

Programa da ação

Fundamentos Técnicos de Cibersegurança: Redes, Sistemas e Proteção de Infraestruturas

Percurso formativo em Cibersegurança — Ação 2 de 6 (sequência cumulativa de 300 horas).

Identificação	Caracterização
Área temática	Tecnologias de Informação e Comunicação / Cibersegurança Técnica
Duração total	50 horas
Modalidade	100% aulas síncronas online através do Microsoft Teams
Nível	Formação técnica de iniciação, com progressão prática supervisionada
Público-alvo	Adolescentes, jovens e adultos em iniciação técnica à cibersegurança, conforme as condições de acesso da candidatura.
Pré-requisitos	Ação 1 concluída ou conhecimentos equivalentes sobre ativos e riscos; não se exige experiência de administração de redes.

Descrição da formação

Esta ação introduz as bases técnicas necessárias para compreender e proteger uma infraestrutura digital simples. Os participantes identificam componentes de rede, interpretam protocolos essenciais, reconhecem serviços e permissões dos sistemas operativos, aplicam princípios de configuração segura, avaliam vulnerabilidades e interpretam registos elementares. O ensino usa laboratórios preparados e tarefas supervisionadas; não inclui exploração ofensiva de sistemas externos nem administração empresarial avançada.

Enquadramento e articulação no percurso de 300 horas

Segunda ação do percurso; substitui a duplicação do antigo Programa 2. Parte do inventário e dos riscos definidos na ação 1, sem voltar a ensinar a metodologia de gestão de risco. Produz um diagnóstico técnico a utilizar nas ações de acessos e fornecedores e de continuidade de serviços.

Objetivo geral

Capacitar os participantes para reconhecer a arquitetura de uma rede simples, verificar configurações básicas de segurança, identificar fragilidades técnicas e produzir um relatório de diagnóstico com medidas correctivas adequadas.

Objetivos específicos

No final da ação, cada formando deverá ser capaz de:

- Explicar funções de dispositivos, endereços IP, portas, DNS, HTTP/HTTPS e serviços essenciais numa rede simples.
- Interpretar um esquema de rede e relacionar equipamentos com os ativos do inventário.
- Identificar contas locais, permissões, serviços e actualizações nos sistemas operativos mais comuns.
- Explicar os princípios e os limites de firewalls, VPN e segmentação de redes.
- Aplicar listas de verificação de configuração segura e protecção de dispositivos em laboratório.
- Distinguir vulnerabilidade, exposição, alerta, evento e incidente sem efectuar exploração não autorizada.
- Interpretar registos simulados de autenticação, actualização e segurança, com reporte adequado.
- Priorizar correcções técnicas e comunicar limitações e resultados verificáveis.

Metodologia

A ação decorre integralmente em 20 sessões síncronas de 2 horas e 30 minutos, em Microsoft Teams. Cada um dos 10 módulos corresponde a 5 horas: 2 horas de explicação e demonstração e 3 horas de prática orientada e avaliação. Deste modo, as 50 horas incluem todos os exercícios, oficinas, apresentações, revisão e avaliação. Não existem horas assíncronas, trabalhos obrigatórios fora das sessões nem formação em contexto de trabalho (FCT).

O formador apresenta os conceitos de forma gradual, demonstra os procedimentos e acompanha tarefas individuais e em grupo. A execução utiliza uma organização fictícia comum às seis ações, designada Atlântico Serviços (nome fictício), com cerca de 30 trabalhadores, portal de clientes, ficheiros administrativos, serviços cloud, rede interna e fornecedores externos. Os dados, contas e registos são simulados; os laboratórios técnicos são isolados ou expressamente autorizados. Cada etapa produz evidências documentadas, e a sua avaliação individual não depende da dimensão do grupo.

As primeiras sessões começam com diagnóstico de competências sem classificação. O formador disponibiliza glossário, instruções, modelos e critérios antes das atividades. A complexidade aumenta através da aplicação dos conhecimentos anteriores a situações novas; quando um conceito transversal reaparece, é mobilizado como pré-requisito, sem nova aula de fundamentos.

Plano de aulas

Mód.	Aulas	Tema	Explic.	Prática	Total
M1	1 e 2	Arquitectura de computadores, serviços e redes	2 h	3 h	5 h
M2	3 e 4	Endereçamento e protocolos essenciais	2 h	3 h	5 h
M3	5 e 6	Sistemas operativos e serviços	2 h	3 h	5 h
M4	7 e 8	Protecção de redes e comunicações	2 h	3 h	5 h
M5	9 e 10	Configuração segura de dispositivos	2 h	3 h	5 h

M6	11 e 12	Vulnerabilidades e gestão de actualizações	2 h	3 h	5 h
M7	13 e 14	Proteção de endpoints e ameaças comuns	2 h	3 h	5 h
M8	15 e 16	Registos, monitorização e detecção inicial	2 h	3 h	5 h
M9	17 e 18	Oficina de diagnóstico técnico de rede e sistemas	2 h	3 h	5 h
M10	19 e 20	Projeto integrador: plano de melhoria técnica	2 h	3 h	5 h
Total	20 sessões	10 módulos	20 h	30 h	50 h

Distribuição de horas por modalidade

Modalidade	Horas	Percentagem
Aulas síncronas online no Microsoft Teams	50 h	100%
Total	50 h	100%

A distribuição entre explicação, demonstração, prática e avaliação representa actividades pedagógicas na mesma modalidade síncrona.

Conteúdos programáticos

M1 — Arquitectura de computadores, serviços e redes (5 horas)

- Componentes básicos: estação, servidor, router, switch, ponto de acesso e serviços cloud.
- Diferença entre Internet, rede local, rede sem fios e serviço remoto.
- Representação de topologia simples e fluxo entre cliente e servidor.
- Ligação entre inventário da ação 1 e equipamento real ou simulado.

Atividade prática: Interpretar uma topologia e localizar 12 ativos num esquema fornecido.

Evidência de aprendizagem: Mapa de rede anotado e correspondência com o inventário.

M2 — Endereçamento e protocolos essenciais (5 horas)

- Conceitos de IP, máscara, gateway e endereçamento privado.
- TCP, UDP e portas como identificação de serviços; DNS e DHCP.
- Funcionamento básico de HTTP/HTTPS e TLS, sem aprofundamento criptográfico.
- Leitura segura de resultados de comandos de diagnóstico em ambiente de treino.

Atividade prática: Identificar endereços, nomes e serviços a partir de dados e testes locais autorizados.

Evidência de aprendizagem: Tabela de protocolos, serviços e resultados interpretados.

M3 — Sistemas operativos e serviços (5 horas)

- Sistemas Windows e Linux: ficheiros, processos, contas e serviços básicos.
- Permissões locais e princípio do menor privilégio enquanto característica do sistema.

- Actualizações suportadas, versões e reinícios planeados.
- Noção de superfície de ataque de serviços desnecessários.

Atividade prática: Analisar configurações de um sistema virtual fornecido e enumerar possíveis melhorias.

Evidência de aprendizagem: Lista de verificação de sistema com evidências de observação.

M4 — Proteção de redes e comunicações (5 horas)

- Função de firewall e regras de tráfego de entrada e saída.
- Segmentação por redes lógicas e separação entre utilizadores, gestão e convidados.
- VPN como canal protegido e limites da protecção de transporte.
- Boas práticas de Wi-Fi e gestão de dispositivos de rede.

Atividade prática: Escolher regras de firewall e segmentos num diagrama simulado, sem alterar uma rede de produção.

Evidência de aprendizagem: Esquema de segmentação e matriz simples de tráfego permitido.

M5 — Configuração segura de dispositivos (5 horas)

- Definições iniciais, serviços expostos e configurações por omissão.
- Bloqueio de sessão, protecção de ecrã e segurança de armazenamento.
- Actualizações, cópias de configuração e restabelecimento de alterações.
- Criação de checklist de endurecimento (hardening) adequado a principiantes.

Atividade prática: Aplicar checklist a uma máquina virtual ou ambiente demonstrativo controlado.

Evidência de aprendizagem: Checklist de configuração com antes/depois e evidências.

M6 — Vulnerabilidades e gestão de actualizações (5 horas)

- Vulnerabilidade, exposição, criticidade e contexto de exploração.
- Ciclo de detecção, validação, priorização, correcção e nova verificação.
- Fontes públicas de avisos de segurança e leitura orientada de uma ficha CVE.
- Diferença entre actualização, mitigação temporária e aceitação formal do risco.

Atividade prática: Classificar vulnerabilidades fictícias e elaborar calendário de correcções.

Evidência de aprendizagem: Lista priorizada de correcções com justificação técnica.

M7 — Proteção de endpoints e ameaças comuns (5 horas)

- Vírus, troianos, ransomware e técnicas gerais de infecção.
- Função e limites de antivírus, EDR e filtros de navegação.

- Comportamentos suspeitos observáveis sem executar código nocivo.
- Procedimentos seguros de isolamento, reporte e preservação de evidências.

Atividade prática: Avaliar alertas simulados de endpoint e definir resposta inicial adequada.

Evidência de aprendizagem: Ficha de análise de alertas e encaminhamento, sem intervenção destrutiva.

M8 — Registos, monitorização e detecção inicial (5 horas)

- Diferença entre evento, alerta, incidente e falso positivo.
- Registos de autenticação, sistema, firewall e actualizações.
- Campos básicos: origem, hora, utilizador, acção e resultado.
- Identificação de padrões simples e comunicação ao responsável de segurança.

Atividade prática: Interpretar um conjunto de registos fictícios e assinalar anomalias.

Evidência de aprendizagem: Relatório de triagem com eventos relevantes e limites da análise.

M9 — Oficina de diagnóstico técnico de rede e sistemas (5 horas)

- Inspeção orientada de topologia, serviços e configurações.
- Identificação de desvios de configuração e oportunidades de redução de exposição.
- Priorização de melhorias sem repetir a matriz de risco organizacional.
- Documentação de evidências verificáveis e de pressupostos não confirmados.

Atividade prática: Auditar uma pequena infraestrutura de laboratório com checklist fornecida.

Evidência de aprendizagem: Relatório de diagnóstico técnico com pelo menos cinco achados.

M10 — Projeto integrador: plano de melhoria técnica (5 horas)

- Consolidação de diagrama, serviços, configurações e registos.
- Selecção de medidas correctivas executáveis num ambiente de formação.
- Validação da configuração após alterações seguras e reversíveis.
- Apresentação técnica acessível a público não especializado.

Atividade prática: Concluir um plano de melhorias, demonstrar duas verificações e apresentar resultados.

Evidência de aprendizagem: Mapa técnico, cinco achados, plano de correcção e evidências de dois testes.

Projeto integrador e avaliação final

O módulo 10 encerra e avalia a ação, sem horas adicionais. O projecto desenvolve-se progressivamente durante as sessões e culmina numa entrega individual, ainda que a elaboração de partes do exercício

possa envolver colaboração entre pares. O formador observa tarefas executadas, confirma a autoria individual e verifica as evidências propostas.

Produto final da ação: Diagrama de rede, inventário técnico complementar, checklist de configuração, relatório de cinco achados e plano de melhoria.

Modalidades e ponderações da avaliação

Componente	Instrumento	Peso
Diagnóstica	Questionário inicial e apoio às dificuldades	Sem peso
Formativa	Questionários curtos e verificação de compreensão	20%
Formativa	Tarefas práticas individuais realizadas em aula	20%
Sumativa	Projeto integrador e demonstração individual	60%
Total		100%

Critérios de classificação do projeto

Critério	Peso no projeto (%)
Interpretação da topologia e dos serviços	20%
Qualidade da checklist e observação técnica	25%
Identificação e fundamentação de achados	25%
Adequação das correções e testes	20%
Clareza da comunicação e evidências	10%
Total	100%

A classificação final resulta de 20% da nota dos questionários, 20% da nota das tarefas práticas e 60% da nota do projecto. A escala de classificação é de 0 a 20 valores. A aprovação pedagógica requer classificação final igual ou superior a 10 valores e classificação do projecto igual ou superior a 10 valores. Os requisitos administrativos de assiduidade e certificação dependem do regulamento aplicável da entidade formadora.

Continuidade pedagógica e produto para a ação seguinte

As contas e os serviços identificados alimentam a ação 3; os resultados sobre exposição e serviços críticos informam as decisões de backup, continuidade e recuperação da ação 4.

Recursos e materiais

- Laboratório com máquinas virtuais ou emulador acessível por partilha de ecrã, sempre em ambiente autorizado.
- Topologias, logs fictícios, fichas de configuração, catálogos de vulnerabilidades de treino.

- Computador com navegador, terminal de demonstração, editor de texto e folha de cálculo.

A participação deve ser possível com computador, ligação estável à Internet, navegador e Microsoft Teams. Sempre que a instalação de ferramentas não seja viável, o formador utiliza laboratório remoto de treino, partilha de ecrã e ficheiros simulados, assegurando a prática síncrona de todos os formandos.

Modelos de documentação

- Ficha técnica: ativo, sistema, versão, endereço, serviço, estado e evidência observada.
- Checklist de configuração: requisito, resultado, evidência, prioridade e acção proposta.
- Relatório: achado, contexto, impacto técnico, recomendação, teste e limitação.

Referências técnicas e normativas

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>

Center for Internet Security. (2024). CIS Critical Security Controls (Version 8.1). <https://www.cisecurity.org/controls/v8-1>

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3). <https://doi.org/10.6028/NIST.SP.800-61r3>

Nota: os referenciais são utilizados para enquadramento pedagógico e não equivalem à certificação dos formandos ou à implementação integral de um sistema de gestão.