são implementadas, com firewalls, VPN, segmentação de rede e outras soluções, configurando regras de acesso e validando-as para garantir a proteção das redes interligadas, com a verificação de parâmetros de segurança e criptografia.

CD 2.5. A monitorização contínua dos dispositivos de interligação é realizada por meio de ferramentas apropriadas, permitindo a deteção proativa de falhas, o ajuste dinâmico de configurações e a otimização do desempenho da rede conforme as necessidades operacionais.

CD 2.6. A automação da configuração e gestão de protocolos de rede é implementada, utilizando ferramentas de gestão de configuração como Ansible ou Terraform, para facilitar a integração e garantir a consistência da configuração ao longo do tempo, com uma abordagem de infraestrutura como código.

EC 3: Assegurar a continuidade e a qualidade do serviço na ligação à rede pública, gerindo incidências e alertas dos dispositivos de interligação e dos utilizadores, seguindo os protocolos de atuação para falhas definidas nos planos de contingência.

CD 3.1. Os sistemas de alerta e alarme são verificados com base nas informações fornecidas pelas ferramentas de monitorização, como Zabbix ou Nagios, para garantir a continuidade e a qualidade dos serviços de comunicação, ajustando os parâmetros de alarme conforme as necessidades operacionais.

CD 3.2. As notificações de incidentes dos utilizadores, recebidas através do Centro de Suporte ao Utilizador, são recolhidas e registadas no relatório ou numa aplicação de software de gestão de incidentes e avarias, para monitorização, estudo e análise.

CD 3.3. Os sintomas registados ou reportados pelos sistemas de alarme são verificados com base no histórico e na documentação técnica dos equipamentos, realizando testes conforme os procedimentos operacionais para diagnosticar a ocorrência.

CD 3.4. O incidente é corrigido utilizando ferramentas específicas para restaurar serviços interrompidos ou deteriorados, garantindo a rápida resolução do problema, e, em caso de falha, a infraestrutura de failover é acionada para assegurar a continuidade dos serviços.

CD 3.5. Os incidentes não resolvidos são reportados através dos canais de comunicação estabelecidos, encaminhando-os para o nível de responsabilidade mais elevado, de acordo com os protocolos de atuação definidos.

CD 3.6. Os testes periódicos de recuperação de desastres e de backup são implementados para garantir a continuidade dos serviços em caso de falhas maiores, incluindo a realização de simulações de falhas e testes de integridade dos backups.

EC 4: Implementar políticas de segurança e conformidade na interligação de redes, assegurando proteção contra ameaças e cumprimento das normas e regulamentações aplicáveis.

CD 4.1. As políticas de segurança são definidas e aplicadas, incluindo regras de firewall, autenticação de utilizadores e segmentação de rede, para mitigar riscos e proteger a comunicação entre redes.

CD 4.2. Os mecanismos de encriptação, como IPSec ou TLS, são implementados para garantir a confidencialidade e a integridade dos dados transmitidos entre redes privadas e públicas.

CD 4.3. A gestão de acessos e privilégios é configurada e auditada regularmente, utilizando sistemas de autenticação multifator e gestão de identidade para prevenir acessos não autorizados.

CD 4.4. As auditorias periódicas e testes de penetração (pentesting) são realizadas para identificar vulnerabilidades nos dispositivos de interligação e garantir a resiliência da infraestrutura de rede, com ênfase na análise de possíveis vetores de ataque e melhorias contínuas.

CD 4.5. Os registos de acesso e eventos de segurança são monitorizados e analisados através de ferramentas SIEM (Security Information and Event Management), permitindo uma resposta rápida a incidentes e ameaças emergentes.

CD 4.6. Os planos de resposta a incidentes de segurança são estabelecidos e testados regularmente, incluindo procedimentos para deteção, contenção, erradicação e recuperação de ataques ou falhas de segurança.

Contexto Profissional

Meios de produção

Ferramentas de gestão de rede. Ferramentas de controlo de linhas de comunicação públicas. Elementos de rede ativos. Analisadores de cabos. Sniffers (farejadores de rede). Mapa de rede atualizado e detalhado. Ferramentas manuais para trabalhos elétricos e mecânicos. Aplicações de software para testes de conectividade. Ferramentas de escritório. Ferramentas de diagnóstico. Aplicações de gestão de incidentes.

Produtos e resultados

Elementos de interligação de redes públicas e privadas mantidos em condições operacionais, garantindo a continuidade e a qualidade dos serviços de comunicação. Protocolos de comunicação nos dispositivos de interligação configurados e otimizados. Nós de interligação entre redes públicas e privadas instalados e funcionais Alertas gerados por sistemas de monitorização de rede geridos de forma eficiente.

Informação utilizada ou gerada

Regulamentos de proteção de dados em vigor. Ordens de serviço detalhadas. Normas aplicáveis ao planeamento de ações preventivas. Regulamentação relativa à propriedade industrial. Normas de proteção ambiental aplicáveis. Relatórios de incidentes documentados. Guias de resolução de problemas atualizados. Relatórios históricos de incidentes e avarias. Cursos de formação especializados. Padrões e critérios de qualidade definidos pela entidade responsável pelo sistema e pela entidade operadora. Relatórios técnicos de comissionamento. Manuais de dispositivos completos.

UC4: MONITORIZAR E DIAGNOSTICAR REDES LOCAIS PARA GARANTIA DE DESEMPENHO E CONTINUIDADE DO SERVIÇO	
Código: UC371_3	Nível: 3

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

EC 1: Monitorizar a rede local para detetar falhas e otimizar o desempenho, assegurando a continuidade dos serviços de comunicação.

CD 1.1. A ferramenta de monitorização de rede é instalada e configurada corretamente, incluindo o servidor de monitorização, as sondas e os sensores, garantindo que todos os componentes estejam operacionais para uma análise de desempenho eficiente.

CD 1.2. A plataforma de monitorização é configurada para incluir filtros de alarmes e relatórios personalizados, otimizando a resposta a incidentes e facilitando a gestão de rede.

CD 1.3. A rede é monitorizada regularmente em tempo real, utilizando ferramentas de gestão de rede para identificar e diagnosticar possíveis falhas de conectividade ou de desempenho, garantindo uma resposta rápida e eficaz, com foco na automação de alertas e ações corretivas.

CD 1.4. Os relatórios de desempenho e status da rede são gerados e revisados periodicamente, com recomendações para ajustes ou otimizações, a fim de manter a rede em operação contínua e eficiente.

CD 1.5. Os testes de performance de rede, como testes de largura de banda, latência, perda de pacotes e jitter, são realizados para garantir que os parâmetros operacionais estejam dentro dos limites estabelecidos pela entidade responsável.

CD 1.6. A configuração de redundância de rede e a implementação de backups são realizadas para garantir a continuidade do serviço em caso de falhas ou interrupções no sistema, com monitoramento contínuo para validar a eficácia das medidas de contingência.

EC 2: Diagnosticar falhas e aplicar soluções para garantir o desempenho ideal da rede local, assegurando a continuidade dos serviços de comunicação.

CD 2.1. O diagnóstico das falhas é realizado com base em alertas e registos de erro fornecidos pelas ferramentas de monitorização, identificando a origem do problema, a sua gravidade e o impacto nas operações da rede.

CD 2.2. As falhas identificadas são analisadas e ações corretivas são tomadas, como a reinicialização de dispositivos, reconfiguração de parâmetros de rede ou a substituição de componentes defeituosos, com base no diagnóstico preciso do problema.

CD 2.3. A análise de falhas é documentada, incluindo as causas prováveis, as soluções implementadas e o tempo de resolução, para garantir a rastreabilidade e a melhoria contínua do processo.

CD 2.4. O histórico de falhas e de diagnóstico é mantido e consultado para identificar padrões recorrentes e realizar ajustes preventivos no sistema, minimizando a ocorrência de falhas futuras.

CD 2.5. Os testes de stress e de capacidade da rede, quando necessário, são realizados para identificar possíveis limitações de desempenho e implementar soluções de escalabilidade.

CD 2.6. As ferramentas de diagnóstico de rede, como ping, traceroute, Wireshark e software de análise de tráfego, são utilizadas para diagnosticar a origem e a natureza de falhas na rede, realizando análises detalhadas para assegurar a precisão do diagnóstico.

EC 3: Garantir a continuidade dos serviços de rede, implementando medidas corretivas e preventivas para assegurar a estabilidade das comunicações.

CD 3.1. Os sistemas de alarme são configurados para notificar imediatamente qualquer falha ou degradação de desempenho, assegurando uma resposta rápida às interrupções ou falhas na rede.

CD 3.2. As incidências de rede são reportadas, documentadas e tratadas de acordo com os protocolos estabelecidos pela organização, garantindo a continuidade dos serviços enquanto as falhas são resolvidas.

CD 3.3. Os planos de contingência são seguidos durante as falhas para garantir que a continuidade dos serviços seja mantida, implementando soluções como failover automático, roteamento alternativo e protocolos de recuperação automática.

CD 3.4. As análises post-mortem são realizadas, após a resolução de falhas, para determinar a causa raiz e implementar medidas preventivas para evitar a recorrência do problema.

CD 3.5. A rede local é continuamente auditada para identificar vulnerabilidades de segurança e problemas de desempenho, com relatórios periódicos sendo gerados e analisados para melhorias contínuas, com a implementação de soluções corretivas imediatas conforme necessário.

CD 3.6. As atualizações de software, firmware e patches de segurança são aplicadas regularmente, de acordo com as especificações do fabricante, para minimizar vulnerabilidades e melhorar a estabilidade da rede, com testes de compatibilidade realizados antes da aplicação das atualizações.

Contexto Profissional

Meios de produção

Ferramentas de monitorização de rede (ex: Nagios, Zabbix, SolarWinds). Ferramentas de diagnóstico de rede (ex: Wireshark, PingPlotter, iPerf). Equipamentos de rede (switches, routers, servidores). Sistemas de backup e recuperação de dados. Ferramentas de análise de tráfego e logs. Plataformas de gestão de capacidade de rede.

Produtos e resultados

Rede local monitorizada e otimizada para desempenho e continuidade do serviço. Problemas de rede rapidamente diagnosticados e resolvidos. Estratégias de redundância e recuperação eficazes, garantindo a continuidade dos serviços em caso de falhas. Planeamento e gestão da capacidade da rede local, garantindo desempenho sustentável a longo prazo.

Informação utilizada ou gerada

Relatórios de monitorização de desempenho. Logs de diagnótico e auditorias de rede. Histórico de incidentes e relatórios de resolução. Planos de redundância e recuperação de rede. Planeamento de capacidade e projeções de crescimento.

FORMATIVO ASSOCIADO AO PERFIL PROFISSIONAL

TIC006_3

INSTALAÇÃO, MONITORIZAÇÃO E SEGURANÇA DE REDES LOCAIS

PROGRAMA FORMATIVO DA QUALIFICAÇÃO PROFISSIONAL			
Código: TIC006_3	Denominação	Instalação, Monitorização e Segurança de Redes Locais	
Nível: 3	Família Profissional	Tecnologias de Informação e Comunicação	
Duração indicativa	960 horas		
Unidades de Competência	N.º	Denominação	Código
	1	Instalar e configurar dispositivos de comunicação em redes locais.	UC368_3
	2	Realizar manutenção preventiva e corretiva em redes locais, otimizando desempenho, confiabilidade e segurança dos dispositivos e serviços de comunicação.	UC369_3
	3	Implementar soluções de interligação entre redes privadas e públicas de forma eficiente.	UC370_3
	4	Monitorizar e diagnosticar redes locais para garantia de desempenho e continuidade do serviço.	UC371_3

UNIDADES FORMATIVAS (UF) Básicas desta Qualificação Profissional				
Denominação			Duração	Código
Inglês Técnico			60 horas	UF468
Ferramentas Informáticas de Escritório			80 horas	UF469
MÓDULOS FORMATIVOS			UNIDADES FORMATIVAS	
N.º	Denominação	Código	Denominação	Código
1	Instalação e Configuração de Redes Locais (160 horas)	MF368_3	Instalação e Configuração de Dispositivos de Comunicação em Redes Locais (70 horas)	UF470
			Configuração e Diagnóstico de Equipamentos e Protocolos em Redes Locais (90 horas)	UF471
2	Manutenção, Monitorização e Segurança de Redes Locais (120 horas)	MF369_3	Monitorização e Manutenção de Redes Locais (60 horas)	UF472
			Segurança Física e Lógica em Redes Locais (60 horas)	UF473
3	Instalação, Monitorização e Gestão de Interligações de Redes Locais e Públicas (120 horas)	MF370_3	Gestão de Desempenho e Solução de Incidentes em Redes (60 horas)	UF474
			Instalação e Configuração de Dispositivos de Interligação entre redes locais e públicas (60 horas)	UF475
4	Gestão Avançada e Otimização de Redes Locais (60 horas)	MF371_3	---	---
MT_TIC006_3		Módulo Formativo em Contexto Real de Trabalho (360 horas)		

UNIDADES FORMATIVAS TRANSVERSAIS

UNIDADE FORMATIVA : Inglês Técnico (468)

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.

UNIDADE FORMATIVA – Ferramentas Informáticas de Escritório

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

RA1: Produzir documentação profissional utilizando aplicações informáticas de tratamento de texto, adequada ao objetivo e destinatário.

CA 1.1. Produzir um documento de texto com formatação consistente, aplicando estilos predefinidos, em ambiente de escritório.

CA 1.2. Inserir tabelas, imagens e objetos num documento de texto, assegurando a organização e a coerência gráfica, utilizando ferramentas de edição de texto.

CA 1.3. Rever e corrigir um documento de texto, utilizando funcionalidades de verificação ortográfica e gramatical, em tratamento de texto.

CA 1.4. Aplicar funcionalidades de automação, como sumário automático, numeração de páginas e índices, para estruturar documentos extensos de forma eficiente e profissional.

CA 1.5. Exportar e partilhar documentos em formatos apropriados (ex: PDF), assegurando a preservação da formatação e a compatibilidade com diferentes dispositivos e plataformas.

RA2: Pesquisar e validar informação técnica relevante para a utilização eficiente de sistemas informáticos em ambiente profissional.

CA 2.1. Pesquisar informação técnica em motores de busca e bases de dados, selecionando fontes fidedignas, mediante critérios de relevância e atualidade.

CA 2.2. Resumir e organizar a informação recolhida em fichas técnicas, utilizando aplicações de processamento de texto.

CA 2.3. Apresentar um relatório de validação de fontes de informação, justificando a escolha de cada fonte, em contexto profissional.

CA 2.4. Aplicar estratégias de verificação cruzada de dados, confrontando a informação recolhida com múltiplas fontes para assegurar a sua fiabilidade.

CA 2.5. Utilizar normas de citação e referenciação adequadas (APA), na apresentação da informação técnica recolhida, garantindo o respeito pelos direitos de autor.

RA3: Criar apresentações multimédia claras, apelativas e adequadas à comunicação em contextos profissionais.

CA 3.1. Criar uma apresentação multimédia estruturada, aplicando princípios de comunicação visual, utilizando software de apresentações.

CA 3.2. Integrar texto, imagens, gráficos e vídeos numa apresentação, respeitando critérios de clareza e coerência, utilizando ferramentas de edição.

CA 3.3. Aplicar transições e animações moderadas numa apresentação, garantindo a fluidez da comunicação, de acordo com boas práticas profissionais.

CA 3.4. 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 3.5. 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.

RA5: Compreender os conceitos e a aplicação prática das ferramentas de escritório em contextos profissionais.

CA 5.1. Definir os conceitos fundamentais das aplicações de escritório, apresentando exemplos práticos, em contexto simulado.

CA 5.2. Identificar as principais categorias de aplicações de escritório, relacionando-as com diferentes necessidades profissionais, através de análise de casos práticos.

CA 5.3. Reconhecer a importância da utilização das aplicações de escritório na organização da informação, através de exercícios de reflexão orientados.

CA 5.4. Analisar as vantagens e limitações das aplicações de escritório, comparando diferentes softwares num relatório escrito.

CA 5.5. Elaborar um plano de utilização integrada de ferramentas de escritório para a resolução de uma tarefa profissional, justificando a escolha das aplicações e funcionalidades.

RA6: Demonstrar atitudes de responsabilidade, organização e colaboração na utilização de ferramentas de escritório.

CA 6.1. Cumprir prazos estabelecidos na execução de tarefas, utilizando o planeamento adequado.

CA 6.2. Respeitar as normas de organização e segurança na utilização dos equipamentos e aplicações informáticas.

CA 6.3. Colaborar de forma eficaz com colegas na realização de atividades práticas de produção documental.

CA 6.4. Comunicar de forma clara e adequada no contexto das tarefas realizadas, utilizando as ferramentas de colaboração disponíveis.

CA 6.5. Apresentar trabalhos de forma organizada, respeitando os requisitos definidos para a formatação e partilha de documentos.

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.

MÓDULOS FORMATIVOS (MF)

MF1: Instalação e Configuração de Redes Locais (MF000_0)		
Código: MF368_3	Nível: 3	Duração Mínima: 160 Horas
Associado à UC368_3: Instalar e configurar dispositivos de comunicação em redes locais.		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
■ Unidade Formativa 1:	Instalação e Configuração de Dispositivos de Comunicação em Redes Locais	UF470
■ Unidade Formativa 2:	Configuração e Diagnóstico de Equipamentos e Protocolos em Redes Locais	UF471

Unidade Formativa 1: Instalação e Configuração de Dispositivos de Comunicação em Redes Locais (UF470)

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

RA1: Compreender os conceitos e tecnologias de redes locais.

- **CA 1.1.** Identificar as principais arquiteturas e tecnologias utilizadas em redes locais, distinguindo as suas aplicações e funcionalidades, considerando diferentes topologias e tipos de redes locais.
- **CA 1.2.** Enumerar os elementos que compõem o mapa físico de uma rede local, explicando suas funções e inter-relações em diferentes cenários de rede.
- **CA 1.3.** Explicar o funcionamento e as características dos dispositivos de rede, detalhando as funções de switches, routers, pontos de acesso, cabos e outras infraestruturas essenciais numa rede local.
- **CA 1.4.** Identificar normas técnicas e regulamentações aplicáveis à implementação de redes locais, considerando as exigências locais e internacionais para conformidade e segurança da rede.

RA2: Instalar e configurar dispositivos de comunicação em redes locais.

- **CA 2.1.** Enumerar e explicar os protocolos configuráveis num nó de rede, considerando os padrões adotados, como TCP/IP, DHCP, DNS, e outros protocolos de comunicação.
- **CA 2.2.** Configurar e instalar interfaces e módulos de equipamentos de rede, como switches, routers, e pontos de acesso, garantindo sua conectividade e funcionalidade para um desempenho eficiente da rede local.
- **CA 2.3.** Realizar a instalação física dos dispositivos em bastidores, verificando condições ambientais e elétricas adequadas, conforme os requisitos de segurança e desempenho.
- **CA 2.4.** Preencher relatórios técnicos documentando a instalação e configuração realizada, incluindo a descrição de cada etapa do processo, decisões tomadas e verificação de funcionalidade.

RA3: Demonstrar responsabilidade e rigor na instalação de redes locais.

- **CA 3.1.** Cumprir normas de segurança durante a instalação dos dispositivos de rede, minimizando riscos físicos e elétricos, e garantindo a correta utilização de equipamentos de proteção individual (EPIs).
- **CA 3.2.** Verificar a conformidade da instalação com as especificações técnicas, realizando testes e ajustes para assegurar a funcionalidade ideal e padrões de qualidade.
- **CA 3.3.** Cooperar em equipe durante a instalação e configuração dos dispositivos, promovendo a troca de conhecimentos técnicos e a colaboração eficaz entre os membros da equipe para alcançar os objetivos de forma eficiente e segura.

RA4: Diagnosticar e resolver falhas pontuais em dispositivos de comunicação de redes locais através da reconfiguração e substituição de componentes.

CA 4.1. Identificar problemas comuns em dispositivos de rede, como falhas de conectividade, problemas de configuração e erros de comunicação, utilizando ferramentas de diagnóstico apropriadas.

CA 4.2. Aplicar procedimentos de diagnóstico e ferramentas de rede, como testes de ping, tracert, e análise de logs, para identificar e localizar falhas nos dispositivos de comunicação.

CA 4.3. Resolver problemas de rede, corrigindo configurações e substituindo componentes defeituosos, garantindo o restabelecimento da conectividade e funcionalidade dos dispositivos de rede.

CA 4.4. Elaborar relatórios técnicos detalhados sobre os problemas encontrados, ações tomadas e soluções implementadas, proporcionando uma visão clara do processo de diagnóstico e resolução.

CA 4.5. Aplicar diferentes abordagens de troubleshooting (top-down, bottom-up, divide and conquer) para resolver falhas de conectividade.

CA 4.6. Utilizar ferramentas de análise de tráfego para monitorização de padrões anómalos e identificação de problemas de desempenho.

RA5: Realizar a monitorização e manutenção de dispositivos de comunicação de redes locais para prevenção de falhas através de manutenção e ajustes de desempenho.

CA 5.1 Implementar processos de monitorização contínua dos dispositivos de rede, utilizando ferramentas e software de gestão de redes para garantir a performance e integridade da infraestrutura.

CA 5.2 Realizar a manutenção preventiva em dispositivos de rede, como a atualização de firmware e a verificação de configurações, para minimizar falhas e otimizar o desempenho da rede.

CA 5.3 Estabelecer planos de manutenção e monitoramento, incluindo a verificação periódica da conectividade, condições ambientais e utilização de recursos da rede, para prolongar a vida útil dos dispositivos e evitar interrupções.

CA 5.4 Documentar as atividades de monitorização e manutenção realizadas, assegurando o acompanhamento e controle das operações e estabelecendo registos para futuras auditorias.

CA 5.5 Configurar e ajustar parâmetros de QoS para melhorar a qualidade e eficiência da rede.

CA 5.6 Implementar técnicas de load balancing para distribuição equilibrada do tráfego na rede.

Conteúdos

1. Fundamentos de Redes Locais

1.1. Conceitos básicos de redes de comunicação

1.1.1. Introdução aos princípios fundamentais de comunicação de dados em redes locais.

1.1.2. Definição de rede local (LAN), suas aplicações e benefícios.

1.2. Elementos constituintes de uma rede local.

1.2.1. Identificação dos principais componentes de uma rede local: switches, routers, pontos de acesso, cabos, interfaces, etc.

1.2.2. Funções e inter-relações de cada componente na operação de uma rede local.

1.3. Arquiteturas e topologias de redes locais

1.3.1. Estudo das principais arquiteturas de redes locais (em estrela, em barramento, em anel, etc.).

1.3.2. Análise das vantagens e desvantagens das diferentes topologias e a sua aplicabilidade em cenários diversos.

1.4. Normas e regulamentos aplicáveis às redes locais.

1.4.1. Compreensão das normas internacionais e locais para a instalação e configuração de redes locais (como IEEE 802, normas de segurança elétrica e regulamentos de conectividade).

1.4.2. Requisitos legais para segurança, proteção de dados e conformidade em instalações de redes.

1.4.3. Procedimentos de conformidade na instalação de redes, incluindo auditoria básica e documentação técnica.

1.4.4. Aplicação de normas de segurança na infraestrutura física da rede, incluindo certificação de cablagem e requisitos elétricos.

2. Meios de Transmissão e Infraestrutura de Rede

2.1. Tipos de meios de transmissão: cabos metálicos, fibra ótica e redes sem fio.

2.1.1. Estudo sobre os diferentes tipos de cabos utilizados em redes locais (cabo de par trançado, cabo coaxial, fibra ótica).

2.1.2. Vantagens e limitações de cada tipo de meio de transmissão, incluindo redes sem fio (Wi-Fi).

2.2. Sistemas de cablagem estruturada

2.2.1. Planeamento e implementação de cablagem estruturada conforme as normas de instalação.

2.2.2. Identificação e escolha dos componentes de cablagem (cabos, conectores, patch panels, etc.) e sua organização física.

2.3. Normas de instalação de cabos e conectores

2.3.1. Regras e boas práticas na instalação de cabos e conectores, conforme os padrões da indústria.

2.3.2. Considerações sobre a distância máxima de transmissão, impedância, e os métodos de proteção contra interferências.

2.4. Efeitos indesejáveis na transmissão: atenuação, ruído e interferências

2.4.1. Definição e explicação dos principais problemas que afetam a qualidade da transmissão de dados em redes locais.

2.4.2. Soluções para mitigar esses problemas, como a utilização de cabos blindados, e posicionamento adequado dos cabos.

2.5. Equipamentos auxiliares: UPS, baterias e climatização.

2.5.1. Importância da utilização de UPS (fontes de alimentação ininterrupta), baterias e sistemas de climatização para garantir o funcionamento contínuo e seguro dos dispositivos de rede.

2.5.2. Considerações sobre a escolha e instalação desses equipamentos de suporte para redes locais.

Outras Capacidades Associadas à Unidade Formativa

- Assumir a responsabilidade pelo trabalho realizado, garantindo a qualidade da instalação e configuração dos dispositivos de rede.
- Respeitar os procedimentos e regras internas da organização ao realizar a instalação dos equipamentos.
- Trabalhar de forma colaborativa, demonstrando respeito pelos colegas e aplicando boas práticas de comunicação profissional.

Unidade Formativa 2: Configuração e Diagnóstico de Equipamentos e Protocolos em Redes Locais (UF471)

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

RA1: Compreender protocolos de comunicação e sua configuração em redes locais (Saber)

- **CA 1.1.** Identificar os principais protocolos de rede utilizados em redes locais e suas respetivas funções.
- **CA 1.2.** Interpretar especificações técnicas para configuração de protocolos de comunicação em dispositivos de rede.
- **CA 1.3.** Explicar os parâmetros de configuração de protocolos que afetam a segurança e desempenho da rede.
- **CA 1.4.** Comparar diferentes protocolos de comunicação em termos de desempenho, escalabilidade e segurança, justificando a escolha mais adequada para diferentes cenários de redes locais.

RA2: Aplicar procedimentos de teste e verificação de conectividade em redes locais.

- **CA 2.1.** Utilizar ferramentas de verificação e monitorização para testar a conectividade e desempenho dos dispositivos de rede.
- **CA 2.2.** Configurar e testar protocolos de gestão remota, como SNMP e SSH, garantindo sua funcionalidade.
- **CA 2.3.** Documentar os procedimentos de teste e verificação, assegurando a rastreabilidade das operações.
- **CA 2.4.** Realizar testes de conectividade em diferentes camadas do modelo OSI, identificando possíveis falhas de rede e propondo soluções adequadas para cada camada.

RA3: Demonstrar proatividade e precisão na resolução de problemas de conectividade.

- **CA 3.1.** Diagnosticar e classificar incidentes de comunicação na rede local, utilizando ferramentas adequadas.
- **CA 3.2.** Aplicar soluções corretivas para incidentes de rede, garantindo a continuidade dos serviços.
- **CA 3.3.** Trabalhar de forma organizada e metódica na identificação e resolução de problemas de conectividade.

RA4: Configurar e otimizar dispositivos de rede para garantir a eficiência e segurança da rede local.

- **CA 4.1.** Configurar dispositivos de rede, como switches e routers, para garantir a comunicação eficiente entre os dispositivos da rede local, ajustando parâmetros de desempenho (como MTU, QoS e VLANs).
- **CA 4.2.** Implementar configurações de segurança, como listas de controle de acesso (ACLs), firewalls e VPNs, para proteger a rede local contra acessos não autorizados e ameaças externas.
- **CA 4.3.** Realizar testes de desempenho e segurança após a configuração, garantindo que os dispositivos estão a funcionar de acordo com as especificações e requisitos de rede.
- **CA 4.4.** Documentar as configurações realizadas, incluindo os parâmetros ajustados e as razões para as escolhas feitas, proporcionando uma base para auditorias e futuras manutenções.

RA5: Monitorizar o desempenho de redes locais e diagnosticar falhas em tempo real.

- **CA 5.1.** Utilizar ferramentas de monitorização, como Wireshark e ferramentas SNMP, para analisar o tráfego de rede e identificar potenciais falhas ou pontos de congestionamento.
- **CA 5.2.** Implementar sistemas de monitorização contínua para avaliar a saúde dos dispositivos de rede e a conectividade entre os nós, garantindo a deteção precoce de problemas.

CA 5.3. Diagnosticar falhas em tempo real, utilizando ferramentas de análise de tráfego e logs de dispositivos para localizar e resolver problemas de conectividade ou desempenho.

CA 5.4. Elaborar relatórios detalhados sobre o estado de monitorização da rede, incluindo a análise de incidentes, soluções aplicadas e recomendações de melhorias para prevenir futuras falhas.

Conteúdos

1. Protocolos e Modelos de Comunicação

1.1. Modelo OSI e TCP/IP

1.1.1. Introdução aos modelos de referência OSI e TCP/IP e suas camadas.

1.1.2. Comparação entre os modelos e suas aplicações práticas em redes locais.

1.2. Protocolos de comunicação em redes locais: Ethernet (IEEE 802.3); Wi-Fi (IEEE 802.11); LANs (IEEE 802.1Q); Bluetooth e outras tecnologias sem fio relevantes.

1.3. Endereçamento lógico e físico.

1.3.1. Endereçamento lógico (IPv4 e IPv6).

1.3.2. Endereçamento físico (MAC).

1.3.3. Sub-redes, máscaras de sub-rede e CIDR.

1.4. Protocolos de gestão e configuração remota.

1.4.1. SNMP (Simple Network Management Protocol).

1.4.2. SSH (Secure Shell).

1.4.3. Telnet e suas diferenças para SSH.

1.4.4. ICMP e sua importância na comunicação de rede.

2. Configuração de Protocolos e Serviços de Rede

2.1. Configuração de endereçamento IP.

2.1.1. Endereçamento IP estático e dinâmico (DHCP).

2.1.2. Subnetting e supernetting.

2.1.3. Configuração de gateway e DNS.

2.2. Configuração de protocolos de roteamento.

2.2.1. Protocolos de roteamento dinâmico: RIP (Routing Information Protocol) e OSPF (Open Shortest Path First).

2.2.2. Roteamento estático e sua utilização em redes locais pequenas.

2.2.3. Tabelas de roteamento e protocolos de roteamento híbridos.

2.3. Configuração de segurança em redes locais.

2.3.1. Implementação de firewalls: conceitos e práticas.

2.3.2. Configuração de VLANs para segmentação de rede.

2.3.3. Implementação de VPNs para segurança de comunicações remotas.

2.3.4. Autenticação e autorização em redes (RADIUS, TACACS+).

2.4. Configuração de qualidade de serviço (QoS).

2.4.1. Princípios e importância do QoS para redes locais.

2.4.2. Implementação de QoS em switches e routers.

2.4.3. Controle de largura de banda, priorização de tráfego e gestão de congestionamento

3. Diagnóstico e testes de conectividade em redes locais

3.1. Ferramentas de Teste e Monitorização de Redes.

3.1.1. Comandos básicos: ping, tracert, netstat, nslookup, ipconfig.

3.1.2. Ferramentas avançadas: Wireshark, Nmap, NetFlow.

3.2. Métodos de verificação de conectividade física e lógica.

3.2.1. Teste de cabos e conectores (utilização de multímetro e testadores de rede).

3.2.2. Análise de conectividade lógica entre dispositivos (checklist de comunicação).

3.3. Diagnóstico e resolução de problemas comuns em redes locais.

3.3.1. Identificação e resolução de problemas de conectividade (cabling, dispositivos e protocolos).

3.3.2. Problemas com DHCP, DNS, roteamento e endereçamento IP.

3.4. Testes de desempenho e monitorização de tráfego.

3.4.1. Testes de latência, perda de pacotes, e largura de banda.

3.4.2. Análise de tráfego de rede, utilizando ferramentas como Wireshark e Iperf.

3.5. Metodologias de diagnóstico e resolução de problemas em redes.

3.5.1. Aplicação do modelo OSI e TCP/IP na resolução de problemas de conectividade.

3.5.2. Abordagens de troubleshooting: top-down, bottom-up e "divide and conquer".

3.5.3. Diagnóstico estruturado de falhas em redes locais com base em padrões de sintomas e respostas.

4. **Gestão de incidentes e manutenção em redes locais**

4.1. Classificação de incidentes em redes locais.

4.1.1. Categorias de incidentes: falhas de conectividade, problemas de desempenho, e ameaças de segurança.

4.1.2. Classificação e priorização de incidentes conforme impacto na rede.

4.2. Processos de gestão de falhas e recuperação de redes.

4.2.1. Implementação de estratégias de recuperação de desastres em redes locais.

4.2.2. Backup de configurações e planos de recuperação para dispositivos de rede.

4.3. Ferramentas de monitorização e análise de logs.

4.3.1. Utilização de ferramentas de monitoramento (Zabbix, Nagios).

4.3.2. Análise de logs de sistemas e dispositivos de rede (syslog, logs de switches e routers).

4.4. Elaboração de relatórios de incidentes e ações corretivas.

4.4.1. Estruturação de relatórios claros e objetivos sobre falhas e soluções aplicadas.

4.4.2. Documentação de melhores práticas para prevenção de falhas futuras e melhorias de rede.

4.5. Gestão de incidentes e manutenção em redes locais.

4.5.1. Ajuste de configurações de QoS para otimizar o desempenho da rede.

4.5.2. Load balancing e gestão de tráfego para evitar congestionamentos e gargalos de rede.

4.5.3. Monitorização de padrões de tráfego anómalos para deteção de falhas e ameaças de segurança.

Outras Capacidades Associadas à Unidade Formativa

- Concluir o diagnóstico e resolução de problemas garantindo adequação, economia e eficácia.
- Adaptar-se a novas situações e contextos ao lidar com problemas inesperados e mudanças nas configurações da rede.
- Adaptar-se a novas situações e contextos ao lidar com problemas inesperados e mudanças nas configurações da rede.
- Aplicar o princípio da igualdade de tratamento e não discriminação na comunicação e na colaboração com a equipa de suporte técnico.

MF2: Manutenção, Monitorização e Segurança de Redes Locais		
Código: MF369_3	Nível: 3	Duração: 160 Horas
Associado à UC369_3: Realizar manutenção preventiva e corretiva em redes locais, otimizando desempenho, confiabilidade e segurança dos dispositivos e serviços.		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
■ Unidade Formativa 1:	Monitorização e Manutenção de Redes Locais	UF472
■ Unidade Formativa 2:	Segurança Física e Lógica em Redes Locais	UF473

Unidade Formativa 1: Monitorização e Manutenção de Redes Locais (UF472)

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

RA1: Explicar os fundamentos da monitorização de redes locais, identificando parâmetros e ferramentas utilizadas para deteção de incidentes.

CA 1.1 Identificar parâmetros que afetam o desempenho de uma rede local, considerando a sua arquitetura e tecnologia de suporte.

CA 1.2 Enumerar ferramentas de hardware e software utilizadas na monitorização de redes locais, destacando as suas especificações técnicas.

CA 1.3 Explicar as funções e propriedades das ferramentas de gestão utilizadas para obtenção de informação de tráfego, deteção de incidentes e isolamento de falhas, conforme as suas especificações.

CA 1.4 Comparar diferentes abordagens e metodologias de monitorização de redes locais, destacando vantagens e desvantagens com base nas necessidades específicas de desempenho e segurança da rede.

RA2: Aplicar técnicas de monitorização e manutenção de redes locais, utilizando ferramentas apropriadas para diagnóstico e resolução de incidentes.

CA 2.1. Instalar e configurar ferramentas de monitorização para garantir uma plataforma de gestão unificada da rede local.

CA 2.2. Analisar registos de atividade e logs da rede, utilizando ferramentas adequadas para identificar erros e falhas.

CA 2.3. Implementar soluções de manutenção corretiva e preventiva, substituindo ou reconfigurando dispositivos de rede defeituosos.

CA 2.4. Documentar ações de manutenção, incluindo diagnósticos e soluções adotadas, utilizando um modelo estruturado de registo de incidentes.

RA3: Demonstrar responsabilidade e organização na execução da monitorização e manutenção de redes locais, respeitando normas e boas práticas.

CA 3.1 Cumprir normas e regulamentos internos ao realizar a monitorização e manutenção da rede, assegurando conformidade e segurança.

CA 3.2 Trabalhar de forma colaborativa, respeitando colegas e procedimentos organizacionais durante a análise e resolução de incidentes.

CA 3.3 Garantir a rastreabilidade e integridade dos processos de manutenção, mantendo registos detalhados das intervenções realizadas.

RA4: Avaliar o desempenho da rede local e implementar otimizações para garantir a sua eficiência e continuidade.

CA 4.1. Realizar testes de desempenho em diferentes segmentos da rede local para identificar gargalos de tráfego e problemas de latência.

CA 4.2. Aplicar métodos de otimização, como a redistribuição de tráfego, ajuste de configurações de QoS (Quality of Service) e balanceamento de carga, para melhorar a performance da rede.

CA 4.3. Analisar e comparar os resultados dos testes de desempenho, documentando as melhorias implementadas e os impactos observados no desempenho da rede.

CA 4.4. Identificar e implementar soluções para a resolução de problemas de congestionamento e interferências na rede, utilizando técnicas de segmentação de rede e ajustes de parâmetros de configuração para otimizar a utilização da largura de banda.

RA5: Garantir a continuidade operacional da rede local através da implementação de planos de recuperação e redundância.

CA 5.1 Desenvolver e implementar planos de contingência e recuperação de desastres para a rede local, incluindo backups de configurações e procedimentos de restauração.

CA 5.2 Configurar soluções de redundância para equipamentos e enlaces críticos da rede, como dispositivos de failover e protocolos de redundância de roteamento (ex: HSRP, VRRP).

CA 5.3 Testar e validar os planos de recuperação e redundância, simulando falhas e verificando a eficácia das soluções implementadas.

CA 5.4 Documentar os procedimentos de recuperação de falhas, garantindo que os planos sejam acessíveis e compreensíveis para todos os envolvidos na manutenção da rede.

Conteúdos

1. Monitorização de Redes Locais

1.1. Conceitos fundamentais de monitorização de redes.

1.1.1. Definição de monitorização de redes locais.

1.1.2. Objetivos e importância da monitorização contínua.

1.1.3. Tipos de monitorização: ativa, passiva e em tempo real.

1.2. Parâmetros de desempenho de redes locais.

1.2.1. Latência, largura de banda e utilização de recursos.

1.2.2. Taxa de erro de pacotes e taxa de perda de pacotes.

1.2.3. Indicadores de saúde da rede.

1.2.4. Parâmetros críticos para redes com alta disponibilidade.

1.3. Ferramentas e técnicas de monitorização.

1.3.1. Ferramentas de hardware e software para monitorização.

1.3.2. Técnicas de captura e análise de tráfego de rede.

1.4. Procedimentos para monitorizar o tráfego de rede.

1.5. Notificações de alarme e identificação de incidentes.

1.5.1. Classificação dos alertas e sua origem.

1.5.2. Métodos de interpretação dos alertas.

2. Manutenção de redes locais

2.1. Tipos de manutenção: preventiva, preditiva e corretiva.

2.1.1. Manutenção preventiva: inspeções regulares, atualizações de segurança.

2.1.2. Manutenção preditiva: análise de tendências de falhas, utilização de algoritmos de previsão.

2.1.3. Manutenção corretiva: resposta a falhas inesperadas, resolução de incidentes críticos.

2.2. Diagnóstico e resolução de problemas em redes locais.

2.2.1. Identificação de falhas e anomalias.

2.2.2. Métodos de análise e testes de conectividade.

2.2.3. Diagnóstico e resolução de problemas em redes locais.

2.3. Ferramentas de suporte para manutenção.

2.3.1. Identificação de falhas e anomalias.

2.3.2. Métodos de análise e testes de conectividade.

2.4. Procedimentos de documentação e rastreamento de falhas.

2.4.1. Histórico de incidentes e avarias.

2.4.2. Relatórios de intervenção técnica.

3. Atualização de dispositivos de comunicação

3.1. Componentes de hardware e software atualizáveis.

3.1.1. Tipos de dispositivos de rede que exigem atualizações: switches, routers, servidores.

3.1.2. Requisitos de hardware e software para atualizações eficientes.

3.2. Compatibilidade e requisitos técnicos para atualização.

3.2.1. Considerações sobre a compatibilidade entre hardware e firmware.

3.2.2. Análise de impacto na rede e compatibilidade com os dispositivos existentes.

3.3. Procedimentos para atualização de software e firmware.

3.3.1. Métodos de backup e recuperação antes da atualização.

3.3.2. Atualização de firmware via fabricante.

3.3.3. Testes e validação pós-atualização.

Outras Capacidades Associadas à Unidade Formativa

- Assumir a responsabilidade pelo trabalho que realiza e por atingir os seus objetivos.
- Concluir o trabalho de acordo com critérios de adequação, economia e eficácia.
- Adaptar-se a novas situações ou contextos.

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

RA1: Explicar os princípios da segurança física e lógica em redes locais, diferenciando mecanismos de proteção e resposta a incidentes.

- **CA 1.1.** Descrever as funções de segurança física e lógica em ferramentas de gestão de redes, conforme especificações da tecnologia adotada.
- **CA 1.2.** Identificar alertas de segurança relacionados com acessos não autorizados, classificando-os de acordo com sua origem e impacto.
- **CA 1.3.** Explicar os mecanismos de rastreamento e auditoria utilizados para garantir a integridade e a rastreabilidade dos dados na rede.
- **CA 1.4.** Comparar diferentes métodos e ferramentas de segurança física e lógica, analisando a sua eficácia em proteger os dados e recursos da rede, considerando o contexto e as necessidades de segurança da organização.

RA2: Aplicar medidas de segurança para proteger dispositivos e dados em redes locais, identificando vulnerabilidades e mitigando riscos.

- **CA 2.5.** Implementar controles de segurança física nos equipamentos de rede, garantindo proteção contra acessos não autorizados.
- **CA 2.6.** Configurar soluções de autenticação e controlo de acessos, assegurando que apenas utilizadores autorizados tenham permissões adequadas.
- **CA 2.7.** Monitorizar eventos de segurança e responder a incidentes, utilizando ferramentas específicas para deteção e mitigação de ameaças.
- **CA 2.8.** Atualizar e reforçar configurações de segurança em dispositivos de comunicação, mitigando vulnerabilidades identificadas.

RA3: Demonstrar comprometimento com a segurança da informação e a proteção de dados, respeitando políticas e normas organizacionais.

- **CA 3.4.** Cumprir regulamentos de segurança da informação, garantindo confidencialidade, integridade e disponibilidade dos dados da rede.
- **CA 3.5.** Aplicar o princípio da igualdade de tratamento e não discriminação no controlo de acessos e na gestão de segurança da rede.
- **CA 3.6.** Demonstrar proatividade na identificação e mitigação de riscos de segurança, garantindo um ambiente seguro para os utilizadores.

RA4: Avaliar a eficácia das medidas de segurança implementadas em redes locais, utilizando ferramentas de auditoria e testes de penetração.

- **CA 4.5.** Realizar auditorias de segurança para avaliar a eficácia das medidas de proteção física e lógica na rede local.
- **CA 4.6.** Identificar vulnerabilidades e pontos críticos de segurança através de testes de penetração e análise de risco.
- **CA 4.7.** Documentar os resultados das auditorias e testes de penetração, propondo soluções para mitigar os riscos identificados.

RA5: Garantir a continuidade da segurança em redes locais, implementando soluções de backup e recuperação de dados.

- **CA 5.1.** Configurar e testar soluções de backup para dados críticos da rede, garantindo a disponibilidade e integridade da informação.
- **CA 5.2.** Implementar planos de recuperação de desastres e continuidade de negócios, assegurando a proteção da rede contra falhas críticas.
- **CA 5.3.** Monitorizar e validar regularmente as soluções de backup e recuperação, garantindo que estão a funcionar de acordo com os requisitos de segurança.

CA 5.4. Realizar testes de recuperação de dados simulando falhas críticas, avaliando a eficácia dos planos de recuperação e o tempo necessário para restaurar os serviços da rede à sua operação normal.

Conteúdos

1. Segurança lógica em redes locais

1.1. Conceitos fundamentais de segurança lógica.

1.1.1. Importância da segurança lógica em redes locais.

1.1.2. Ameaças cibernéticas e vulnerabilidades comuns em redes locais.

1.2. Controlo de acesso e autenticação.

1.2.1. Métodos de autenticação: Senhas, biometria, autenticação multifator.

1.2.2. Políticas de controle de acesso: Privilégios de utilizador, listas de controlo de acesso (ACLs).

1.2.3. Sistemas de autorização e gestão de permissões.

1.3. Ferramentas para segurança lógica.

1.3.1. Métodos de autenticação: Senhas, biometria, autenticação multifator.

1.3.2. Políticas de controle de acesso: Privilégios de utilizador, listas de controlo de acesso (ACLs).

1.3.3. Sistemas de autorização e gestão de permissões.

1.4. Rastreabilidade e auditoria de redes.

1.4.1. Monitorização de Acessos e Eventos: Ferramentas de log e análise de tráfego.

1.4.2. Análise de Logs e Ficheiros de Auditoria.

2. Segurança física em redes locais

2.1. Conceitos de segurança física em redes

2.1.1. Importância da segurança física para a proteção de infraestruturas de TI.

2.1.2. Ameaças físicas a dispositivos e equipamentos de rede.

2.2. Proteção de infraestruturas de redes.

2.2.1. Normas e Boas Práticas de Segurança Física: ISO 27001, NIST.

2.2.2. Controle de acesso a equipamentos críticos: Áreas restritas, biometria, controlo de entradas

2.2.3. Proteção contra acesso físico não autorizado: Sistemas de alarme, vigilância, barreiras físicas.

2.3. Medidas de mitigação contra falhas físicas e ambientais.

2.3.1. Sistemas de Climatização e Proteção Elétrica.

2.3.2. Estratégias de redundância para continuidade operacional: Fontes de alimentação ininterrupta (UPS), sistemas de backup de energia

2.3.3. Proteção contra desastres naturais e ambientais: Sensores de ambiente, localização estratégica de servidores

3. Gestão de incidentes e resposta a alertas

3.1. Identificação e classificação de incidentes de segurança.

3.1.1. Tipos de incidentes: Tentativas de intrusão, falhas de segurança, incidentes físicos.

3.1.2. Classificação de incidentes: Baixo, médio e alto impacto.

3.2. Procedimentos de resposta a alertas de segurança

3.2.1. Métodos de Isolamento e Mitigação de Ameaças: Segmentação de rede, desconexão de dispositivos comprometidos.

3.2.2. Técnicas de contenção e recuperação: Reversão de alterações e restaurar sistemas de backups seguros.

3.3. Documentação e rastreabilidade de ações corretivas.

3.3.1. Procedimentos de documentação de incidentes: Registro detalhado das ações e decisões tomadas.

3.3.2. Relatórios pós-incidente: Análise de causa raiz, lições aprendidas, recomendações de melhoria

4. Continuidade e recuperação de dados

4.1. Backup e recuperação de dados críticos.

4.1.1. Definição de dados críticos e importância do backup.

4.1.2. Soluções de backup: Local, remoto e na nuvem.

4.1.3. Verificação da integridade e confiabilidade dos backups.

4.2. Planos de recuperação de desastres (DRP).

4.2.1. Elaboração de planos de recuperação: Planejamento para cenários de falhas físicas e lógicas

4.2.2. Testes de planos de recuperação: Simulações de falhas e validação das estratégias

Outras Capacidades Associadas à Unidade Formativa

- Respeitar os procedimentos e as regras internas da organização.
- Demonstrar uma atitude de respeito pelos colegas, procedimentos e regras da empresa.
- Implementar eficazmente o princípio da igualdade de tratamento e da não discriminação nas condições de trabalho entre mulheres e homens.

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: Instalação, Monitorização e Gestão de Interligações de Redes Locais e Públicas		
Código: MF370_3	Nível: 3	Duração: 160 Horas
Associado à UC370_3: Implementar soluções de interligação entre redes privadas e públicas de forma eficiente..		

Este MF é subdividido nas seguintes Unidades Formativas: caso necessário

		Código
Unidade Formativa 1:	Gestão de Desempenho e Solução de Incidentes em Redes.	UF474
Unidade Formativa 2:	Instalação e Configuração de Dispositivos de Interligaçao entre redes locais e públicas	UF475

Unidade Formativa 1: Gestão de Desempenho e Solução de Incidentes em Redes. (UF474)

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

RA1: Identificar os parâmetros e critérios de desempenho em redes locais e públicas, explicando como avaliar e melhorar a qualidade do serviço (QoS) nas redes.

- **CA 1.1.** Identificar os parâmetros críticos de desempenho, como largura de banda, latência e disponibilidade, explicando o seu impacto no funcionamento da rede com base em especificações técnicas.
- **CA 1.2.** Descrever os principais indicadores de desempenho (KPIs) para avaliar a qualidade do serviço (QoS) em redes locais e públicas, conforme parâmetros operacionais definidos.
- **CA 1.3.** Explicar a relação entre os serviços oferecidos e os parâmetros de desempenho da rede, discutindo como a monitorização de rede pode garantir a qualidade do serviço, dentro dos parâmetros operacionais.
- **CA 1.4.** Comparar diferentes abordagens e técnicas de melhoria de QoS, como priorização de tráfego, controle de congestionamento e técnicas de gestão de largura de banda, explicando como cada uma impacta a qualidade do serviço em redes locais e públicas, com base nas necessidades operacionais.

RA2: Aplicar procedimentos de monitorização e gestão de desempenho em redes locais e públicas, utilizando ferramentas adequadas para a deteção de problemas de desempenho.

- **CA 2.1.** Utilizar ferramentas de monitorização de rede para identificar e registar métricas de desempenho, como tempo de resposta e utilização da largura de banda dentro dos parâmetros definidos.
- **CA 2.2.** Aplicar procedimentos para configurar e ajustar parâmetros de desempenho em dispositivos de rede, como switches e routers, com base nas necessidades da rede.
- **CA 2.3.** Executar testes de carga e análise de tráfego para avaliar o impacto de diferentes configurações de rede no desempenho, com base nos dados obtidos.
- **CA 2.4.** Realizar ajustes nas configurações da rede para otimizar o desempenho, com base nos resultados da monitorização e testes realizados, garantindo a continuidade do serviço.

RA3: Demonstrar um compromisso com a melhoria contínua da rede, realizando análises periódicas e aplicando boas práticas de gestão de desempenho.

- **CA 3.1.** Implementar práticas de monitorização contínua e revisão periódica das configurações de rede para garantir a manutenção do desempenho ideal.
- **CA 3.2.** Demonstrar iniciativa na identificação de oportunidades de melhoria na rede, propondo soluções para otimizar a performance com base nos testes de desempenho.
- **CA 3.3.** Cumprir regulamentos e políticas de gestão de desempenho, assegurando a integridade, a disponibilidade e a qualidade da rede.

RA4: Identificar as principais causas de incidentes de desempenho em redes locais e públicas, explicando as suas origens e impactos no funcionamento da rede.

CA 4.5. Identificar as causas mais comuns de incidentes que afetam o desempenho da rede, como congestionamento, falhas de hardware ou configuração inadequada.

CA 4.6. Descrever como a sobrecarga de tráfego, falhas de dispositivos ou ataques cibernéticos podem impactar negativamente o desempenho da rede, afetando a qualidade do serviço.

CA 4.7. Explicar a importância da análise de logs e métricas para detetar incidentes e avaliar o impacto no desempenho da rede.

RA5: Aplicar procedimentos de diagnóstico e resolução de incidentes em redes locais e públicas, garantindo a recuperação do desempenho ideal da rede.

CA 5.1. Utilizar ferramentas de diagnóstico para identificar e isolar incidentes que afetam o desempenho da rede, como falhas de equipamentos ou interrupções de serviços, dentro dos processos operacionais.

CA 5.2. Implementar soluções corretivas para restaurar a normalidade do desempenho da rede, como reconfiguração de dispositivos, substituição de componentes ou ajuste de parâmetros, conforme as necessidades de serviço.

CA 5.3. Realizar testes pós-correção para garantir que os incidentes foram resolvidos e que o desempenho da rede foi restaurado aos níveis esperados, dentro dos parâmetros de desempenho.

CA 5.4. Documentar os incidentes e as ações corretivas tomadas, criando relatórios técnicos para futuras referências e melhoria contínua da gestão de desempenho.

RA6: Implementar soluções para garantir a continuidade do serviço e gestão de incidências.

CA6.1 Identificar e diagnosticar falhas na interligação de redes, utilizando ferramentas adequadas como Wireshark, Nagios e Zabbix.

CA6.2 Aplicar soluções corretivas e preventivas para otimizar o desempenho e minimizar interrupções na comunicação.

CA6.3 Utilizar sistemas de monitorização para prever e mitigar possíveis falhas na interligação das redes.

RA7: Aplicar políticas de segurança para interligação segura entre redes privadas e públicas.

CA7.1 Implementar regras de firewall e sistemas de prevenção de intrusão (IPS) para mitigar riscos de segurança, conforme as melhores práticas de segurança.

CA7.2 Aplicar mecanismos de tunelamento seguro, como VPNs e TLS, para garantir a proteção dos dados em trânsito, de acordo com os requisitos de segurança da rede.

CA7.3 Realizar auditorias de segurança para verificar a conformidade com normas e boas práticas, com base em políticas de segurança definidas.

CA7.4 Identificar vulnerabilidades e propor medidas corretivas para mitigar ameaças de segurança, com base nas análises periódicas da infraestrutura de rede.

Conteúdos

1. Fundamentos da interligação de redes e desempenho

1.1. Arquitetura e funcionamento de dispositivos de interligação (routers, switches, gateways, etc.).

1.2. Interfaces e classificações dos dispositivos de interligação.

1.3. Serviços de interligação de redes: características, funcionalidades e impacto no desempenho.

1.4. Conceitos de Qualidade de Serviço (QoS): parâmetros críticos (largura de banda, latência, jitter, perda de pacotes).

2. Protocolos de comunicação e encaminhamento

2.1. Modelo OSI e pilha de protocolos TCP/IP.

2.2. Protocolos de encaminhamento: conceitos de roteamento dinâmico e estático.

2.3. Algoritmos de encaminhamento (RIP, OSPF, EIGRP, BGP) e a sua influência no desempenho da rede.

2.4. Redes Privadas Virtuais (VPN): implementação e impacto no desempenho da rede.

2.5. Segurança na interligação de redes: filtragem de pacotes, NAT, redireccionamento de portas e criptografia.

3. Monitorização e gestão de desempenho de redes

3.1. Conceitos de gestão e monitorização de redes: SNMP, NetFlow, sFlow.

3.2. Ferramentas de monitorização (Wireshark, Nagios, PRTG, Zabbix).

3.3. Análise de tráfego e identificação de gargalos de desempenho.

3.4. Indicadores de desempenho (KPIs) e sua interpretação.

3.5. Métodos de otimização de redes para garantir a qualidade de serviço.

4. Diagnóstico e resolução de problemas de desempenho

4.1. Identificação das principais causas de incidentes de desempenho (congestionamento, falhas de hardware, configuração inadequada).

4.2. Técnicas de diagnóstico: análise de logs, testes de conectividade (ping, traceroute, MTR), deteção de falhas.

4.3. Procedimentos sistemáticos para resolução de problemas: ITIL, boas práticas de troubleshooting.

4.4. Testes pós-correção para garantir a restauração da performance da rede.

4.5. Documentação e relatório de incidentes: boas práticas e padrões.

Outras Capacidades Associadas à Unidade Formativa

Unidade Formativa 2: Instalação e Configuração de Dispositivos de Interligação entre redes locais e públicas (UF475)

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

RA1: Identificar e descrever os dispositivos de interligação entre redes locais e públicas, explicando suas funções, características e requisitos de instalação.

CA 1.1. Identificar corretamente os dispositivos e componentes adequados para a interligação de redes privadas e públicas, tendo em conta requisitos de desempenho e segurança.

CA 1.2. Descrever as tecnologias e arquiteturas de comunicação utilizadas na interligação entre redes, destacando os padrões e protocolos envolvidos.

CA 1.3. Explicar os tipos de interfaces presentes nos dispositivos de interligação e suas funções, considerando o tipo de rede a ser interligado.

CA 1.4. Comparar os diferentes tipos de dispositivos de interligação, como roteadores, switches e firewalls, explicando as suas funções específicas na gestão de tráfego e segurança entre redes locais e públicas.

RA2: Aplicar procedimentos de instalação e configuração de dispositivos de interligação entre redes locais e públicas, garantindo a sua funcionalidade de acordo com especificações técnicas.

CA 2.1. Realizar corretamente a instalação física dos dispositivos de interligação de acordo com as especificações técnicas, assegurando a integridade e segurança dos dispositivos.

CA 2.2. Efetuar a configuração inicial dos dispositivos de interligação, assegurando a comunicação entre redes privadas e públicas, conforme as especificações do fabricante.

CA 2.3. Testar a conectividade entre os dispositivos de interligação e resolver problemas identificados, aplicando procedimentos de diagnóstico conforme as especificações técnicas.

CA 2.4. Documentar o processo de instalação e configuração, gerando relatórios técnicos que descrevem os dispositivos instalados e os parâmetros configurados, conforme os padrões definidos.

RA3: Demonstrar responsabilidade na instalação e configuração de dispositivos de interligação, seguindo as melhores práticas de segurança e garantindo o funcionamento adequado das redes.

CA 3.1. Cumprir as normas de segurança aplicáveis durante a instalação de dispositivos de interligação, assegurando a proteção física e lógica dos equipamentos.

CA 3.2. Demonstrar proatividade na resolução de problemas durante a instalação e configuração, antecipando necessidades de ajustes para garantir a continuidade do serviço.

CA 3.3. Garantir que as configurações de segurança, como firewalls e criptografia, sejam aplicadas de acordo com as normas de segurança e as especificações do cliente.

RA4: Identificar e descrever os protocolos de comunicação utilizados na interligação de redes locais e públicas, explicando suas funções e aplicações em diferentes tipos de rede.

CA 4.1. Identificar os protocolos de comunicação utilizados na interligação entre redes locais e públicas, explicando suas funções e compatibilidade com os dispositivos de interligação, conforme as especificações operacionais.

CA 4.2. Descrever as funções dos principais protocolos de interligação, como TCP/IP, VPN, OSPF, RIP, entre outros, e explicar como eles são aplicados na comunicação entre redes, dentro do contexto técnico.

CA 4.3. Explicar os processos de encapsulamento e roteamento de pacotes nos protocolos de interligação, destacando as etapas envolvidas na troca de informações entre redes privadas e públicas, conforme os requisitos da arquitetura de rede.

RA5: Aplicar procedimentos de verificação e otimização dos dispositivos de interligação entre redes locais e públicas, garantindo a eficiência da comunicação e a continuidade do serviço.

CA 5.1. Verificar a configuração de dispositivos de interligação após a instalação, utilizando ferramentas de teste para validar os parâmetros de rede e a conectividade entre as redes locais e públicas, conforme as necessidades operacionais.

CA 5.2. Aplicar técnicas de diagnóstico para identificar e corrigir problemas de conectividade ou desempenho em dispositivos de interligação entre redes, com base nos parâmetros de rede e nos relatórios de teste.

CA 5.3. Implementar melhorias na configuração dos dispositivos de interligação, ajustando os parâmetros de rede para otimizar o desempenho, a segurança e a continuidade do serviço, conforme a avaliação dos testes realizados.

CA 5.4. Gerar relatórios de desempenho e diagnóstico, detalhando os ajustes realizados e a eficácia das melhorias aplicadas, para garantir a rastreabilidade das ações de otimização e conformidade com os parâmetros definidos.

RA6: Configurar protocolos de comunicação para a interligação eficiente entre redes privadas e públicas.

CA6.1 Aplica corretamente a configuração de protocolos de encaminhamento, como OSPF, BGP e EIGRP, assegurando a interligação eficiente das redes.

CA6.2 Implementa endereçamento IP adequado, incluindo sub-redes, NAT e VLANs, garantindo uma comunicação eficiente e segura.

CA6.3 Testa e valida a configuração dos protocolos, garantindo a continuidade do serviço.

Conteúdos

1. **Arquitetura, funcionalidades e tecnologias dos dispositivos de interligação**
   - **1.1.** Estrutura e componentes dos dispositivos de interligação de redes (routers, switches, firewalls, gateways).
   - **1.2.** Requisitos físicos e elétricos para a instalação de dispositivos de interligação.

1.3. Tecnologias de interligação de redes:

1.3.1. IPv4 vs. IPv6 e suas implicações na interligação.

1.3.2. NAT (Network Address Translation) e PAT (Port Address Translation).

1.3.3. VLANs e segmentação de redes.

1.3.4. SD-WAN e outras tecnologias emergentes.

2. Procedimentos de instalação e configuração de dispositivos de interligação

2.1. Normas e boas práticas de segurança física e elétrica na instalação de dispositivos de rede.

2.2. Métodos de configuração inicial:

2.2.1. Interface de linha de comandos (CLI) e interfaces gráficas (GUI).

2.2.2. Carregamento e backup de configurações.

2.3. Configuração de interfaces de rede e endereçamento IP:

2.3.1. Endereçamento IPv4 e IPv6, máscaras de sub-rede e gateways padrão.

2.3.2. Atribuição manual vs. DHCP.

2.4. Configuração básica de serviços essenciais:

2.4.1. Tabelas de roteamento estático e dinâmico.

2.4.2. Configuração de NAT e VLANs.

3. Monitorização e testes de conectividade dos dispositivos de interligação

3.1. Ferramentas de monitorização e diagnóstico:

3.1.1. Comandos básicos de testes de conectividade (ping, traceroute, nslookup).

3.1.2. Ferramentas SNMP, NetFlow e Syslog para monitorização de desempenho.

3.2. Testes de conectividade e desempenho:

3.2.1. Testes de largura de banda e latência.

3.2.2. Verificação de estabilidade e confiabilidade da conexão.

3.2.3. Identificação e resolução de falhas de conectividade.

4. Protocolos e parâmetros de configuração para interligação de redes

4.1. Protocolos de comunicação e encaminhamento de tráfego:

4.1.1. Roteamento dinâmico (RIP, OSPF, BGP).

4.1.2. Protocolos de tunelamento e segurança (IPSec, GRE, VPNs).

4.2. Configuração avançada de NAT e VLANs:

4.2.1. NAT estático e dinâmico, PAT e suas aplicações.

4.2.2. Configuração de VLANs e trunking para segmentação de tráfego.

4.3. Parâmetros essenciais para comunicação eficiente:

4.3.1. Ajustes de MTU e fragmentação de pacotes.

4.3.2. QoS (Qualidade de Serviço) para priorização de tráfego crítico.

Outras Capacidades Associadas à Unidade Formativa

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: Gestão Avançada e Otimização de Redes Locais		
Código: MF371_3	Nível: 3	Duração: 60 Horas
Associado à UC371_3: Monitorizar e diagnosticar redes locais para garantia de desempenho e continuidade do serviço.		

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

RA1: Compreender os princípios e metodologias de monitorização e diagnóstico de redes locais

CA 1.1. Explicar os conceitos fundamentais de monitorização e diagnóstico de redes locais, incluindo métricas de desempenho, protocolos de monitorização e análise de tráfego.

CA 1.2. Identificar e descrever ferramentas e técnicas utilizadas para monitorizar redes locais, considerando diferentes cenários de aplicação.

CA 1.3. Explicar a importância da monitorização contínua para a otimização do desempenho e a garantia da continuidade dos serviços de rede.

RA2: Configurar e utilizar ferramentas de monitorização de redes locais para deteção e resolução de falhas

CA 2.1. Instalar e configurar ferramentas de monitorização de redes locais, assegurando a correta parametrização de sensores, alarmes e relatórios.

CA 2.2. Monitorizar a rede local em tempo real, utilizando ferramentas apropriadas para detetar falhas de conectividade, degradação de desempenho e vulnerabilidades.

CA 2.3. Analisar registos de eventos e alertas gerados pelas ferramentas de monitorização, diagnosticando problemas e propondo soluções adequadas.

CA 2.4. Aplicar técnicas de filtragem e análise avançada de dados provenientes das ferramentas de monitorização para identificar padrões e tendências de falhas recorren60+tes, propondo melhorias preventivas.

RA3: Diagnosticar falhas e implementar soluções corretivas e preventivas para garantir a continuidade dos serviços de rede

CA 3.1. Realizar testes de desempenho da rede, como latência, largura de banda, perda de pacotes e jitter, para verificar a conformidade com os parâmetros estabelecidos.

CA 3.2. Aplicar metodologias de resolução de falhas, incluindo reconfiguração de equipamentos, substituição de componentes e ajustes de parâmetros de rede.

CA 3.3. Documentar o processo de diagnóstico e resolução de falhas, assegurando a rastreabilidade e melhoria contínua dos procedimentos de gestão da rede.

CA 3.4. Implementar soluções preventivas baseadas na análise de falhas anteriores, como atualizações de firmware, ajustes de configuração e políticas de redundância, para evitar a recorrência de problemas semelhantes.

RA4: Assegurar boas práticas na gestão e manutenção da rede local, garantindo a fiabilidade e segurança dos serviços

CA 4.1. Seguir protocolos e normas de boas práticas na monitorização e manutenção da rede local, garantindo a conformidade com padrões técnicos e regulatórios.

CA 4.2. Demonstrar proatividade na identificação e resolução de problemas de rede, antecipando possíveis falhas e implementando medidas preventivas.

CA 4.3. Promover a atualização contínua de software, firmware e configurações de segurança, minimizando riscos e garantindo a estabilidade dos serviços.

RA5: Compreender e aplicar metodologias avançadas de gestão de redes locais para otimização de desempenho e segurança

CA 5.1. Explicar os princípios da gestão avançada de redes locais, incluindo QoS (Qualidade de Serviço), VLANs, segmentação de rede e políticas de segurança.

CA 5.2. Analisar métricas de desempenho e indicadores-chave (KPIs) para avaliar a eficiência e fiabilidade da rede local.

CA 5.3. Identificar e aplicar estratégias para minimizar congestionamentos e garantir a escalabilidade da rede.

RA6: Implementar políticas de segurança e gestão de tráfego para garantir a resiliência da rede local

CA 6.1. Configurar e gerir VLANs, listas de controlo de acesso (ACLs) e políticas de QoS para otimizar a utilização de recursos de rede.

CA 6.2. Implementar mecanismos de redundância, como protocolos de failover (HSRP, VRRP) e balanceamento de carga, garantindo a continuidade dos serviços.

CA 6.3. Aplicar medidas de segurança avançadas, como segmentação de rede, encriptação e controlo de acessos, para minimizar vulnerabilidades e ataques cibernéticos.

RA7: Adotar uma abordagem proativa e estratégica na gestão e otimização de redes locais

CA7.1 Demonstrar iniciativa na identificação de oportunidades de melhoria no desempenho e segurança da rede local.

CA7.2 Implementar práticas de gestão preventiva, antecipando possíveis falhas e assegurando a continuidade operacional da rede.

CA7.3 Colaborar eficazmente com equipas técnicas e utilizadores, garantindo uma comunicação clara e eficiente na gestão de redes locais.

Conteúdos

1. Fundamentos da monitorização e diagnóstico de redes locais

1.1. Conceitos fundamentais de monitorização e diagnóstico de redes.

1.2. Métricas de desempenho (latência, largura de banda, jitter, perda de pacotes).

1.3. Protocolos de monitorização (SNMP, NetFlow, ICMP, Syslog).

1.4. Ferramentas de análise de tráfego (Wireshark, PRTG, Nagios, Zabbix).

1.5. Importância da monitorização contínua para a estabilidade da rede.

1.6. Integração de ferramentas de monitorização (ex: Wireshark + Nagios + Zabbix).

2. Ferramentas e técnicas para monitorização de redes locais

2.1. Instalação e configuração de ferramentas de monitorização.

2.2. Parametrização de sensores, alarmes e relatórios.

2.3. Monitorização de redes em tempo real e deteção de falhas.

2.4. Análise de eventos e alertas gerados por ferramentas de monitorização.

2.5. Diagnóstico de problemas e propostas de solução.

2.6. Automatização de monitorização: Configuração de alertas automáticos para falhas ou anomalias com base nas métricas de desempenho (como latência ou perda de pacotes).

3. Diagnóstico e Resolução de Falhas em Redes Locais

3.1. Testes de desempenho e sua interpretação.

3.2. Métodos de resolução de falhas (reconfiguração, substituição de componentes, otimização de parâmetros).

3.3. Documentação de diagnósticos e soluções implementadas.

3.4. Gestão de registos de falhas e histórico de ocorrências.

3.5. Análise de falhas utilizando Syslog e SNMP.

3.6. Técnicas de troubleshooting com múltiplas camadas

3.6.1. Metodologias para diagnosticar problemas complexos que envolvem tanto a camada física da rede (cabos, switches) quanto as camadas mais altas (protocolos e desempenho de aplicações).

4. Gestão avançada de redes locais

4.1. Conceitos avançados de QoS, VLANs e segmentação de rede

4.2. Políticas de segurança e isolamento de tráfego

4.3. Indicadores-chave de desempenho (KPIs) para redes locais

4.4. Estratégias para minimizar congestionamentos e aumentar a escalabilidade

4.5. Estratégias de segmentação de rede para otimizar a segurança.

5. Implementação de políticas de segurança e gestão de tráfego

5.1. Configuração de VLANs e listas de controlo de acesso (ACLs)

5.2. Gestão de políticas de QoS para otimização do tráfego de rede

5.3. Implementação de redundância (failover, VRRP, HSRP) e balanceamento de carga

5.4. Medidas de segurança avançadas: encriptação, segmentação de rede e controlo de acessos

5.5. Implementação de Firewalls e Segmentação Avançada:

5.5.1. Configurar firewalls de rede para controlar e segmentar o tráfego de dados, reforçando a segurança da rede interna.

5.6. Gestão de tráfego com SDN: Introdução às redes definidas por software (SDN) e como elas podem ser utilizadas para otimizar a gestão do tráfego de dados e melhorar a flexibilidade da rede.

6. Estratégias proativas na gestão de redes locais

6.1. Identificação de oportunidades de melhoria na rede

6.2. Práticas de gestão preventiva e antecipação de falhas

6.3. Comunicação eficaz entre equipas técnicas e utilizadores

6.4. Planeamento estratégico para a resiliência da infraestrutura de rede

6.5. Plano de contingência para falhas de rede:

6.5.1. Desenvolvimento e implementação de um plano de contingência, incluindo a criação de backups e a definição de procedimentos de recuperação após falhas (ex: utilização de redundância e failover).

6.6. Cálculo da disponibilidade da rede:

6.6.1. Determinação do tempo de inatividade da rede e métodos para melhorar a disponibilidade, utilizando medidas como SLAs (Acordos de Nível de Serviço).

7. Boas práticas na gestão e manutenção de redes locais

7.1. Normas e protocolos técnicos de monitorização e manutenção

7.2. Conformidade com padrões regulatórios e de segurança

7.3. Proatividade na deteção e resolução de problemas

7.4. Atualização contínua de software, firmware e configurações de segurança

7.5. Estratégias de prevenção de falhas e gestão de riscos

7.6. Documentação técnica e de rede:

7.6.1. Criar e manter documentação atualizada sobre a infraestrutura de rede, incluindo diagramas de rede, configuração de dispositivos e políticas de segurança.

7.7. Processos de auditoria de rede.

8. **Gestão avançada da infraestrutura de rede**

8.1. Estratégias de melhoria contínua da infraestrutura de rede

8.2. Monitorização de desempenho contínuo para ajustes e melhorias

8.3. Planeamento de upgrades de rede

8.1.1. Análise e identificação de pontos críticos da infraestrutura para planear upgrades eficientes (ex: melhoria de switches, aumento de largura de banda, troca de cabeamento).

8.2. Avaliação contínua de desempenho.

8.3. Gestão da eficiência energética em redes locais: Introdução à otimização do consumo de energia nas infraestruturas de rede, considerando práticas e dispositivos que possam reduzir o consumo energético.

Outras Capacidades Associadas ao Módulo

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.

MÓDULO FORMATIVO EM CONTEXTO REAL DE TRABALHO	MT_TIC006
Nível: 4	Duração indicativa: 360 Horas
Associado a todas as Unidades de Competência	

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

RA1: Instalar e configurar dispositivos de comunicação em redes locais

CA 1.1. Enumerar e explicar os protocolos configuráveis em um nó de rede, considerando os padrões adotados, como TCP/IP, DHCP, DNS, e outros protocolos de comunicação.

CA 1.2. Configurar e instalar interfaces e módulos de equipamentos de rede, como switches, routers, e pontos de acesso, garantindo a sua conectividade e funcionalidade para um desempenho eficiente da rede local.

CA 1.3. Realizar a instalação física dos dispositivos em bastidores, verificando condições ambientais e elétricas adequadas, conforme os requisitos de segurança e desempenho.

CA 1.4. Preencher relatórios técnicos documentando a instalação e configuração realizada, incluindo a descrição de cada etapa do processo, decisões tomadas e verificação de funcionalidade.

RA2: Demonstrar responsabilidade e rigor na instalação de redes locais

CA 2.1. Cumprir normas de segurança durante a instalação dos dispositivos de rede, minimizando riscos físicos e elétricos, e garantindo a utilização correto de equipamentos de proteção individual (EPIs).

CA 2.2. Verificar a conformidade da instalação com as especificações técnicas, realizando testes e ajustes para assegurar a funcionalidade ideal e padrões de qualidade.

CA 2.3. Cooperar em equipe durante a instalação e configuração dos dispositivos, promovendo a troca de conhecimentos técnicos e a colaboração eficaz entre os membros da equipe para alcançar os objetivos de forma eficiente e segura.

RA3: Aplicar procedimentos de monitorização e gestão de desempenho em redes locais e públicas, utilizando ferramentas adequadas para a deteção de problemas de desempenho

CA 3.1. Utilizar ferramentas de monitorização de rede para identificar e registar métricas de desempenho, como tempo de resposta e utilização da largura de banda.

CA 3.2. Aplicar procedimentos para configurar e ajustar parâmetros de desempenho em dispositivos de rede, como switches e routers, com base nas necessidades da rede.

CA 3.3. Executar testes de carga e análise de tráfego para avaliar o impacto de diferentes configurações de rede no desempenho.

CA 3.4. Realizar ajustes nas configurações da rede para otimizar o desempenho, baseando-se nos resultados da monitorização e testes realizados.

RA4: Diagnosticar e resolver problemas em dispositivos de comunicação de redes locais

CA 4.1. Identificar problemas comuns em dispositivos de rede, como falhas de conectividade, problemas de configuração e erros de comunicação, utilizando ferramentas de diagnóstico apropriadas.

CA 4.2. Aplicar procedimentos de diagnóstico e ferramentas de rede, como testes de ping, tracert, e análise de logs, para identificar e localizar falhas nos dispositivos de comunicação.

CA 4.3. Resolver problemas de rede, corrigindo configurações e substituindo componentes defeituosos, garantindo o restabelecimento da conectividade e funcionalidade dos dispositivos de rede.

CA 4.4. Elaborar relatórios técnicos detalhados sobre os problemas encontrados, ações tomadas e soluções implementadas, proporcionando uma visão clara do processo de diagnóstico e resolução.

RA5: Compreender protocolos de comunicação e sua configuração em redes locais

CA 5.1. Identificar os principais protocolos de rede utilizados em redes locais e suas respectivas funções.

CA 5.2. Interpretar especificações técnicas para configuração de protocolos de comunicação em dispositivos de rede.

CA 5.3. Explicar os parâmetros de configuração de protocolos que afetam a segurança e desempenho da rede.

CA 5.4. Comparar diferentes protocolos de comunicação em termos de desempenho, escalabilidade e segurança, justificando a escolha mais adequada para diferentes cenários de redes locais.

RA6: Aplicar procedimentos de teste e verificação de conectividade em redes locais

CA 6.1. Utilizar ferramentas de verificação e monitoramento para testar a conectividade e desempenho dos dispositivos de rede.

CA 6.2. Configurar e testar protocolos de gestão remota, como SNMP e SSH, garantindo sua funcionalidade.

CA 6.3. Documentar os procedimentos de teste e verificação, assegurando a rastreabilidade das operações.

CA 6.4. Realizar testes de conectividade em diferentes camadas do modelo OSI, identificando possíveis falhas de rede e propondo soluções adequadas para cada camada.

RA7: Demonstrar proatividade e precisão na resolução de problemas de conectividade

CA 7.1. Diagnosticar e classificar incidentes de comunicação na rede local, utilizando ferramentas adequadas.

CA 7.2. Aplicar soluções corretivas para incidentes de rede, garantindo a continuidade dos serviços.

CA 7.3. Trabalhar de forma organizada e metódica na identificação e resolução de problemas de conectividade.

RA8: Explicar os fundamentos da monitorização de redes locais

CA 8.1. Identificar parâmetros que afetam o desempenho de uma rede local, considerando a sua arquitetura e tecnologia de suporte.

CA 8.2. Enumerar ferramentas de hardware e software utilizadas na monitorização de redes locais, destacando as suas especificações técnicas.

CA 8.3. Explicar as funções e propriedades das ferramentas de gestão utilizadas para obtenção de informação de tráfego, deteção de incidentes e isolamento de falhas, conforme suas especificações.

CA 8.4. Comparar diferentes abordagens e metodologias de monitorização de redes locais, destacando vantagens e desvantagens com base nas necessidades específicas de desempenho e segurança da rede.

RA9: Aplicar técnicas de monitorização e manutenção de redes locais

CA9.1: Instalar e configurar ferramentas de monitorização para garantir uma plataforma de gestão unificada da rede local.

CA9.2: Analisar registos de atividade e logs da rede, utilizando ferramentas adequadas para identificar erros e falhas.

CA9.3: Implementar soluções de manutenção corretiva e preventiva, substituindo ou reconfigurando dispositivos de rede defeituosos.

CA9.4: Documentar ações de manutenção, incluindo diagnósticos e soluções adotadas, utilizando um modelo estruturado de registo de incidentes.

RA10: Explicar os princípios da segurança física e lógica em redes locais

CA10.1: Descrever as funções de segurança física e lógica em ferramentas de gestão de redes, conforme especificações da tecnologia adotada.

CA10.2: Identificar alertas de segurança relacionados com acessos não autorizados, classificando-os de acordo com sua origem e impacto.

CA10.3: Explicar os mecanismos de rastreamento e auditoria utilizados para garantir a integridade e a rastreabilidade dos dados na rede.

CA10.4: Comparar diferentes métodos e ferramentas de segurança física e lógica, analisando sua eficácia em proteger os dados e recursos da rede, considerando o contexto e as necessidades de segurança da organização.

RA11: Aplicar medidas de segurança para proteger dispositivos e dados em redes locais

CA11.1: Implementar controles de segurança física nos equipamentos de rede, garantindo proteção contra acessos não autorizados.

CA11.2: Configurar soluções de autenticação e controlo de acessos, assegurando que apenas utilizadores autorizados tenham permissões adequadas.

CA11.3: Monitorizar eventos de segurança e responder a incidentes, utilizando ferramentas específicas para deteção e mitigação de ameaças.

CA11.4: Atualizar e reforçar configurações de segurança em dispositivos de comunicação, mitigando vulnerabilidades identificadas.

