



INSTITUTO DO EMPREGO
E FORMAÇÃO PROFISSIONAL



worldskills
Portugal

DESCRITIVO TÉCNICO

CAMPEONATO NACIONAL DAS PROFISSÕES DIGITAIS | SKILLSPORTUGAL DIGITAL 2021

SPD 3 | CYBER SECURITY

TÍTULO

WorldSkills Portugal - **Descritivo Técnico** da Competição de **Cyber Security**

PROMOTOR E CONCETOR

Instituto do Emprego e Formação Profissional, I.P. - Departamento de Formação Profissional

R. de Xabregas, 52, 1900-003 Lisboa

Tel: (+351) 21 861 41 00

Website: www.iefp.pt

<https://worldskillsportugal.iefp.pt>

Facebook: www.facebook.com/WorldskillsPortugal

APROVAÇÃO

- António Leite - WorldSkills Portugal | Delegado Oficial
- Conceição Matos - Diretora do Departamento de Formação profissional

CONCEÇÃO METODOLÓGICA E COORDENAÇÃO GERAL

- Carlos Fonseca - WorldSkills Portugal | Delegado Técnico

EQUIPA TÉCNICA/CONCETORES

- Carlos Diogo - Delegado Técnico Assistente da WorldSkills Portugal
- Vasco Vaz – WorldSkills Portugal
- Maria Germano – Secretariado da WorldSkills Portugal
- Fábio Amaral | Presidente de Júri da SkillsPortugal Digital

DESIGN

- Sandra Sousa Bernardo - WorldSkills Portugal | Marketing & Comunicação
- Nuno Viana – Conceção e Design Gráfico

Nos termos do Regulamento em vigor, este Descritivo Técnico está aprovado pela Worldskills Portugal.

[palavras com aplicação em género devem aplicar-se automaticamente também ao outro]

Correspondência com referenciais	<ul style="list-style-type: none">• 481344 - Técnico/a Especialista em Cibersegurança (Referencial nível 5 CNC)• 54 – Cyber Security (WorldSkills International)
----------------------------------	---

OBSERVAÇÕES

Portugal, através do Instituto do Emprego e Formação Profissional, I.P. (IEFP), é membro fundador da *WorldSkills International* (WSI) e da *WorldSkills Europe* (WSE), estando representado nos Comités Estratégicos e Técnicos das referidas Organizações. Cabe ao IEFP a promoção, organização e realização de todas as atividades relacionadas com os Campeonatos das Profissões.

O Descritivo Técnico é o instrumento que elenca as condições de desenvolvimento da competição contextualizada no âmbito de uma determinada profissão.

Conteúdo

TÍTULO	1
PROMOTOR E CONCETOR	1
APROVAÇÃO	1
CONCEÇÃO METODOLÓGICA E COORDENAÇÃO GERAL	1
EQUIPA TÉCNICA/CONCETORES.....	1
DESIGN	1
OBSERVAÇÕES	1
1 INTRODUÇÃO.....	3
1.1 ENQUADRAMENTO	3
1.2 RELEVÂNCIA E SIGNIFICADO DO PRESENTE DESCRITIVO TÉCNICO (DT)	3
1.3 DOCUMENTOS ASSOCIADOS AO DESENVOLVIMENTO DO DT	3
2 REFERENCIAL DE EMPREGO.....	4
2.1 DESIGNAÇÃO E DESCRIÇÃO DA PROFISSÃO.....	4
2.2 ATIVIDADES OPERACIONAIS.....	4
2.3 ÁREAS/UNIDADES DE COMPETÊNCIA.....	5
2.4 PROVA-TIPO (projeto-tipo no âmbito do mercado de trabalho)	10
2.5 QUADRO: ÁREAS/UNIDADES DE COMPETÊNCIA vs CRITÉRIOS DE AVALIAÇÃO vs MÓDULOS	11
3 REFERENCIAL DE AVALIAÇÃO DE DESEMPENHO.....	12
3.1 CRITÉRIOS DE AVALIAÇÃO.....	12
3.2 ESTRUTURA GLOBAL DA PROVA	13
3.3 RELAÇÃO ENTRE OS CRITÉRIOS DE AVALIAÇÃO E OS MÓDULOS DA COMPETIÇÃO	14
3.4 MÓDULOS: FASES DE PRÉ-SELEÇÃO E NACIONAL.....	15
3.5 Procedimentos específicos de avaliação	16
4 ESTRUTURA DA PROVA	16
4.1 NOTAS GERAIS	16
4.2 FORMATO/ESTRUTURA DA PROVA	17
4.3 FICHA DE AVALIAÇÃO	18
4.4 DESENVOLVIMENTO DA PROVA.....	19
5 REQUISITOS DE SEGURANÇA.....	19
5.1 GERAIS	19
6 ORGANIZAÇÃO DA COMPETIÇÃO	20
6.1 INFRAESTRUTURAS TÉCNICAS.....	20
6.2 DA RESPONSABILIDADE DO CONCORRENTE	20
6.3 MATERIAIS E EQUIPAMENTOS PROIBIDOS NA ÁREA DE COMPETIÇÃO	20
6.4 LAY-OUT TIPO DO POSTO DE TRABALHO.....	21
6.5 ATIVIDADES DE PROMOÇÃO DA PROFISSÃO.....	21
6.6 SUSTENTABILIDADE ECONÓMICA / FINANCEIRA E AMBIENTAL.....	21
7 CONCEITOS.....	22

1 INTRODUÇÃO

1.1 ENQUADRAMENTO

PROFISSÃO: CYBER SECURITY
Natureza da competição: Individual
Aplicação: Preparação e organização das provas de avaliação de desempenho profissional do SkillsPortugal Digital; Como referência a outros eventos associados à preparação e organização de provas de desempenho profissional, como por exemplo as previstas no âmbito da formação profissional.
Condições de participação no campeonato das profissões: Escala 1 – 16 ≤ 19 anos (a 31 de dezembro de 2021) Escala 2 – 20 ≤ 35 anos (a 31 de dezembro de 2021) Experiência:

1.2 RELEVÂNCIA E SIGNIFICADO DO PRESENTE DESCRITIVO TÉCNICO (DT)

Nos termos previsto no Artigo 25º, nº 3, do Regulamento Geral e do Artº 17 do Regulamento do Campeonato das Profissões, o presente Descritivo Técnico (DT) é o instrumento de harmonização das condições técnicas de desenvolvimento do campeonato das profissões a nível local, regional e nacional, para a profissão de **CyberSecurity** constituindo-se como um guia para a preparação dos jovens e formadores para os campeonatos, para a elaboração e organização das provas e própria qualidade do campeonato e da formação profissional.

1.3 DOCUMENTOS ASSOCIADOS AO DESENVOLVIMENTO DO DT

O presente DT foi elaborado na base dos padrões definidos a nível nacional e internacional, aconselhando-se a consulta dos seguintes instrumentos:

- *WorldSkills International* – O que fazemos
<https://worldskills.org/what/>
- WorldSkills Portugal - Regulamento do Campeonato das Profissões
<https://worldskillsportugal.iefp.pt/wp-content/uploads/2019/07/Regulamento-do-Campeonato-das-Profiss%C3%B5es.pdf>
- *WorldSkills International* - Quadro das Normas de Especificação
<https://worldskills.org/what/projects/wsss/>
- Catálogo Nacional de Qualificações - Perfil profissional e de formação
<https://catalogo.anqep.gov.pt/qualificacoesDetalhe/1587>
- WorldSkills International - Recursos *on-line*
<https://worldskills.org/skills/>

2 REFERENCIAL DE EMPREGO

2.1 DESIGNAÇÃO E DESCRIÇÃO DA PROFISSÃO

Designação da atividade

Técnico/a de Especialista em Cibersegurança

Descrição Geral da Atividade Profissional

O técnico especialista em Cibersegurança é o profissional que tem como principal objetivo identificar ameaças e vulnerabilidades de segurança, configurar soluções que permitam reduzir a superfície de ataque de servidores, clientes, dispositivos de rede, sistemas industriais e dispositivos móveis, bem como a monitorizar e responder a incidentes de Segurança Informática.

2.2 ATIVIDADES OPERACIONAIS

No âmbito da sua atividade profissional, o/a Técnico/a de Especialista em Cibersegurança desenvolve as seguintes atividades operacionais:

1. Instalar, configurar e colocar em produção plataformas de cibersegurança ao nível das infraestruturas de comunicações e de segurança perimétrica, de tecnologias de informação, e de suporte aos ambientes colaborativos.
2. Configurar de firewalls, IPS/IDS, serviços de servidor e de soluções de segurança web proteção de informação confidencial.
3. Monitorizar falhas de segurança e investiga violações.
4. Responder a situações anómalas e incidentes de cibersegurança.
5. Realizar testes de penetração simulando ataques para procurar vulnerabilidades antes que possam ser explorados por razões maliciosas.
6. Reunir, preservar, processar, analisar e apresentar provas para mitigar a vulnerabilidade das redes de atividades criminosas, fraudes e outras atividades hostis.
7. Utilizar táticas, técnicas e procedimentos, utilizando uma gama completa de ferramentas e processos de investigação.
8. Apoiar os planos de recuperação de desastres das organizações, que descreve as etapas e procedimentos para restaurar o bom funcionamento dos sistemas e redes de TI de uma organização após um desastre ou ataque.
9. Devem acompanhar os métodos mais recentes utilizados pelos invasores para se infiltrarem nos sistemas informáticos, bem como com as novas tecnologias de segurança que podem ajudar as organizações a combater estas ameaças com sistemas e medidas robustos.
10. Recolher e efetuar o tratamento de informação e evidências, utilizando ferramentas especializadas.
11. Preparar os inputs necessários como apoio à elaboração de relatórios forense por parte de especialistas certificados seguindo os preceitos e regras de rigor forense.

2.3 ÁREAS/UNIDADES DE COMPETÊNCIA

Área funcional: PLANEAMENTO E ORGANIZAÇÃO	Importância relativa (%)
PLANEAMENTO E ORGANIZAÇÃO	5%

Os concorrentes **conhecer e compreender:**

- A legislação aplicável á sua profissão;
- Informática na ótica do utilizador (tratamento de texto, digitalização e paginação);
- Os fundamentos do sistema que contribuem para a sustentabilidade do produto final;
- Preparar adequadamente a lista de requisitos dos projetos a desenvolver;
- As técnicas associadas à recolha de informação;
- Os princípios inerentes ao planeamento e organização do trabalho, em função dos requisitos, prioridades e prazos.

Os concorrentes **terão de conseguir:**

- Seguir as normas e regulamentos de saúde e segurança;
- Manter um ambiente de trabalho seguro e confortável;
- Definir uma metodologia de trabalho;
- Aplicar conhecimentos relativos à correta construção do guião;
- Identificar e utilizar adequadamente os softwares informáticos em função do objetivo;
- Planear a sequência de operações/técnicas a aplicar na resolução do problema;
- Nomear/Organizar e Arquivar adequadamente os ficheiro digitais.

UNIDADES DE COMPETÊNCIA

- Planeamento de Tarefas;
- Recolha e Sintetização de Informação;
- Gestão do tempo;
- Estrutura de pastas e ficheiros;
- Organização do posto de trabalho;
- Ergonomia, segurança e higiene.

Área funcional: Técnica	Importância relativa (%)
Desenho e Criação de Sistemas Seguros	25%

Os concorrentes **conhecer e compreender**:

- Sistemas operativos de servidor e de cliente;
- Redes informáticas;
- Os princípios e métodos de segurança informática e privacidade que se aplicam ao desenvolvimento de software.

Os concorrentes **terão de conseguir**:

- Aplique os princípios de privacidade e segurança informática aos requisitos organizacionais (relevantes à confidencialidade, integridade, disponibilidade, autenticação, não-repúdio) ao projetar e documentar os procedimentos gerais de teste e avaliação.
- Realizar avaliações abrangentes e independentes dos controles de segurança de gestão, operacionais e técnicos e melhoramentos dos controlos aplicados ou herdados por sistemas de tecnologia da informação para determinar a eficácia geral dos controlos;
- Desenvolver e realizar avaliações de sistemas para avaliar se estão em conformidade com especificações e requisitos;
- Analise a segurança de aplicativos/programas de computador novos ou existentes, software ou programas utilitários especializados, para fornecer resultados acionáveis;
- Desenvolver regras e requisitos de tecnologia da informação, por forma que a segurança informática seja aplicada nas arquiteturas de base;
- Garantir que os requisitos de segurança necessários para proteger a missão da organização e os processos de negócios sejam adequadamente tratados em todos os aspetos da arquitetura empresarial, incluindo modelos de referência, arquiteturas de segmento e solução e os sistemas resultantes que suportam essas missões e processos de negócios;
- Avaliar os requisitos funcionais e traduzir os requisitos funcionais em soluções técnicas;
- Planejar, preparar e executar testes de sistemas;
- Projetar, desenvolver, testar e avaliar a segurança do sistema de informações ao longo do ciclo de vida de desenvolvimento de sistemas.

UNIDADES DE COMPETÊNCIA:

- Análise e criação de sistemas operativos seguros;
- Análise e Criação de arquitetura de rede seguros;
- Análise e Criação de serviços de cloud seguros;
- Utilização de últimos padrões.

Área funcional: Técnica	Importância relativa (%)
Operação e Manutenção de Sistemas Seguros	25%

Os concorrentes **conhecer e compreender**:

- Conceitos de arquitetura de segurança de rede, incluindo topologia, protocolos (TCP/IP), componentes e princípios;
- Serviços de rede como DHCP, DNS e Active Directory;
- Conceitos e funções de Servidor Web, FTP e SMB;
- Noções básicas de segurança de rede (“honeypots”, tipos de malware, tipos de hackers e seus métodos, ataques de engenharia social e ataques de password);
- Conceitos e metodologias de análise de “malware”;
- Conceitos e funções de firewall e Proxy;
- Técnicas de administração de sistemas, rede e proteção do sistema operativo;
- Políticas de segurança de utilizador de tecnologia da informação organizacional (TI) (por exemplo, criação de conta, regras de palavra-chave e controle de acesso);
- Princípios e métodos de segurança de tecnologia da informação (TI);
- Capacidades e ferramentas de operações cibernéticas de parceiros internos e externos;
- Métodos de autenticação, autorização e controle de acesso.

Os concorrentes **terão de conseguir**:

- Instalar, configurar, testar, operar, manter e gerir a infraestrutura de rede em segurança;
- Gerir servidores que permitam a partilha e transmissão de dados;
- Instalar, configurar, solucionar problemas e manter as configurações do servidor (hardware e software) para garantir sua confidencialidade, integridade e disponibilidade;
- Adicionar e/ou editar regras de firewall e proxy;
- Gerir e criar contas de utilizador em relação ao controle de acesso, palavras-chaves e administração;
- Analisar os sistemas das organizações e atualizar as soluções dos sistemas de informação para ajudá-los a operar com mais segurança, eficiência e eficácia;
- Implementar segurança em cloud e virtualização;
- Implementar segurança em sistemas operativos (Por exemplo aplicação de LAPS e Tiers);
- Realizar auditorias de programas de tecnologia da informação (TI), rede de infraestrutura para fornecer otimização contínua, segurança informática e suporte para resolução de problemas.

UNIDADES DE COMPETÊNCIA:

- Gestão e manutenção de serviços de TCP/IP;
- Gestão e manutenção de Firewall;
- Gestão e manutenção de serviços de autenticação;
- Aplicação de políticas de segurança.

Área funcional: Técnica	Importância relativa (%)
Proteção e Defesa de Sistemas Seguros	25%

Os concorrentes **conhecer e compreender**:

- Conceitos de encriptação de sistemas operativos, discos e serviços;
- Conceitos de CA e certificados;
- Conceitos de aplicação de defesa em profundidade e proteção em perímetro;
- Conceitos nos tipos de ameaças (físicas, wireless, port scanning e DNS);
- Métodos e técnicas usados para detetar várias atividades de exploração;
- Padrões da indústria e princípios de análise, métodos, ferramentas para identificação de vulnerabilidades;
- Estrutura, abordagem e estratégia de ferramentas de exploração (por exemplo, “sniffers”, “keyloggers”) e técnicas (por exemplo, obter acesso “backdoor”, recolher/exfiltrar dados, conduzir análise de vulnerabilidade de outros sistemas na rede);
- Investigações de ameaças, relatórios, ferramentas investigação e leis/regulamentos;
- Realizar pesquisas (incluindo testes de penetração) para avaliar potenciais vulnerabilidades em sistemas;
- Vulnerabilidade de segurança informática e princípios de privacidade;
- Exploração ou ameaças emergentes conforme se aplicam a sistemas e software instalados;
- Táticas internas para antecipar e/ou emular recursos e ações de ameaças;
- Categorias de incidentes, resposta e metodologias de tratamento de incidentes;
- Aplicação de medidas para riscos de segurança identificados;
- Abordagens de autenticação, autorização e acesso (por exemplo, controle de acesso baseado em função, controle de acesso obrigatório e controle de acesso discricionário).

Os concorrentes **terão de conseguir**:

- Implementar encriptação em sistemas operativos, discos, ficheiros e serviços;
- Implementar CA e/ou SCA e aplicação de certificados em serviços;
- Testar, implementar, manter, rever e administrar o hardware e software de infraestrutura necessários para gerir com eficácia a rede de computadores e os seus recursos;
- Monitorizar a rede para corrigir ativamente atividades não autorizadas;
- Responder a crises ou situações urgentes dentro de suas próprias áreas de especialização para mitigar ameaças imediatas e potenciais;
- Use abordagens de mitigação, preparação, resposta e recuperação, conforme necessário, para maximizar a sobrevivência da vida, preservação da propriedade e segurança da informação;
- Implementar e/ou configurar sistemas de identificação de vulnerabilidades na rede (Por exemplo o OpenVAS);
- Realizar avaliações de ameaças e vulnerabilidades;
- Analisar as informações recolhidas para identificar vulnerabilidades e potencial de exploração;
- Determinar desvios de configurações aceitáveis, empresa ou política local;
- Avaliar o nível de risco e desenvolver e/ou recomendar contramedidas de mitigação adequadas em situações operacionais e não operacionais;
- Siga os procedimentos documentados da empresa para preparação e resposta a incidentes.

UNIDADES DE COMPETÊNCIA:

- Desenvolvimento de sistemas e serviços encriptados;
- Gestão de vulnerabilidades;
- Gestão de incidentes.

Área funcional: Técnica	Importância relativa (%)
Investigação, Recolha e Análise Digital	20%

Os concorrentes **conhecer e compreender:**

- Ficheiros de sistema (por exemplo, ficheiros de log, ficheiros de registo, ficheiros de configuração) que contêm informações relevantes e onde encontrar esses ficheiros de sistema;
- Recursos e repositórios de inteligência cibernética/coleta de informações;
- Fontes de disseminação de informações de vulnerabilidade (por exemplo, alertas, avisos e boletins);
- Tipos e recolhas de dados persistentes;
- Conceitos de cópias de segurança e restauro;
- Importância da preparação para recuperação em casos de desastres naturais.

Os concorrentes **terão de conseguir:**

- Analisar informações sobre ameaças de várias fontes, disciplinas e agências em toda a comunidade;
- Sintetizar e colocar as informações de inteligência no contexto, extrair percepções sobre as possíveis implicações;
- Use medidas defensivas e informações recolhidas de uma variedade de fontes para identificar, analisar e reportar eventos que ocorrem ou podem ocorrer dentro da rede para proteger informações, sistemas de informação e redes contra-ameaças;
- Recolher, processar, preservar, analisar e apresentar evidências relacionadas com segurança cibernética em apoio à mitigação de vulnerabilidade de rede e/ou investigações de aplicação da lei;
- Aplicar conhecimentos linguísticos, culturais e técnicos para apoiar a recolha de informações, análise e outras atividades de segurança cibernética;
- Realizar cópias de segurança e restauro de sistemas e/ou serviços;
- Execute a recuperação de dados e sistemas com sucesso em caso de perda.

UNIDADES DE COMPETÊNCIA:

- Centralização, gestão e análise de logs;
- Análise de ficheiros de sistemas e rede;
- Gestão de cópias de segurança e recuperação.

2.4 PROVA-TIPO (projeto-tipo no âmbito do mercado de trabalho)

Para efeito de aferição das competências e de avaliação do desempenho profissional, o/a concorrente terá de solucionar um problema concreto do mercado de trabalho, associado à atividade de segurança informática.

A prova a desenvolver, de acordo com especificações técnicas pré-estabelecidas, deverá assentar em 4 áreas de atividade (módulos):

- Desenvolvimento de Segurança em Sistemas Operativos;
- Desenvolvimento de Segurança em Redes;
- Identificação e Exploração de Vulnerabilidades;
- Proteção e Defesa de Vulnerabilidades.

2.5 QUADRO: ÁREAS/UNIDADES DE COMPETÊNCIA vs CRITÉRIOS DE AVALIAÇÃO vs MÓDULOS

Quadro correspondência de Critérios de Áreas de Competência Unidades de Competência com Critérios de Avaliação e Módulos																						
		ÁREAS DE COMPETÊNCIA																				
		Planeamento e Organização		Desenho e Criação de Sistemas Seguros		Operação e Manutenção de Sistemas Seguros		Proteção e Defesa de Sistemas Seguros		Investigação, Recolha e Análise Digital												
		5%		25%		25%		25%		20%												
		UNIDADES DE COMPETÊNCIA																				
		Planeamento de Tarefas	Recolha e Sintetização de Informação	Gestão do tempo	Estrutura de pastas e ficheiros	Organização do posto de trabalho	Ergonomia, segurança e higiene	Análise e criação de sistemas operativos seguros	Análise e Criação de serviços de rede seguros	Análise e Criação de serviços de cloud seguros	Utilização de últimos padrões	Gestão e manutenção de serviços de TCP/IP	Gestão e manutenção de Firewall	Gestão de identidade e acesso	Aplicação de políticas de segurança	Desenvolvimento de sistemas e serviços encriptados	Gestão de vulnerabilidades	Gestão de incidentes	Centralização, gestão e análise de logs	Análise de ficheiros de sistemas e rede	Gestão de cópias de segurança e recuperação	
Critérios	Planeamento e Organização	X	X	X	X	X	X															
	Desenho e Criação de Sistemas Seguros							X	X	X	X											
	Operação e Manutenção de Sistemas Seguros											X	X	X	X							
	Proteção e Defesa de Sistemas Seguros															X	X	X				
	Investigação, Recolha e Análise Digital																		X	X	X	
Módulos	Desenvolvimento de Segurança em Sistemas Operativos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						X
	Desenvolvimento de Segurança em Redes	X	X	X	X	X	X		X	X	X	X	X		X	X						X
	Identificação e Exploração de Vulnerabilidades	X	X	X	X	X	X				X						X				X	
	Proteção e Defesa de Vulnerabilidades	X	X	X	X	X	X				X					X	X	X	X	X		

3 REFERENCIAL DE AVALIAÇÃO DE DESEMPENHO

3.1 CRITÉRIOS DE AVALIAÇÃO

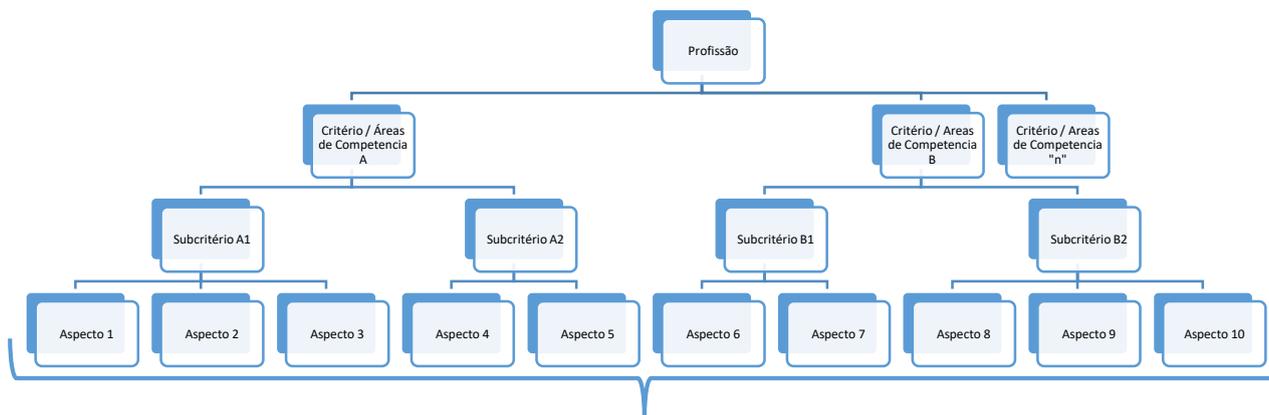
Decorrente da análise do perfil de emprego, ponderadas as importâncias relativas das diversas áreas de competência, os critérios de avaliação a considerar na elaboração da prova são os seguintes:

- A - Planeamento e Organização
- B - Desenho e Criação de Sistemas Seguros
- C - Operação e Manutenção de Sistemas Seguros
- D - Proteção e Defesa de Sistemas Seguros
- E - Investigação, Recolha e Análise Digital

Os critérios de avaliação e a respetiva notação para esta prova em concreto são as constantes do quadro seguinte:

Critérios de Avaliação		Natureza e Ponderação		
		Mensurável	Ajuizável	Total
A	Planeamento e Organização		5	5
B	Desenho e Criação de Sistemas Seguros	25		25
C	Operação e Manutenção de Sistemas Seguros	25		25
D	Proteção e Defesa de Sistemas Seguros	25		25
E	Investigação, Recolha e Análise Digital	20		20
Total		95	5	100

Nota: Cada critério será dividido em subcritérios e estes divididos em aspetos a observar.



A observar/avaliar no decorrer da Prova

3.2 ESTRUTURA GLOBAL DA PROVA

O objetivo da prova é fornecer condições de evidência das competências requeridas no âmbito da profissão e proporcionar condições de avaliação completas, equilibradas, justas e transparentes de acordo com as exigências técnicas da profissão. A relação entre a prova, o referencial de competências/critérios de avaliação é um dos indicadores chave para a garantia da qualidade do campeonato.

A prova assume contornos de uma competição **modular**, visando a avaliação individual das diferentes competências necessárias a um desempenho profissional exemplar. Consiste no desenvolvimento de trabalhos práticos, na base de um conjunto de atividades associadas à resolução de problemas e ao desenvolvimento de um produto ou serviço, e a avaliação do conhecimento teórico está limitado ao estritamente necessário à conclusão prática do projeto (prova).

Os módulos de avaliação estruturam a forma de organização da prova e correlacionam os critérios de avaliação com as atividades operacionais (do módulo) a que os concorrentes serão sujeitos.

Neste contexto, no caso da competição em apreço, a estrutura da prova assenta no âmbito dos seguintes 4 módulos de competição.

1. Desenvolvimento de Segurança em Sistemas Operativos
2. Desenvolvimento de Segurança em Redes
3. Identificação e Exploração de Vulnerabilidades
4. Proteção e Defesa de Vulnerabilidades

A prova tem duração total entre 12 e 15 horas.

Toma-se como referência a seguinte distribuição da competição pelos 4 dias do campeonato:

Quadro Módulos Tempo Dia de prova			
	Módulos	Tempo	Dia sugerido
1	Desenvolvimento de Segurança em Sistemas Operativos	3h	C1
2	Desenvolvimento de Segurança em Redes	3h	C2
3	Identificação e Exploração de Vulnerabilidades	3h	C3
4	Proteção e Defesa de Vulnerabilidades	3h	C4

3.3 RELAÇÃO ENTRE OS CRITÉRIOS DE AVALIAÇÃO E OS MÓDULOS DA COMPETIÇÃO

A relação entre os critérios de avaliação e os módulos de competição, incluindo as pontuações associadas, são as descritas no quadro seguinte:

Quadro correspondência de Critérios de Avaliação Módulos						
		Critérios de Avaliação				
		A	B	C	D	E
		Planeamento e Organização	Desenho e Criação de Sistemas Seguros	Operação e Manutenção de Sistemas Seguros	Proteção e Defesa de Sistemas Seguros	Investigação, Recolha e Análise Digital
Módulos	Desenvolvimento de Segurança em Sistemas Operativos	X	X	X	X	X
	Desenvolvimento de Segurança em Redes	X	X	X	X	X
	Identificação e Exploração de Vulnerabilidades	X	X		X	X
	Proteção e Defesa de Vulnerabilidades	X	X		X	X

3.4 MÓDULOS: FASES DE PRÉ-SELEÇÃO E NACIONAL

Quadro correspondência de Critérios de Avaliação Módulos Fases do Campeonato											
 Critérios de Avaliação		Módulos de Avaliação				Fase de Pré-seleção			Fase Nacional		
		Desenvolvimento de Segurança em Sistemas Operativos	Desenvolvimento de Segurança em Redes	Identificação e Exploração de Vulnerabilidades	Proteção e Defesa de Vulnerabilidades	Referência					
						25% do previsto no Descritivo Técnico			100% do previsto no Descritivo Técnico		
						Carga Horária:					
						1 - 3 horas			12 - 15 horas		
						Nível de exigência da prova					
						Baixa	Média	Alta	Baixa	Média	Alta
A	Planeamento e Organização					X					X
B	Desenho e Criação de Sistemas Seguros					X					X
C	Operação e Manutenção de Sistemas Seguros										X
D	Proteção e Defesa de Sistemas Seguros										X
E	Investigação, Recolha e Análise Digital										X
Fases do Campeonato	Pré-seleção	X	X			Nível de exigência da prova: Alto: 100% do estabelecido para a alta exigência; Médio: 75% do estabelecido para a alta exigência; Baixo: 50% do estabelecido para a alta exigência					
	Nacional	X	X	X	X						

3.5 Procedimentos específicos de avaliação

No âmbito da profissão em apreço, determina-se a aplicação das seguintes condicionantes de avaliação:

- Não poderá ser atribuída pontuação aos aspetos que o concorrente não consiga completar devido a falta de ferramenta/equipamento na sua caixa de ferramenta (aplicável nos casos em que a ferramenta/equipamento seja da responsabilidade do concorrente ou respetiva entidade);
- Se algum concorrente não poder completar operações/tarefas da prova devido a falhas que não lhe sejam imputadas, tais como:
 - Falhas do posto de trabalho
 - Avarias de equipamentos não imputável a mau uso do concorrente
 - Falhas de energia

As pontuações referentes a essas operações/tarefas devem ser atribuídas aos concorrentes que tentaram/iniciaram a execução da (s) mesma (s);

- Em todos os casos os jurados têm de avaliar, na íntegra, todos os aspetos da ficha de avaliação em cada concorrente, ainda que não tenha terminado a prova;
- A pontuação atribuída aos aspetos a avaliar pode variar de acordo com a escala definida para cada competição. No entanto, deve refletir o grau de complexidade/dificuldade aceitável pela realidade do sector;
- Na constituição dos grupos de jurados para avaliação, devem ser tidas em consideração a experiência em campeonatos das profissões e a experiência profissional;
- O grupo de jurados responsável pela avaliação de um determinado subcritério deverá avaliar todos os aspetos, referentes a esse subcritério, em todos os concorrentes;

Poderão ser consideradas para efeitos de penalização, com impacto na avaliação, as seguintes infrações

- O não cumprimento das regras de higiene e segurança no trabalho e de proteção do meio ambiente;
- A utilização de equipamentos ou softwares não autorizados no módulo/prova;
- O acesso ou permanência no ambiente de desenvolvimento da prova fora dos períodos autorizados;
- O acesso a qualquer informação, por qualquer meio, acerca da prova e do modo em que esta se realiza;

Qualquer destas infrações será aceite para discussão e posterior aplicação de penalização adequada sempre que, haja prova ou, na falta desta, seja observada e reportada pelo mínimo de dois jurados.

4 ESTRUTURA DA PROVA

4.1 NOTAS GERAIS

A prova será desenhada para uma execução num período não inferior a 12 horas e não superior a 15 horas, sendo constituída pelos seguintes 4 módulos de competição:

1. Desenvolvimento de Segurança em Sistemas Operativos
2. Desenvolvimento de Segurança em Redes
3. Identificação e Exploração de Vulnerabilidades
4. Proteção e Defesa de Vulnerabilidades

No desenho da prova deverão, ainda, ser levados em consideração os seguintes requisitos:

- Estar em conformidade com o prescrito no presente DT e respeitar as exigências e as normas de avaliação estabelecidas;
- Ser acompanhada por uma grelha de avaliação a validar pelos jurados antes do início da prova;
- Ser, obrigatoriamente, testada antes de ser proposta à WorldSkills Portugal, para garantir que foi aferido o seu funcionamento/construção/realização dentro do tempo previsto etc. (segundo as exigências da profissão), assim como a fiabilidade e a adequação da lista de infraestruturas;
- Ser acompanhada de meios de prova da sua exequibilidade no tempo previsto. Por exemplo, a fotografia de um projeto realizado segundo os parâmetros da prova, com o auxílio do software e do equipamento previsto, segundo os conhecimentos requeridos e dentro dos tempos definidos;
- Ter em atenção aspetos associados à sustentabilidade, visando por um lado a minimização dos custos associados à sua organização, e por outro o respeito pelas normas ambientais e consequentemente a diminuição da pegada ecológica associada ao evento;
- Não incidir em áreas não abrangidas pelo presente Descritivo Técnico, nem alterar a distribuição da avaliação nele prevista;
- Apenas prevê a avaliação do conhecimento e compreensão através da sua aplicação em contexto de prática real de trabalho;
- Não avalia o conhecimento sobre regras e regulamentos da WorldSkills.

4.2 FORMATO/ESTRUTURA DA PROVA

A prova é constituída por:

- Orientações gerais para a equipa de jurados (antes, durante e após a realização das provas);
- Cronograma de desenvolvimento da prova;
- Orientações para os concorrentes;
- Caracterização e descrição da prova: memória descritiva, desenhos técnicos e outras especificações;
- Ficha de avaliação por concorrente, critérios, subcritérios, aspetos a avaliar e pontuações associadas;
- Ata, termo de aceitação e outra documentação associada.

Na estruturação da prova dever-se-á, ainda, considerar o seguinte:

- A avaliação estará dividida por 4 módulos, a serem desenvolvidos num posto (s) de trabalho (s);
- Todos os concorrentes têm de competir em todos os módulos;
- A prova terá como duração mínima - 12 horas;
- A prova terá como duração máxima - 15 horas;
- O concorrente tem de executar as tarefas de forma independente.

Especificações de cada módulo a considerar na estruturação da prova:

1. Desenvolvimento de Segurança em Sistemas Operativos

- Security Hardening em Active Directory (GPO, LAPS e identidade);
- Security Hardening em servidor de ficheiros;
- Gestão e configuração de antivírus;
- Encriptação de ficheiros e discos;
- Gestão de Firewall;

2. Desenvolvimento de Segurança em Redes

- Security Hardening de serviços web;
- Security Hardening de serviços de transferência de ficheiros e outros;
- Security Hardening de Acesso Remoto.
- Gestão e implementação de proxy;
- Gestão de firewall.

3. Identificação e Exploração de Vulnerabilidades

- Análise de ficheiros de sistemas e redes;
- Pesquisa de vulnerabilidades;
- Gestão de incidentes;
- Identificação de processos e ficheiros maliciosos;
- Realização de pentest (Enumeration, ataque servidor web, ataques a base de dados, ataques a sistemas Windows, root access, cryptography e steganography).

4. Proteção e Defesa de Vulnerabilidades

- Implementação de zonas de redes, honeypot e firewall;
- Implementação de PKI;
- Implementação de mecanismos de proteção (reconnaissance, application detection, malware/exploits, phishing, lateral propagation/botnet e data leakage);
- Implementação de gestão de logs.

A avaliação assenta em atividades representativas da profissão. O cronograma da prova, sempre que possível, deve ser elaborado de modo a garantir atividades de avaliação durante todo o tempo da competição.

4.3 FICHA DE AVALIAÇÃO

Na ficha de avaliação são registados todos os aspetos a avaliar, aglutinados em subcritérios (b) (unidades de competência) e critérios (a) (áreas de competência)

Exemplo de ficha de avaliação.

		Skill name							
		Profissão XXXXX							
		Critério / Área de Competência		Pontuação					
		A	Critério A	10					
		B	Critério B	10					
Sub Critérios ID	Sub Critérios Nome e Descrição	Tipo Avaliação M=Mens. J = Ajuiz.	Descrição dos Aspectos	Pontos Ajuizável	Explicações detalhadas (M ou J) OU Descrição dos pontos Ajuizáveis	Medida Requerida (Só para M)	Áreas de Competência	Pontuação Máxima	
A1	Subcritério 1	J	Aspecto Ajuizável 1	0	Desempenho abaixo do padrão da indústria, incluindo não tentativa		1	2,00	
b)			c)	1	O desempenho de acordo com o padrão da indústria (Produto ou serviço de gama baixa)				
				2	O desempenho supera o padrão da indústria (Produto ou serviço de gama média)				
				3	Excelente desempenho em relação às expectativas da indústria (Produto ou serviço de luxo)				
		M	Aspecto Mensurável 1		Descrição detalhada	Medida Pretendida	1	2,00	
		M	Aspecto Mensurável 2		Descrição detalhada	Sim / Não	1	2,00	

Os aspetos poderão ser de duas naturezas, **mensuráveis** e **ajuizáveis**

Os aspetos a observar de **natureza mensurável** (d) englobam:

- Cumpriu / Não cumpriu
- Fez / não fez / fez parte
- Preparou / não preparou / parcialmente
- Existe / Não existe / Existe parte

Os aspetos a observar de **natureza ajuizável** (c) serão comparados com um padrão / standard. Vão ser acompanhados de descritores em texto (e), foto e/ou padrões que clarifiquem os standards e ajudem à correta avaliação.

Na avaliação de **aspetos ajuizáveis** (c) o gosto ou opinião pessoal não podem interferir, esta avaliação baseia-se na confrontação com os standards previamente definidos.

4.4 DESENVOLVIMENTO DA PROVA

4.4.1 Quem é responsável pela conceção da prova

A prova poderá ser desenvolvida:

- pelo Presidente de Júri

4.4.2 Em que momento (s) é a prova desenvolvida

A prova é desenvolvida de acordo com o seguinte calendário:

	Período/momento	Atividade
1	No final da competição	É atualizado o DT para a competição seguinte e definidas características da próxima prova
2	6 meses antes da competição	As provas são elaboradas pelo concetor de acordo com o definido no ponto 1
3	Desejavelmente as provas não serão divulgadas na integra	
4	3 meses de antecedência	Serão divulgadas características técnicas de equipamentos e uma estrutura tipo da prova
5	Um mês antes da competição	Se possível, divulgação de elementos técnicos dos equipamentos a fornecer pela entidade parceira
6	Na preparação da competição C-4 a C-2	A prova e ficha de avaliação é apresentada aos jurados, testada/finalizada. Caso a prova tenha sido divulgada deve ser alterada pelo menos 30%, por votação entre a equipa de jurados.

Nota: A alteração “30%” não pode implicar, em qualquer caso, alterações à lista de infraestruturas previamente aprovada.

5 REQUISITOS DE SEGURANÇA

5.1 GERAIS

O Regulamento de Segurança encontra-se divulgado no site da Worldskills Portugal e integra uma ficha de segurança específica, de cumprimento **OBRIGATÓRIO**, e que se organiza em torno dos seguintes itens:

- Os concorrentes devem deixar a sua área de trabalho livre de qualquer objeto, de modo a evitar que tropecem, escorreguem ou caiam;
- O local de trabalho deverá ser bem iluminado e devidamente climatizado.
- Respeitar as regras de ergonomia e descanso regular.

6 ORGANIZAÇÃO DA COMPETIÇÃO

A prova deve ser desenvolvida de acordo com a lista especificada neste ponto, onde são identificados de forma precisa, o “hardware” e software a utilizar.

6.1 INFRAESTRUTURAS TÉCNICAS

Os requisitos de infraestrutura técnica a seguir identificados são **fornecidos pelo organizador** da competição e a quantidade deverá ser adequada ao n.º de concorrentes em competição.

- Acesso a duas virtual machine na cloud, contendo os seguintes softwares e sistemas operativos (a lista definitiva de software e respetivas versões será disponibilizada mais perto da realização do campeonato):
 - Windows 10 professional
 - Microsoft 365 Educação
 - Microsoft TEAMS
 - Adobe acrobat reader
 - Firefox and Chrome browsers
 - 7-Zip Compressão ficheiros
 - VLC Media Player
 - Kali Linux com todo o software de base.
- Disponibilização e configuração de IPCAM a cada participante.

6.2 DA RESPONSABILIDADE DO CONCORRENTE

Os concorrentes deverão ter um acesso físico aos computadores virtuais:

- Mesa ou secretária de trabalho
- Cadeira (de escritório se possível)
- Eletricidade para os equipamentos
- Iluminação adequada à tarefa.
- Desktop ou Portátil capaz de suportar o acesso à cloud
- Um ou mais monitores
- Teclado, Rato e respetivo tapete.
- Acesso à internet com pelo menos 40/40 Mbps

Os concorrentes poderão utilizar outras ferramentas pessoais de trabalho, desde que, durante a fase de preparação da prova (C-4 a C-1), tal seja autorizado pelo presidente do júri.

6.3 MATERIAIS E EQUIPAMENTOS PROIBIDOS NA ÁREA DE COMPETIÇÃO

Na área de trabalho é apenas permitido o equipamento previsto. Outros equipamentos dos concorrentes só poderão ser utilizados com aprovação do presidente de júri.

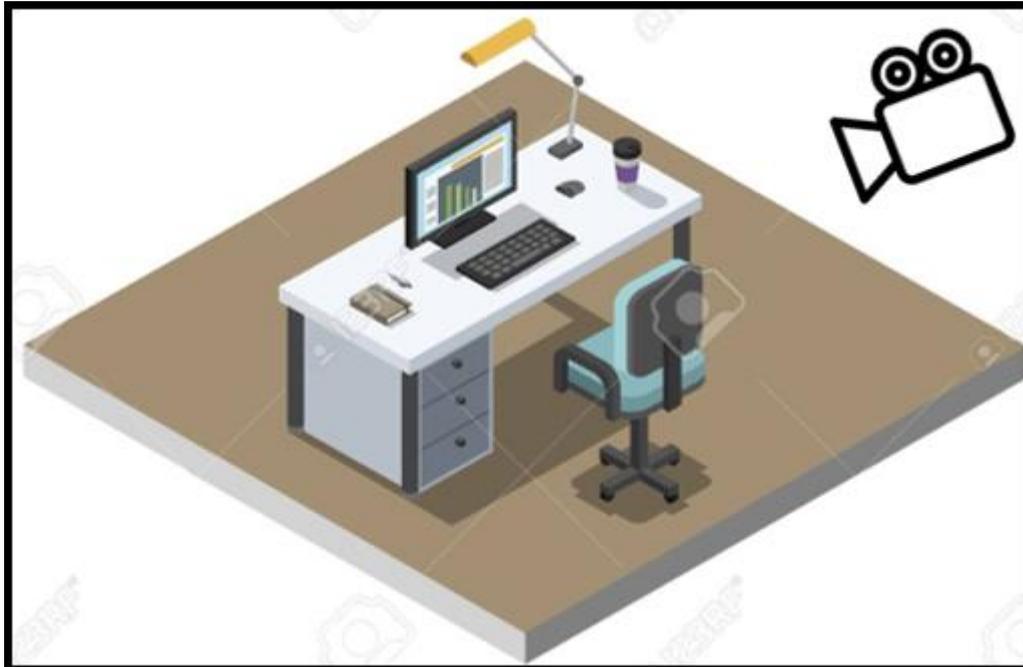
No caso de um concorrente não seguir esta orientação, poderá sofrer penalização no critério “preparação do trabalho” da respetiva prova.

Os jurados devem informar, clara e inequivocamente, sobre os tipos de equipamento e software que não podem ser utilizados na competição.

Os concorrentes NÃO devem/podem:

- Utilizar tecnologia de armazenamento de dados (Pen USB, Discos Externos)
- Utilizar telemóvel;
- Informação digital gravada
- Fazer cópias dos documentos disponibilizados
- Comunicar com o seu jurado durante os períodos de prova.

6.4 LAY-OUT TIPO DO POSTO DE TRABALHO



Características adicionais do posto de trabalho

- Boa iluminação
- Deve estar num lugar com baixo ruído
- Ter disponíveis ligações à rede elétrica
- Ter disponíveis ligações à internet (Wired or Wi-Fi).

6.5 ATIVIDADES DE PROMOÇÃO DA PROFISSÃO

Sempre que as condições o permitam, deverá a organização, os patrocinadores e a equipa de jurados trabalhar no sentido de disponibilizar live stream do trabalho realizado pelos concorrentes.

6.6 SUSTENTABILIDADE ECONÓMICA / FINANCEIRA E AMBIENTAL

Tendo em vista a otimização dos recursos, deve constar apenas o indispensável, evitando o desnecessário e o excessivo. Deve ser excluída a necessidade de impressão de qualquer documento.

7 CONCEITOS

REFERENCIAL DE EMPREGO

O referencial de emprego elenca, para cada profissão, a **designação da profissão** e a **descrição geral da atividade profissional**, as **atividades operacionais** e as **áreas de competência nucleares** identificadas a partir dos referenciais nacionais e internacionais.

DESIGNAÇÃO DA PROFISSÃO

Identifica a designação do profissional no âmbito do mercado de trabalho, tendo por referência a designação estabelecida no âmbito da ANQEP e/ou da *WorldSkills International*.

DESCRIÇÃO DA PROFISSÃO

Descreve, de forma sintética, o objetivo da profissão e a sua importância para o mercado de trabalho, designadamente na produção de um determinado produto ou serviço. É utilizada a descrição existente no Perfil Profissional da ANQEP e/ou da *WorldSkills International*.

ATIVIDADES OPERACIONAIS

Identificação das atividades que integram a profissão, numa lógica de processo produtivo. Compreende a decomposição da profissão em atividades (numa lógica funcional ou processual), identificadas a partir do referencial nacional, designadamente do Perfil profissional da profissão constante do CNQ.

ÁREAS DE COMPETÊNCIA

Refere-se a uma **combinação de conhecimentos, aptidões e atitudes** adequados a um determinado contexto profissional, tendo em vista o desenvolvimento, no todo ou em parte, de um bem, seja ele um produto e/ou serviço, com valor para o mercado de trabalho. A cada área de competência associar-se-á um peso relativo da sua importância para a profissão. Esse peso poderá ser identificado a partir da complexidade, utilização, criticidade ou outro.

FICHA DE AVALIAÇÃO/GRELHA DE OBSERVAÇÃO

É o instrumento de base dos jurados para observação do desempenho dos concorrentes para a correspondente avaliação. A observação poderá desenvolver-se em tempo real (isto é, no decurso da execução), ou na lógica do produto final.

CRITÉRIO DE AVALIAÇÃO

Considerando que a avaliação pretende aferir se um desempenho está de acordo com um padrão planeado, esperado e desejado, os critérios de avaliação segmentam o referencial de emprego em 4 a 6 grandes áreas (de competência ou funcionais). Ou seja, os critérios de avaliação definem o âmbito da avaliação do desempenho profissional esperado.

SUB-CRITÉRIO DE AVALIAÇÃO

O subcritério de avaliação é a decomposição do critério de avaliação (em áreas de produção ou do conhecimento), facilitando o desenvolvimento de instrumentos de medição do desempenho (aspetos) de forma clara, justa e transparente.

ASPETOS (INDICADORES)

Os aspetos (indicadores de avaliação) decorrem da decomposição dos subcritérios em indicadores de desempenho esperados, vertidos numa ficha de avaliação/grelha de observação, que facilite a medição do desempenho no desenvolvimento da prova, considerando as tarefas, operações atitudes e comportamentos esperados e observáveis. Podem ser considerados aspetos a altura, ângulo, peso, nivelamento, erros, tolerâncias, tempo de execução, processo, etc.

PROVA

É o instrumento que fornece a informação necessária e específica de execução das tarefas a executar, de acordo com o perfil de emprego, áreas de competência, critérios e subcritérios de avaliação definidos (para jurados e concorrentes).

MÓDULO DA COMPETIÇÃO

Os módulos estruturam a prova, integrando, de forma organizada, um conjunto de tarefas e/ou operações afins, tendo em vista o desenvolvimento de um produto ou serviço com valor para o mercado de trabalho. O módulo de

avaliação deverá corresponder no todo ou em parte a uma área de competência. Haverá tantos módulos quantos os necessários a avaliar todas as áreas de competência.

LISTA DE INFRAESTRUTURAS, SOFTWARE E EQUIPAMENTOS

Refere-se à identificação das características das infraestruturas, ferramentas e equipamentos necessários à organização e desenvolvimento da prova.

LAYOUT-TIPO DA COMPETIÇÃO

Refere-se à organização do espaço da competição, identificando áreas e posicionamento de postos de trabalho e de áreas associadas a jurados, supervisor de infraestruturas e concorrentes.