REFERENCIAL DE CURSO

Cisco Certified Network Associate – Cybersecurity Operations

(Designação do Curso)

Código do Curso: E0191B4P

Pontos de crédito: 09

Tipologia: Especialização

Observações:

Página intencionalmente em branco

DOCUMENTO I – FICHA DE CONTROLO DO CURSO

DESIGNAÇÃO DO CURSO

☐ NOVO CURSO

Cisco Certified Network Associate – Cybersecutity Operations

BREVE DESCRIÇÃO DO MOTIVO DA REVISÃO (QUANDO APLICÁVEL)

☒ REVISÃO

DISCIPLINA NATO (SE APLICÁVEL)	**CÓDIGO DO CURSO**	**UNIDADE FORMADORA**
Outro	E0191B4P	Escola das Armas

N.º	ATIVIDADE	ENTIDADE	ASSINATURA	DATA
1	Valido a criação/revisão do Curso.	Chefe da RTEQ	Nome: Posto:	
2	Valido a Proposta de Curso (Doc II).	Subdiretor de Formação	Nome: Posto:	
3	Valido o plano de Formação (Doc III).	Chefe da RTEQ	Nome: Posto:	
4	Aprovo o Referencial de Curso.	Diretor de Formação	Nome: Posto:	
5	Aprovo a descontinuação do curso.	Diretor de Formação	Nome: Posto:	

Página intencionalmente em branco

REGISTO DE ALTERAÇÕES

DESIGNAÇÃO DO CURSO: *Cisco Certified Network Associate – Cybersecutity Operations* **CÓDIGO:** E0191B4P

IDENTIFICAÇÃO DA ALTERAÇÃO (N.º e Data)	DATA DA INTRODUÇÃO	ENTRADA EM VIGOR (Data)	IDENTIFICAÇÃO DE QUEM INTRODUZIU (Assinatura, Posto, Unidade)

Página intencionalmente em branco

E0191B4P DOCUMENTO II – PROPOSTA DE CURSO

DESIGNAÇÃO DO CURSO: *Cisco Certified Network Associate – Cybersecutiry Operations* **CÓDIGO:** E0191B4P

PARTE - 1: ESPECIFICAÇÃO DO CURSO.

1. Descrição da necessidade formativa.

Os militares da Arma de Transmissões, com responsabilidades na instalação, configuração, operação, gestão e monitorização dos Sistemas de Informação e Comunicações - Tático (SIC-T) e dos Sistemas de Informação e Comunicações - Operacional (SIC-Op), necessitam de formação altamente especializada para detetar, proteger e responder de uma forma eficaz às *cyber* ameaças.

2. Finalidade do Curso.

Habilitar os formandos com as competências necessárias para o exercício de funções como técnico ou administrador de redes de comunicação do SIC-Op e SIC-T das U/E/O de Transmissões, na área específica de cibersegurança.

3. Tipologia de Curso.

Especialização

4. Área de Educação e Formação.

863 Segurança Militar

5. Conselho Setorial para a Qualificação.

Defesa e Segurança

6. Idioma do Curso.

Português

7. Audiência Alvo.

a. Forma de Prestação de Serviço[1]:

☒ QP ☒ RCE ☒ RC ☐ RV ☐ MPCE

b. Categoria:

☒ Oficiais ☒ Sargentos ☒ Praças ☒ Civis ☐ Alunos

c. Especificação do(s) Posto(s) (se aplicável):

Nada a referir.

[1] QP – Quadro Permanente; RCE – Regime de Contrato Especial; RC – Regime de Contrato; RV – Regime de Voluntariado

d. Especificação da Arma, Serviço ou Especialidade (se aplicável):

Nada a referir.

e. Entidades Nacionais:

☒ Ramo Exército ☒ Outros Ramos ☒ Forças de Segurança ☐ Entidades Civis

f. Entidades Estrangeiras ao abrigo de relações bilaterais com Portugal:

☐ Sim ☒ Não

g. Outras especificações (se aplicável):

Na categoria de Praças, o curso só se aplica aos militares do QP ou RCE.

8. Número de Formandos por edição de curso.

a. Mínimo:

6 (seis) formandos.

b. Máximo:

12 (doze) formandos.

9. Número de formandos estimados por ano.

12 (doze) formandos.

10. Número de edições previstas por ano.

01 (uma) edição por ano.

11. Pré-Requisitos.

a. Formação:

- Possuir curso de *IT – Essentials* (ou equivalente).

b. Experiência Profissional:

-Nada a referir.

c. Proficiência Linguística:

Idioma	Compreensão da Língua Falada	Capacidade da Expressão Oral	Compreensão da Língua Escrita	Capacidade da Expressão Escrita
Inglês[2]	2	2	2	2

d. Exames

☐ Médicos ☐ Psicotécnicos ☐ Físicos

[2] Documentação de estudo e exames do curso no idioma inglês.

e. Credenciação necessária para frequentar Curso.

(1) NACIONAL:

Não Aplicável

(2) OTAN:

Não aplicável

(3) UE:

Não Aplicável

f. Outros:

Nada a referir.

12. Estratégia Formativa.

Formação presencial com a duração de 135 tempos de formação, distribuídos por 20 dias úteis de formação.

13. Validade do Curso.

Após três (3) anos sem exercer funções no âmbito desta qualificação, os formandos perdem a validade da qualificação, devendo frequentar o curso novamente.

14. Nível de Proficiência.

a. QNQ:

5

b. NATO:

300

15. Entidade(s) Formadora(s).

Regimento de Transmissões

16. Anexo(s).

Nada a referir.

PARTE - 2: PERFIL DE COMPETÊNCIAS.

Mapeamento de Unidades de Competência.

N.º	Designação da UC	Carga Horária	Pontos de Crédito	Código UC (Exército)	Código UC (CNQ)
01	Desenvolver atividades de analista de segurança num Centro de Operações de Segurança (SOC) - Parte 1.	50	4,5	E01911A	TBD
02	Desenvolver atividades de analista de segurança num Centro de Operações de Segurança (SOC) - Parte 2.	50	4,5	E01912A	TBD

UNIDADE DE COMPETÊNCIA

UC E01911A |	**TBD**	**Desenvolver atividades de analista de segurança num Centro de Operações de Segurança – Parte 1**
UFCD E01911A |	**TBD**	**Tarefas de um analista de segurança num centro de Operações de Segurança – Parte 1**

1. Pontos de Crédito.

4,5 pontos de crédito.

2. Nível de Proficiência.

a. QNQ:

5

b. NATO:

300

3. Realizações.

R1. Analisar o cenário atual em relação a *cyber* segurança.
R2. Caracterizar as funções de analista de operações de segurança cibernética numa organização.
R3. Distinguir os recursos e as características do sistema operacional *Windows* e *Linux*.
R4. Analisar a operação de protocolos e serviços de rede.
R5. Analisar o funcionamento da infraestrutura de rede.

Resultados de aprendizagem.

b. Conhecimentos:

- Características do cenário atual em relação a *cyber* segurança;
- Características da ameaça;
- Características do *Security Operations Center* (SOC);
- Características do defensor;
- Características e funcionamento de sistemas operativos *Windows* e *Linux*;
- Procedimentos de operação de protocolos e serviços de rede;
- Funcionamento de uma rede de computadores;
- Processos de comunicação de rede;
- Protocolos de comunicação;
- Procedimentos de encapsulamento de dados;
- Tarefas, deveres e responsabilidades de um analista de segurança, de nível associado, dentro de um SOC.

c. Aptidões:

- Instalar máquinas virtuais para criar um ambiente seguro para implementar e analisar eventos de ameaças à segurança cibernética;
- Utilizar os recursos do sistema operativo *Windows* e *Linux*;
- Identificar os processos de comunicação de rede;
- Operar protocolos e serviços de rede;
- Operar a infraestrutura de rede.

d. Atitudes:

- Realizar as suas funções de forma diligente e responsável, respeitando o cumprimento de ordens e regulamentos;
- Desempenhar de forma proativa e autónoma as suas tarefas;
- Ser responsável por garantir a segurança dos equipamentos e da documentação que lhe estão distribuídas ou confiadas.

4. Critérios de Desempenho.

Desenvolver atividades de analista de segurança num Centro de Operações de Segurança – Parte 1.
CD 1. Reconhecendo a evolução histórica da guerra no ciberespaço. CD 2. Identificando os agentes da ameaça. CD 3. Analisando o impacto da ameaça. CD 4. Identificando as características do SOC moderno. CD 5. Descrevendo as competências de um defensor de *cyber* segurança numa rede. CD 6. Reconhecendo a arquitetura e operação do *Windows*. CD 7. Efetuando configurações e monitorizações no *Windows*. CD 8. Percebendo a segurança do *Windows*. CD 9. Operando na *Shell* do *Linux*. CD 10. Funcionando com o sistema de arquivo de *Linux*. CD 11. Utilizando *a Graphical User Interface (GUI)* do *Linux*. CD 12. Utilizando o processo de comunicação de rede. CD 13. Identificando os protocolos de comunicação de rede. CD 14. Reconhecendo o funcionamento do encapsulamento de dados. CD 15. Cumprindo os protocolos *Ethernet* e *Internet Protocol* (IP). CD 16. Verificando a conectividade. CD 17. Cumprindo o protocolo de resolução de endereços. CD 18. Caracterizando a camada de transporte. CD 19. Distinguindo os serviços de rede. CD 20. Identificando dispositivos de comunicação de rede. CD 21. Analisando a infraestrutura de segurança de rede.

5. Contexto (Exemplos de uso da competência).

- No exercício de funções de comando e chefia das companhias de transmissões, das Repartições de Comunicações, do Departamento de Operações de Comunicações e Sistema de informações, dos Centros de Comunicações e Sistemas de informações e o do Núcleo *Computer Incident Response Capability.*

6. Recursos.

- Computador com *software* de virtualização.

7. Observações.

- Nada a referir.

8. Qualificações.

- Nada a referir.

Página intencionalmente em branco

UNIDADE DE COMPETÊNCIA

UC E01912A |	**TBD**	**Desenvolver atividades de analista de segurança num Centro de Operações de Segurança – Parte 2**
UFCD E01912A |	**TBD**	**Tarefas de um analista de segurança num Centro de Operações de Segurança – Parte 2**

1. Pontos de Crédito.

4,5 pontos de crédito.

2. Nível de Proficiência.

a. QNQ:

5

b. NATO:

300

3. Realizações.

R1. Usar ferramentas de monitorização de rede para identificar e classificar ataques contra protocolos e serviços de rede.
R2. Evitar o acesso mal-intencionado a redes, *hosts* e dados de computadores.
R3. Investigar vulnerabilidades e ataques de *endpoints*.
R4. Avaliar alertas de segurança e analisar dados de invasão de rede para identificar *hosts* e vulnerabilidades comprometidos.
R5. Aplicar modelos de resposta a incidentes para gerir incidentes de segurança de rede.

Resultados de aprendizagem.

b. Conhecimentos:

- Características dos atacantes e das suas ferramentas;
- Tipos de *Malware*;
- Tipos de ataques de rede;
- Ferramentas de monitorização de rede para identificação de ataques;
- Noções básicas de defesa;
- Acesso mal-intencionado a redes, *hosts* e dados de computadores;
- Fontes de informação e serviços da inteligência de ameaças;
- Características da criptografia;
- Funcionamento da proteção de *endpoints*;
- Processo de avaliação de vulnerabilidades e ataques de *endpoints*;
- Modelos de resposta a incidentes de segurança de rede.

c. Aptidões:

- Classificar tipos de ataques à rede;

- Usar ferramentas de monitorização de rede;
- Prevenir e evitar o acesso mal-intencionado;
- Investigar as vulnerabilidades e ataques de *endpoints*;
- Monitorizar protocolos comuns;
- Avaliar alertas de segurança;
- Analisar dados de invasão de rede;
- Trabalhar com dados de segurança de rede;
- Aplicar modelos de resposta a incidentes de segurança de redes.

d. Atitudes:

- Realizar as suas funções de forma diligente e responsável, respeitando o cumprimento de ordens e regulamentos;
- Desempenhar de forma proativa e autónoma as tarefas de analista de segurança cibernética num centro de operações de segurança (*Security Operations Center* - SOC);
- Ser responsável por garantir a segurança dos equipamentos e da documentação que lhe estão distribuídos ou confiados.

4. Critérios de Desempenho.

Desenvolver atividades de analista de segurança num Centro de Operações de Segurança – Parte 2
CD 1. Identificando o invasor e suas ferramentas. CD 2. Reconhecendo as ameaças e ataques comuns. CD 3. Controlando a monitorização de rede. CD 4. Utilizando ferramentas de monitorização. CD 5. Entendendo como os recursos de protocolos são usados para ataques cibernéticos. CD 6. Identificando os recursos que são mais suscetíveis de ser atacados. CD 7. Aplicando noções básicas de defesa de redes. CD 8. Implementando medidas de controlo de acesso. CD 9. Analisando a inteligência da ameaça. CD 10. Implementando a criptografia. CD 11. Protegendo *endpoints.* CD 12. Avaliando vulnerabilidades de *endpoints.* CD 13. Analisando como os protocolos de rede interagem e impactam a monitorização da segurança de rede. CD 14. Interpretando dados de segurança de rede. CD 15. Avaliando alertas de intrusão. CD 16. Trabalhando com dados de segurança de rede. CD 17. Conhecendo o funcionamento da computação forense digital. CD 18. Analisando evidências. CD 19. Implementando modelos de resposta a incidentes.

5. Contexto (Exemplos de uso da competência).

- No exercício de funções de comando e chefia das companhias de transmissões, das Repartições de Comunicações, do Departamento de Operações de Comunicações e Sistema de informações, dos Centros de Comunicações e Sistemas de informações e o do Núcleo *Computer Incident Response Capability*.

6. Recursos.

- Computador com *software* de virtualização.

7. Observações.

- Nada a referir.

8. Qualificações.

- Nada a referir.

Página intencionalmente em branco

DOCUMENTO III – PLANO DE FORMAÇÃO

DESIGNAÇÃO DO CURSO: *Cisco Certified Network Associate – Cybersecurity Operations*

CÓDIGO: E0191B4P

PARTE - 1: PERFIL DE FORMAÇÃO.

1. Mapeamento de Unidades de Formação de Curta Duração.

NO	Unidades de Competência				Unidades de Formação de Curta Duração				CH	PC
1	**EXE**	E01911A	**CNQ**	TBD	**EXE**	E01911A	**CNQ**	TBD	50	4,5
	Desenvolver atividades de analista de segurança num Centro de Operações de Segurança (SOC) - Parte 1				Tarefas de um analista de segurança num Centro de Operações de Segurança (SOC) – Parte 1					
2	**EXE**	E01912A	**CNQ**	TBD	**EXE**	E01912A	**CNQ**	TBD	50	4,5
	Desenvolver atividades de analista de segurança num Centro de Operações de Segurança (SOC) - Parte 2				Tarefas de um analista de segurança num Centro de Operações de Segurança (SOC) – Parte 2					

Legenda: NO – Número de Ordem; EXE – Código do Exército; CNQ – Código do Catálogo Nacional de Qualificações; CH – Carga Horária; PC – Pontos de Crédito.

2. Carga horária complementar

Atividade	TF
Cerimónia de abertura	1
Procedimentos administrativos	2
Treino físico	8
Reforço da formação	18
Preparação de máquinas virtuais	2
Desmontagem de laboratórios	1
Correção de testes	2
Cerimónia de encerramento	1
Total	**35**

3. Descriminação da Carga horária.

a. A distância:

Nada a referir.

b. Presencial:

135 tempos de formação.

c. Total:

135 tempos de formação.

4. Dias Úteis de Formação.

a. A distância:

Nada a referir.

b. Presencial:

20 (vinte) dias úteis.

c. Total:

20 (vinte) dias úteis.

5. Total de Pontos de Crédito do curso.

09 pontos de crédito.

6. Estágios.

a. Finalidade:

Nada a referir.

b. Duração:

Nada a referir.

c. Avaliação:

Nada a referir.

7. Classificação Final do curso (fórmula de avaliação).

a. $CF = \frac{\text{Class na UFCD.E01911A + Class na UFCD.E01912A}}{2}$

b. Considerando a alínea d. do número 308. da PAD 240-01 Regulamento da Formação, "para efeitos de certificação por entidade externa podem ser admitidas outras escalas de avaliação, desde que autorizadas pelo Diretor de Formação". O aproveitamento é obtido consoante as seguintes condições:

1) Classificação final igual ou superior a 70%, na escala de 0 - 100%;
2) Em todas as avaliações é aplicada a obtenção de nota mínima de 70%;
3) Em caso de reprovação em alguma avaliação, existe a possibilidade de repetir essa avaliação, ficando o formando com a nota máxima de 70% nessa avaliação;
4) A repetição de uma avaliação apenas pode ocorrer uma vez durante todo o curso;
5) As repetições são realizadas no final de todas as outras avaliações;
6) Em caso de reprovação em duas avaliações os formandos ficam automaticamente eliminados do curso.

8. Anexos.

Anexo: Horário-tipo

PARTE - 2: CUSTOS DA FORMAÇÃO.

1. Mapeamento dos Custos da Formação.

01	FCF	Tarefas de um analista de segurança num Centro de Operações de Segurança (SOC) – Parte 1	Código	FCF.E01911A1
	Imputáveis à Fazenda Nacional	Imputáveis à Entidade Formadora	P/ Formando do Exército	P/ Formando Externo
	11 560,33 €	361,17 €	963,36 €	207,14 €
02	FCF	Tarefas de um analista de segurança num Centro de Operações de Segurança (SOC) – Parte 2	Código	FCF.E01912A1
	Imputáveis à Fazenda Nacional	Imputáveis à Entidade Formadora	P/ Formando do Exército	P/ Formando Externo
	11 560,33 €	361,17 €	963,36 €	207,14 €

2. Resumo dos custos afetos ao curso.

a. Total de Custos Imputáveis à Fazenda Nacional.

23 120,66 €

b. Total de Custos Imputáveis à Entidade Formadora.

722,34 €

c. Total de Custos por Formando do Exército.

1 926,72 €

d. Total de Custos por Formando Externo.

414,28 €

Página intencionalmente em branco

UNIDADE DE FORMAÇÃO DE CURTA DURAÇÃO

UC E01911A |	**TBD**	**Desenvolver atividades de analista de segurança num Centro de Operações de Segurança - Parte 1**
UFCD E01911A |	**TBD**	**Tarefas de um analista de segurança num Centro de Operações de Segurança – Parte 1**

1. Carga Horária.

50 horas.

2. Pontos de Crédito.

4,5 pontos de crédito.

3. Nível de Proficiência.

a. QNQ:

5

b. NATO:

300

4. Objetivos de Aprendizagem.

OA1. Analisar o cenário atual em relação a *cyber* segurança.
OA2. Caracterizar as funções do soldado na guerra contra o crime digital.
OA3. Distinguir os recursos e as características do sistema operacional *Windows* e *Linux*.
OA4. Analisar a operação de protocolos e serviços de rede.
OA5. Analisar a operação da infraestrutura de rede.

5. Especificação da Formação.

CONTEÚDOS	MÉTODO	TFD	TFN	EAD	EXC	REFERÊNCIAS
OA1. Analisar o cenário atual em relação a *cyber* segurança.						
OE1.1. Reconhecer a evolução histórica da guerra no ciberespaço. 1.1.1. Pessoas sequestradas. 1.1.2. Empresas resgatadas. 1.1.3. Nações-alvo. 1.1.4. Anatomia de um ataque.	Expositivo	1		☐	☐	A: Módulo 1
OE1.2. Caracterizar a ameaça. 1.2.1. Agentes da ameaça: – Segurança da *Internet of Things* (IoT); – Detalhes de um ataque. 1.2.2. Impacto da ameaça. 1.2.3. Conjuntos de informações. 1.2.4. Vantagem competitiva perdida. 1.2.5. Política e segurança nacional.	Expositivo	1		☐	☐	A: Módulo 1
OA2. Caracterizar as funções do soldado na guerra contra o crime digital.						
OE2.1. Caracterizar o *Security Operations Center (SOC)*	Expositivo	1		☐	☐	A: Módulo 2

	2.1.1. Componentes de um SOC. 2.1.2. Pessoas no SOC. 2.1.3. Processos no SOC. 2.1.4. Tecnologias no SOC (SIEM e SOAR). 2.1.5. Métricas SOC. 2.1.6. Segurança corporativa. 2.1.7. Segurança versus disponibilidade.						
	OE2.2. Formar um defensor. 2.2.1. Certificações. 2.2.2. Aprofundar conhecimentos. 2.2.3. Informações sobre a carreira. 2.2.4. Obter experiência. 2.2.5. Como ser um defensor.	Expositivo	1		☐	☐	A: Módulo 2
OA3. Distinguir os recursos e as características do sistema operacional *Windows e Linux*.							
	OE3.1. Utilizar os recursos do sistema operativo *Windows*. 3.1.1. História do Windows: – Sistema operativo de disco; – Versão do *Windows*; – *Graphical User Interface (GUI)* do *Windows*; – Vulnerabilidades do sistema. 3.1.2. Arquitetura e operações do Windows: – Camada de abstração de *hardware*; – Modo de utilizador e modo *kernel*; – Sistema de arquivos do *Windows*; – Fluxo de dados alternativos; – Arranque do *Windows*; – Encerramento do *Windows*; – Processos, ameaças e serviços; – Alocação e identificadores de memória; – O registro do *Windows*. 3.1.3. Configuração e monitorização do *Windows*: – Execução como administrador; – Utilizadores e domínios locais; – *Command Line Interface (CLI)* e *PowerShel*l; – Instrumentos de gestão do *Windows*; – Gestor de tarefas; – Redes e recursos de redes; – Servidor *Windows*. 3.1.4. Configuração de segurança do *Windows*: – O comando *netstat*; – Visualizador de eventos; – *Windows Update*; – Política de segurança local; – Firewall do Windows defender.	Demonstrativo	3		☐	☐	A: Módulo 3
	OE3.2. Utilizar os recursos do sistema operativo *Linux*. 3.2.1. Conceitos de básicos de *Linux*: – O que é *Linux*; – O valor do *Linux*;	Demonstrativo	5		☐	☐	A: Módulo 4

	– Linux no SOC; – Ferramentas *Linux*. 3.2.2. Linux Shell: – O Shell do *Linux*; – Comandos básicos; – Comandos de arquivo e diretório; – Trabalhar com arquivos de texto; – Importância dos arquivos de texto no *Linux*. 3.2.3. Servidores e clientes *Linux:* – Introdução às comunicações Cliente-Servidor; – Servidores, serviços e suas portas; – Clientes. 3.2.4. Administração do servidor: – Arquivos de configuração de serviço; – Fortalecimento de dispositivos (*hardering*); – *Logs* de serviço de monitorização. 3.2.5. Sistema de arquivos *Linux*: – Tipos de sistema de arquivos no Linux; – Funções do Linus e permissões de arquivo; – Links rígidos e links simbólicos. 3.2.6. *GUI Linux:* – *Sistema X Windows;* – *A GUI do Linux.* 3.2.7. *Host Linux:* – *Instalação e execução de aplicações num host Linux;* – *Manter o sistema atualizado;* – *Processos e Forks;* – *Malware num host Linux;* – *Verificação de RootKit;* – *Comandos de piping.*						
OA4. Analisar a operação de protocolos e serviços de rede.							
OE4.1. Identificar os processos de comunicação de rede. 4.1.1. Redes de vários tamanhos. 4.1.2. Comunicações cliente servidor. 4.1.3. Sessões típicas. 4.1.4. Traçar o caminho.		Expositivo	1		☐	☐	A: Módulo 5
OE4.2. Descrever os protocolos de comunicação. 4.2.1. O que são protocolos. 4.2.2. Protocolos e a rede. 4.2.3. Conjunto de protocolos *Transmission Control Protocol /Internet Protocol (TCP/IP).* 4.2.4. Formatação e encapsulamento de mensagens. 4.2.5. Tamanho da mensagem. 4.2.6. Temporização de mensagem. 4.2.7. *Unicast, broadcast* ou *multicast*.		Expositivo	2		☐	☐	A: Módulo 5

	4.2.8. Benefícios de usar um modelo em camadas. 4.2.9. Modelo de referência *Open System Interconnection (OSI).* 4.2.10. Modelo de protocolo TCP/IP.						
	OE4.3. Descrever o encapsulamento de dados. 4.3.1. Segmentação de mensagens. 4.3.2. Sequenciamento. 4.3.3. *Protocol Data Unit (PDU).* 4.3.4. Três endereços. 4.3.5. Exemplo de encapsulamento. 4.3.6. Exemplo e desencapsulamento. 4.3.7. Introdução ao *Wireshark*.	Expositivo	2		☐	☐	A: Módulo 5
OA5. Analisar a operação da infraestrutura de rede.							
	OE5.1. Conhecer os protocolos *Ethernet* e *Internet Protocol (IP).* 5.1.1. Protocolo *Ethernet*: – Encapsulamento *Ethernet*; – Campos de um quadro *Ethernet*; – Formato do endereço *MAC-Address.* 5.1.2. Protocolo Internet Protocol (IP)v4: – A camada de rede; – Encapsulamento IP; – Características IP; – Cabeçalho do pacote IPv4; – Campos do cabeçalho de pacote IPv4. 5.1.3. Noções básicas de endereçamento IP: – Partes de rede e de host; – A máscara de sub-rede; – Comprimento do prefixo; – Determinar a rede (lógica AND); – Endereços de rede, hots e broadcast; – Sub redes e domínios de Broadcast. 5.1.4. Tipos de endereços IPv4: – Classes de endereços IPv4 e máscaras de sub-rede padrão; – Endereços privados reservados. 5.1.5. Configuração do *default gateway:* – Decisão de encaminhamento do *host*; – *Default Gateway*; – Tabelas de roteamento dos *hosts*. 5.1.6. Protocolo IPv6: – Necessidade de IPv6; – Formatos de endereços IPv6; – Regras de escrita; – Comprimentos do prefixo; – Endereçamento de camada 2 e camada 3.	Expositivo	5		☐	☐	A: Módulo 6
	OE5.2. Verificar a conectividade entre dispositivos. 5.2.1. *Internet Control Message Protocol (ICMP):* – Mensagens ICMPv4; – Mensagens ICMPv6. 5.2.2. Comando *Ping* e *Traceroute*: – Teste de conectividade;	Demonstrativo	2		☐	☐	A: Módulo 7

	– *Ping* ao *loopback, defautl gateway* e a um *host* remoto; – *Traceroute*; – Formato de pacote ICMP.						
	OE5.3. Descrever o protocolo de resolução de endereços. 5.3.1. Diferenciação MAC e IP: – Destino na mesma rede; – Destino em rede remota. 5.3.2. *Address Resolution Protocol (ARP):* – Visão geral do ARP; – Funções do ARP; – Operação ARP; – Remoção de entradas numa tabela ARP; – Tabela ARP. 5.3.3. Problemas do ARP: – Transmissão de ARP; – Falsificação de ARP.	Expositivo	3		☐	☐	A: Módulo 8
	OE5.4. Caracterizar a camada de transporte. 5.4.1. Camada de transporte: – Propósito da camada de transporte; – Responsabilidades da camada de transporte; – Protocolos da camada de transporte; – Transmission Control Protocol (TCP); – User Datagram Protocol (UDP); – Pares de sockets. 5.4.2. Sessão na camada de transporte: – Processos em servidores TCP; – Estabelecimento de conexão TCP; – Encerramento da sessão; – Análise do Handshake Triplo do TCP. 5.4.3. Confiabilidade da camada de transporte: – Entrega garantida e solicitada; – Números de sequência e reconhecimentos; – Perda de dados e retransmissão; – Tamanho da janela e confirmações; – Tamanho máximo do segmento; – Prevenção de congestionamentos.	Expositivo	3		☐	☐	A: Módulo 9
	OE5.5. Descrever os serviços de rede. 5.5.1. *Dynamic Host Configuration Protocol (DHCP):* – Protocolo DHCP; – Operação DHCP; Formato da mensagem de DHCP. 5.5.2. Protocolo *Domain Name System* (DNS): – A hierarquia de domínio DNS; – O processo de pesquisa de DNS; – Formato de mensagem DNS, – DNS dinâmico. 5.5.3. Protocolo Network *Address Translation:* – Espaço de endereços privados IPv4;	Expositivo	5		☐	☐	A: Módulo 10

	– O que é o NAT; – Como funciona o NAT; – Port Address Translation (PAT). 5.5.4. Serviços de transferência e de partilha de arquivos: – File Transfer Protocol (FTP); – Trivial File Transfer Protocol (TFTP); – Server Message Block (SMB). 5.5.5. Protocolos de *E-mail*: – Simple Mail Transfer Protocol (SMTP); – Post Office Protocol (POP); – Internet Message Acess Protocol (IMAP. 5.5.6. *Hypertext Transfer Protocol (HTTP)*: – Protocolo HTTP e Hypertex Markup Language (HTML); – Uniform Resource Locator (URL); – Operação HTTP; – Código de status HTTP; – HTTP/2; – Protegendo HTTP – HTTPSecure.						
OE5.6. Identificar os dispositivos de comunicação de rede.							
5.6.1. Dispositivos de rede: – Dispositivos finais; – Routers; – Endereçamento de camada 2 e camada 3; – Processo de decisão de encaminhamento de pacotes; – Informação de roteamento; – Encaminhamento ponto a ponto; – Roteamento estático e dinâmico; – Hubs, Bridges, switches; – Operação de switching; – Tabelas de endereços MAC em switches; – Virtual Local Area Network (VLANs); – Spanning Tree Protocol (STP); – Comutação Multilayer. 5.6.2. Comunicações sem fio: – Local Area Netwirk (LAN) sem fio versus com fio; – Estrutura de frame 802.11; – Carrier Sense Miltiple Access Colision Avoidance (CSMA/CA); – Associação de cliente sem fio e ponto de acesso; – Modo de descoberta passiva e ativa; – Dispositivos sem fio – Access Point (AP), Lightwieght Access Point (LWAP) e Wireless LAN Controller (WLC).	Expositivo	2		☐	☐	A: Módulo 11
OE5.7. Conhecer a infraestrutura de segurança de rede.							
5.7.1. Tipologias de rede: – Representação de rede;	Expositivo	3		☐	☐	A: Módulo 12

	– Diagramas de topologia; – Redes de vários tamanhos; – LAN e Wide Area Network (WAN). – O modelo de design de rede de três camadas. – Arquiteturas de segurança comuns. 5.7.2. Dispositivos de segurança: – Firewalls; – Descrição de tipo de firewall; – Dispositivos de prevenção e deteção de intrusão; – Vantagens e desvantagens de Intrusion Detection Systems (IDS) e Intrusion Prevention Systems (IPS); – Tipos de IPS; – Dispositivos de segurança especializados. 5.7.3. Serviços de segurança: – Controlo de tráfego com Access Control List (ACL); – ACLs – Recursos importantes; – Simple Network Management Protocol (SNMP); – NetFlow; – Espelhamento de portas; – Servidores Syslog; – Network Time Protocol (NTP); – Servidores de Authentication, Authorization, Accounting (AAA); – Virtual Private Network (VPN).						
Outras Atividades							
	Avaliação: Teste escrito (*Cisco Practice Final Exam*). Avaliação: Teste escrito (*Cisco Final Exam*). Avaliação: Teste escrito (RTm *Quiz*). Avaliação: Prova prática (*Hands-on Skills Exam Cisco*). Avaliação: Prova prática (*Hands-on Skills Lab Mix*). Avaliação: Prova prática (*Hands-on Skills Exam* RTm). Avaliação: Prova prática de treino (*Hand-on game mission*).		10				

Legenda: TFD – Tempos de Formação Diurnos; TFN – Tempos de Formação Noturnos; EAD- Ensino a Distância; ExC – Exercícios de Campo.

6. Especificação da Carga Horária.

a. Formação presencial:

50 tempos de formação.

b. Formação não presencial:

Nada a referir.

7. Critérios de avaliação.

Correspondem aos critérios de desempenho da Unidade de Competência.

8. Referências.

A: Curso de *CyberOps Associate* da Plataforma *Cisco NetAcad*.

9. Formadores.

a. Requisitos de formação:

- Possuir o curso de Formação Pedagógica Inicial de Formadores;
- Possuir o curso de *Cisco Certified Network Associate* (CCNA);
- Possuir o curso de *Cyber Ops Associate*;
- Certificação profissional Cisco *Cybersecurity Operations Associate* (*CBROPS)* 200-201 ou *CCNA* 200-301.

b. Experiência profissional:

- Nada a referir.

c. Outros requisitos:

Proficiência Linguística:

Idioma	Compreensão da Língua Falada	Capacidade da Expressão Oral	Compreensão da Língua Escrita	Capacidade da Expressão Escrita
Inglês	2	2	2	2

10. Classificação final da UFCD (fórmula de avaliação).

a. Class da UFCD = $\frac{10*PFE + 10*FE + 20*RTQ + 20*CL + 20*RTL + 20*LM}{100}$

PFE – *Cisco Practice Final Exam*
FE – *Cisco Final Exam*
RTQ – *RTm Quiz*
CL – *Cisco Lab Skills Assessment*
RTL – *RTm Lab Skills Assessment*
LM – *Lab Mix Skills Assessment*

b. Considerando a alínea d. do número 308. da PAD 240-01 Regulamento da Formação, "para efeitos de certificação por entidade externa podem ser admitidas outras escalas de avaliação, desde que autorizadas pelo Diretor de Formação". O aproveitamento é obtido consoante as seguintes condições:

1) Classificação final igual ou superior a 70%, na escala de 0 - 100%;
2) Em todas as avaliações é aplicada a obtenção de nota mínima de 70%;
3) Em caso de reprovação em alguma avaliação, existe a possibilidade de repetir essa avaliação, ficando o formando com a nota máxima de 70% nessa avaliação;

4) A repetição de uma avaliação apenas pode ocorrer uma vez durante todo o curso;
5) As repetições são realizadas no final de todas as outras avaliações;
6) Em caso de reprovação em duas avaliações, os formandos ficam automaticamente eliminados do curso.

11. Observações.

- Nada a referir

Página intencionalmente em branco

UNIDADE DE FORMAÇÃO DE CURTA DURAÇÃO

UC	**E01912A | TBD**	**Desenvolver atividades de analista de segurança num Centro de Operações de Segurança - Parte 2**
UFCD	**E01912A | TBD**	**Tarefas de um analista de segurança num Centro de Operações de Segurança - Parte 2**

1. Carga Horária.

50 horas.

2. Pontos de Crédito.

4,5 pontos de crédito.

3. Nível de Proficiência.

a. QNQ:

5

b. NATO:

300

4. Objetivos de Aprendizagem.

OA1. Usar as ferramentas de monitorização de rede para identificar e classificar ataques contra protocolos e serviços de rede.
OA2. Evitar o acesso mal-intencionado a redes, *hosts* e dados de computadores.
OA3. Investigar vulnerabilidades e ataques de *endpoints*.
OA4. Avaliar alertas de segurança e analisar dados de invasão de rede para identificar *hosts* e vulnerabilidades comprometidos.
OA5. Aplicar modelos de resposta a incidentes para gerir incidentes de segurança de rede.

5. Especificação da Formação.

CONTEÚDOS	MÉTODO	TFD	TFN	EAD	EXC	REFERÊNCIAS
OA1. Usar ferramentas de monitorização de rede para identificar e classificar ataques contra protocolos e serviços de rede.						
OE1.1. Identificar características dos atacantes e das suas ferramentas. 1.1.1. Quem ataca a nossa rede: – Ameaça, vulnerabilidade e risco; – Hacker vs. Ameaças; – Evolução dos atores de ameaças; – Cyber criminosos; – Tarefas de cyber segurança; – Indicadores de ameaças cibernéticas; – Partilha de ameaças e criação de conscientização. 1.1.2. Ferramentas do agente da ameaça: – Introdução de ferramentas de ataques; – Evolução de ferramentas de segurança; – Categorias de ataques.	Expositivo	1		☐	☐	A: Módulo 13

OE1.2. Identificar ameaças e ataques comuns. 1.2.1. Tipos de *Malware*: – Vírus; – Cavalos de Troia; – *Worms*; – *Ransomware*; – Outro *Malwares*; – Comportamentos comuns de *Malware*. 1.2.2. Ataques de redes comuns: – Tipos de ataques de rede; – Ataques de reconhecimento; – Ataques de acesso; – Ataques de engenharia social; – Fortalecimento do elo mais fraco. 1.2.3. Outros ataques de rede: – Ataques de *Denial of Service* (DoS); – Ataques *de Distributed DoS*. (DDoS); – Ataques de Buffer *Overflow*; – Métodos de evasão.	Expositivo	2		☐	☐	A: Módulo 14
OE1.3. Usar ferramentas de monitorização de rede. 1.3.1. Monitorização de uma rede IP: – Topologia de segurança de rede; – Métodos de monitorização de rede; – *Taps* de rede; – *Port mirroring* e *Switch Port Analyzer* (SPAN). 1.3.2. Ferramentas de monitorização de rede: – Ferramentas de monitorização de segurança; – Analisadores de protocolo; – NetFlow; – Security information Event Management (SIEM) e Security Orchestration Automation and Response (SOAR); – Sistemas SIEM.	Demonstrativo	1		☐	☐	A: Módulo 15
OE1.4. Descrever um ataque na base. 1.4.1. Campos do *Protocol Data Unit (PDU) IP*: – IPv4 e IPv6; – Cabeçalho do pacote IPv4; – Cabeçalho do pacote IPV6. 1.4.2. Vulnerabilidades *IP:* – Ataques (*Internet Control Message Protocol* (ICMP); – Ataques de amplificação, reflexão; – Ataques de falsificação de endereços. 1.4.3. Vulnerabilidades *Transmission Control Protocol (*TCP*)* e *User Datagram Protocol (*UDP*):* – Cabeçalho do segmento TCP; – Serviços TCP; – Ataques TCP; – Operação e cabeçalho do segmento UDP; – Ataques UDP.	Expositivo	2		☐	☐	A: Módulo 16
OA2. Evitar o acesso mal-intencionado a redes, *hosts* e dados de computadores.						
OE2.1. Identificar as vulnerabilidades dos serviços corporativos.	Expositivo	2		☐	☐	A: Módulo 17

	2.1.1. Serviços IP: – Vulnerabilidades *Address Resolution Protocol* (ARP); – Envenenamento e cache ARP; – Ataque de *Domain Name Service* (DNS); – Tuneis DNS; – *Dynamic Host Configuration Pro*tocol (DHCP); – Ataques ao DHCP. 2.1.2. Serviços corporativos: – *Hypertext Transfer Protocol (HTTP) e HTTPSecure*; – Explorações HTTP comuns; – E-mail; – Banco de dados expostos pela Web; – Scripts do lado do cliente; – Atacar um banco de dados *MySQL*; – Leitura de *logs* do servidor.						
	OE2.2. Descrever as noções básicas de defesa.						
	2.2.1. Montagem de defesa em profundidade: – Ativos; – Vulnerabilidades; – Ameaças; – A segurança *Onion* e *Artichoke*. 2.2.2. Políticas, regulamentos e padrões de segurança: – Políticas de negócios; – Política de segurança; – Políticas BYOD; – Conformidade com regulamentos e padrões.	Expositivo	2		☐	☐	A: Módulo 18
	OE2.3. Descrever os conceitos de controlo de acesso.						
	2.3.1. Conceitos de controlo de acesso: – Segurança das comunicações – *Confidentiality, Integrity, Avaiability* (CIA); – Segurança Zero Trust; – Modelos de controlo de acesso. 2.3.2. Utilização e operação *do Authentication, Authorization, Accounting (AAA):* – Operação AAA; – Autenticação; – Registos de contabilidade.	Expositivo	2		☐	☐	A: Módulo 19
	OE2.4. Conhecer a inteligência de ameaças.						
	2.4.1. Fontes de informação: – Comunidades de inteligência de rede; – Relatórios de segurança cibernética da Cisco; – Blogs *e podcasts* de segurança. 2.4.2. Serviços de inteligência de ameaças. – *Cisco Talos*; – *FireEye*; – Partilha automática de indicadores; – Banco de dados de inteligência de ameaças; – Padrões de comunicação de inteligência de ameaças; – Plataformas de inteligência de ameaças.	Expositivo	2		☐	☐	A: Módulo 20

OE2.5. Entender criptografia. 2.5.1. Integridade e autenticidade: – Comunicações seguras; – Funções criptográficas de *hash*; – Operação de *hash* criptográfico; – *Message-Digest Algotithm* (MD5) e *Secure Hash Algorithm* (SHA); – Autenticação da origem. 2.5.2. Confidencialidade: – Sigilo dos dados; – Criptografia simétrica; – Criptografia assimétrica; – Confidencialidade, autenticação e integridade; – Diffie-Hellman (DH). 2.5.3. Criptografia de chave pública: – Uso de assinaturas digitais; – Assinaturas digitais para assinatura de código; – Assinaturas digitais para certificados digitais. 2.5.4. Autoridades e o sistema de confiança *Public Key Infrastructure* (PKI): – Gestão de chave pública; – A infraestrutura de chave pública; – O sistema de autoridade PKI; – O sistema de confiança PKI; – Interoperabilidade de diferentes fornecedores de PKI; – Inscrição, autenticação e revogação de certificados. 2.5.5. Aplicações e impactos da criptografia: – Aplicações PKI; – Transações de rede criptográfica; – Criptografia e monitorização de segurança.	Expositivo	3		☐	☐	A: Módulo 21
OA3. Investigar vulnerabilidades e ataques de *endpoints*.						
OE3.1. Descrever o funcionamento da proteção de *endpoints*. 3.1.1. Proteção *antimalware*: – Ameaças de *endpoints*; – Segurança de *endpoints*; – Proteção contra *malware* baseada em *host*; – Proteção contra *malware* com base na rede. 3.1.2. Prevenção de intrusão baseada em *host*: – *Firewalls* baseadas em *host*; – Deteção de intrusão baseada em *host*; – Operação *Host-based Intrusion Detection System* (HIDS); – Produtos HIDS. 3.1.3. Segurança das aplicações: – Superfície de ataque; – Lista negra e lista branca de aplicações; – *Sandboxing* baseado em sistema.	Expositivo	3		☐	☐	A: Módulo 22
OE3.2. Avaliar as vulnerabilidades de *endpoints*. 3.2.1. Perfil de rede e servidor: – Perfil de rede.	Demonstrativo	4		☐	☐	A: Módulo 23

	– Perfil de servidor. – Deteção de anomalias de rede. – Teste de vulnerabilidades de rede. 3.2.2. Sistema de pontuação de vulnerabilidades *Common Vulnerability Scoring System (*CVSS): – Visão geral do CVSS; – Grupos métricos CVSS; – Grupo métrico base CVSS; – O processo CVSS; – Relatórios CVSS; – Outras fontes de informação sobre vulnerabilidades. 3.2.3. Gestão segura de dispositivos: – Gestão de risco; – Gestão de vulnerabilidades; – Gestão de ativos; – Gestão de dispositivos móveis; – Gestão de configurações; – Gestão corporativa de *pacthes*; – Técnicas de gestão de *patches*. 3.2.4. Sistemas de gestão de segurança da informação: – Sistemas de gestão de segurança; – *International Organization for Standardization* (ISO)-27001; – *National Institute of Standards and Technology* (NIST) *Cybersecurity Framework*.						
OA4. Avaliar alertas de segurança e analisar dados de invasão de rede para identificar hosts e vulnerabilidades comprometidos.							
OE4.1. Monitorizar protocolos comuns. 4.1.1. Monitorização de protocolos comuns: – *Syslog e Network Time Protocol* (NTP); – NTP; – DNS; – HTTP e HTTPSecure; – Protocolos de *e-mail*; – ICMP. 4.1.2. Tecnologias de segurança: – *Access Control List* (ACL); – *Network Address Translation* (NAT) e *Port Address Translation* (PAT); – Criptografia, encapsulamento e desencapsulamento; – Rede ponto a ponto e Tor; – Balanceamento de carga.	Demonstrativo	2		☐	☐	A: Módulo 24
OE4.2. Analisar dados de segurança de rede. 4.2.1. Tipos de dados de segurança: – Dados de alerta; – Dados de sessão e transação; – Capturas de pacotes completos; – Dados estatísticos. 4.2.2. Registo de dispositivos de dados: – *Logs* de *host*; – Syslog;	Demonstrativo	3		☐	☐	A: Módulo 25

	– *Logs* do servidor; – *Security Infromation and Event Management* (SIEM) e coleta de *logs*. 4.2.3. *Logs* de rede: – *TCPdump*. – *NetFlow*. – Visibilidade e controlo da aplicação. – *Logs* de filtro de conteúdo. – Registo de dispositivos Cisco. – *Logs* de *proxy*. – *Cisco Firepower*. – *Tracking* de pacotes.						
	OE4.3. Avaliar alertas. 4.3.1. Fontes de alertas: – *Security Onion*; – Ferramentas de deteção para coleta de dados de alerta; – Ferramentas de análise; – Geração de alertas; – Regras e alertas; – Estrutura de regra *Snort*. 4.3.2. Visão geral da avaliação de alerta: – Necessidade de avaliação de alerta; – Avaliação de alertas; – Análise determinística e analise probabilística.	Demonstrativo	3		☐	☐	A: Módulo 26
	OE4.4. Trabalhar com dados de segurança de rede. 4.4.1. Plataforma de dados comuns: – *Elasticsearch, Logstash and Kibana* (ELK); – Redução de dados; – Normalização de dados; – Arquivamento de dados. 4.4.2. Investigação de dados de rede: – Trabalhar em *Sguil*; – Consultas *Sguil*; – Pivotante a partir de *Sguil*; – Manipulação de eventos *Sguil*; – Trabalhar no ELK; – Consultas no ELK; – Investigar chamadas de processo ou *Application Programming Interface* (API); – Investigar detalhes do arquivo; – Isolar *host* comprometido; – Investigar uma exploração de *malware*; – Investigar um ataque a um *host* Windows. 4.4.3. Trabalho do analista de dados: – Painéis e visualizações; – Gestão do fluxo de trabalho.	Demonstrativo	3		☐	☐	A: Módulo 27
OA5. Aplicar modelos de resposta a incidentes para gerir incidentes de segurança de rede.							
	OE5.1. Caracterizar a computação forense digital e análise e resposta a incidentes. 5.1.1. Manuseio de evidências e atribuição de ataque: – Perícia digital; – O processo forense digital;	Expositivo	2		☐	☐	A: Módulo 28

	– Tipos de evidência; – Ordem de colheita de evidências; – Cadeia de custódia; – Integridade e preservação dos dados; – Atribuição de ataque; – A estrutura MITRE *Adversarial Tactics, Techniques & Common Knowledge* (ATT&CK). 5.1.2. *Cyber kill chain:* – Etapas da cyber *kill chain*; – Reconhecimento; – Armamento; – Entrega; – Exploração; – Instalação; – Comando e controlo; – Ações sobre os objetivos. 5.1.3. Modelo Diamond de análise de intrusão: – Visão geral do modelo Diamond; – Pivotante em todo o modelo Diamond; – O modelo Diamond e a *Cyber Kill Chain*. 5.1.4. Resposta a incidentes: – Estabelecimento de um recurso de resposta; – Partes interessadas da resposta; – Ciclo de vida de resposta a incidentes do NIST; – Preparação, deteção e análise; – Contenção, erradicação e recuperação; – Atividades pós-incidente; – Coleta e retenção de dados de incidentes; – Requisitos de relatórios e partilha de informações.						
OE5.2. Responder a incidentes. 5.2.1. Estabelecimento de um recurso de resposta. 5.2.2. Partes interessadas da resposta. 5.2.3. Ciclo de vida de resposta a incidentes do NIST. 5.2.4. Preparação, deteção e análise. 5.2.5. Contenção, erradicação e recuperação. 5.2.6. Atividades pós-incidente. 5.2.7. Coleta e retenção de dados de incidentes. 5.2.8. Requisitos de relatórios e partilha de informações.		Demonstrativo	3		☐	☐	A: Módulo 28
Outras Atividades							
Avaliação: Teste escrito (*Cisco Practice Final Exam*). Avaliação: Teste escrito (*Cisco Final Exam*). Avaliação: Teste escrito (RTm *Quiz*). Avaliação: Prova prática (*Hands-on Skills Exam Cisco*). Avaliação: Prova prática (*Hands-on Skills Lab Mix*). Avaliação: Prova prática (*Hands-on Skills Exam* RTm). Avaliação: Prova prática de treino (*Hand-on game mission*).			10				

Legenda: TFD – Tempos de Formação Diurnos; TFN – Tempos de Formação Noturnos; EAD- Ensino a Distância; ExC – Exercícios de Campo.

6. Especificação da Carga Horária.

a. Formação presencial:

50 tempos de formação.

b. Formação não presencial:

Nada a referir.

7. Critérios de avaliação.

Correspondem aos critérios de desempenho da Unidade de Competência.

8. Referências.

A: Curso *CyberOps Associate* da Plataforma *Cisco NetAcad*.

9. Formadores.

a. Requisitos de formação:

- Possuir o curso de Formação Pedagógica Inicial de Formadores;
- Possuir o curso de *Cisco Certified Network Associate*;
- Possuir o curso *Cyber Ops Associate*;
- Certificação profissional CBROPS 200-201 ou CCNA 200-301.

b. Experiência profissional:

- Nada a referir.

c. Outros requisitos:

Proficiência Linguística:

Idioma	Compreensão da Língua Falada	Capacidade da Expressão Oral	Compreensão da Língua Escrita	Capacidade da Expressão Escrita
Inglês	2	2	2	2

10. Classificação final da UFCD (fórmula de avaliação).

a. $$\frac{\text{Class da UFCD} = 10*PFE + 10*FE + 20*RTQ + 20*CL + 20*RTL + 20*LM}{100}$$

PFE – *Cisco Practice Final Exam*
FE – *Cisco Final Exam*
RTQ – RTm *Quiz*
CL – *Cisco Lab Skills Assessment*
RTL – RTm *Lab Skills Assessment*
LM – *Lab Mix Skills Assessment*

b. Considerando a alínea d. do número 308. da PAD 240-01 Regulamento da Formação, "para efeitos de certificação por entidade externa podem ser admitidas outras escalas de avaliação, desde que autorizadas pelo Diretor de Formação". O aproveitamento é obtido consoante as seguintes condições:

1) Classificação final igual ou superior a 70%, na escala de 0 - 100%;
2) Em todas as avaliações é aplicada a obtenção de nota mínima de 70%;
3) Em caso de reprovação em alguma avaliação, existe a possibilidade de repetir essa avaliação, ficando o formando com a nota máxima de 70% nessa avaliação;
4) A repetição de uma avaliação apenas pode ocorrer uma vez durante todo o curso;
5) As repetições são realizadas no final de todas as outras avaliações;
6) Em caso de reprovação em duas avaliações os formandos ficam automaticamente eliminados do curso.

11. Observações.

- Nada a referir.

Página intencionalmente em branco

FICHA DE CUSTOS DA FORMAÇÃO

1. Código – Designação

FCF.E01911A1 - Tarefas de um analista de segurança num Centro de Operações de Segurança – Parte 1

2. Cálculo de custos com pessoal

a. Custos com formandos

FORMANDOS					
Posto/Categoria	N.º Formandos (por posto)	Remuneração (por hora)	Outras despesas (Ajudas de Custo)	Duração (em horas)	Custos
Capitão	1	18,69 €	93,43	50	1 027,72 €
Tenente	2	14,84 €	74,19	50	1 557,95 €
Alferes	1	13,39 €	66,97	50	736,70 €
Saj Ajudante	1	15,32 €	76,59	50	842,52 €
1º Sargento	3	13,39 €	66,97	50	2 076,17 €
2ºSargento	2	12,43 €	62,16	50	1 305,41 €
Furriel	1	9,07 €	45,33	50	498,59 €
Cabo Adjunto	1	9,07 €	45,33	50	498,59 €
				Total	8 543,65 €

b. Custos com formadores

FORMADORES (INTERNOS E EXTERNOS)				
Posto/Categoria	Remuneração (por hora)	Outras despesas	Horas lecionadas	Custos
Capitão	18,69 €	0,00 €	25	700,72 €
Sargento-ajudante	15,32 €	0,00 €	25	574,45 €
			Total	1 275,17 €

c. Custos com pessoal de apoio permanente

PESSOAL DE APOIO PERMANENTE				
Posto/Categoria	Função	Remuneração (por hora)	Duração (em horas)	Custos
Major	Chefe Secção Formação	21,57 €	50	30,42 €
Capitão	Diretor de Curso	18,69 €	50	26,35 €
Sargento Chefe	Adjunto do Chefe Secção Formação	17,24 €	50	24,31 €
Sargento Ajudante	Adjunto do Diretor de Curso	15,32 €	50	21,60 €
			Total	102,68 €

d. Custos com pessoal de apoio temporário

Posto/Categoria	Ação a desempenhar	N.º de elementos (por posto)	Remuneração (por hora)	Horas Despendidas	Outras despesas	Custos
					Total	

3. Amortizações

Designação dos Bens	Qtd	Valor Patrimonial	Taxa de Amortização	Horas de Afetação	Custos
Sala aula (laboratório)	1	20 000,00 €	5,00%	50	2,89 €

Camarata	1	50 000,00 €	5,00%	50	7,23 €
Computadores	13	5 000,00 €	5,00%	50	9,40 €
Projetor Multimédia	1	3 149,07 €	25,00%	50	2,28 €
Tela Projeção	1	73,74 €	12,00%	50	0,03 €
Quadro Branco	1	209,16 €	12,50%	50	0,08 €
UPS	6	2 300,00 €	12,00%	50	4,79 €
				Total	26,70 €

4. Despesas Gerais

a. Despesas com combustíveis e lubrificantes

Viatura	Consumo médio	Km a Percorrer	Preço/Litro	Custos
Nada a referir.				
			Total	

b. Despesas com munições, explosivos e artifícios

Designação da Munição	Quantidade	Preço Unitário	Custos
Nada a referir.			
		Total	

c. Despesas com Limpeza e Higiene

Encargos com Limpeza e Higiene (LH)	Efetivo Médio	N.º de Formandos	Duração (DUF)	Custos
11 247,16 €	256	12	10	14,44 €

d. Despesas com alimentação - refeições fornecidas

Designação da Refeição	Número de Refeições	Preço Refeição	Custos
1ºRefeição	120	1,00 €	120,00 €
2ºRefeição	120	2,50 €	300,00 €
3ºRefeição	120	2,50 €	300,00 €
		Total	720,00 €

e. Despesas com vestuário e artigos pessoais

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

f. Despesas com materiais de consumo

Designação do Material de Consumo	Qtd	Preço	Custos
Agrafos 24/6 (CX)	1	0,16 €	0,16 €
Clips nº4 (CX100)	1	0,16 €	0,16 €
Folhas A4 (resma de 500)	1	2,71 €	2,71 €
Marcadores para Quadro Didax	3	0,61 €	1,82 €
Esferográficas	15	0,08 €	1,27 €
Recarga para apagador quadro Didax (*pack*) de 10	1	2,54 €	2,54 €

Folha Cartolina A4 cor p/Diploma	15	0,29 €	4,36 €
Impressões (preto/branco)	250	0,02 €	5,00 €
		Total	18,01 €

g. Despesas material de consumo clínico

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

h. Despesas com prémios, condecorações e ofertas

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

i. Despesas com encargos das instalações

Encargos com Instalações	Efetivo médio	N.º de Formandos	Duração (DUF)	Custos
166 698,68 €	256	12	10	214,08 €

j. Despesas com conservação de bens

Encargos com Conservação de bens	Efetivo médio	N.º de Formandos	Duração (DUF)	Custos
89 260,66 €	256	12	10	114,63 €

k. Despesas com comunicações

Descrição da despesa com comunicações	Custos
Nada a referir.	
Total	

l. Despesas com transportes

Tipologia da viatura alugada	Custos
Nada a referir.	
Total	

m. Despesas com a utilização de infraestruturas de transportes

Portagens a utilizar	N.º de Utilizações	Preço	Custos
Nada a referir.			
		Total	

5. Custos por Unidade de Formação de Curta Duração

Tipologia	Global	Por Formando
Custo total	11 560,33 €	963,36 €
Custos Imputável à Direção de Formação	530,97 €	44,25 €
Custos Imputável ao Comando do Pessoal	9 921,49 €	826,79 €
Custos Imputável ao Comando da Logística	746,70 €	62,23 €
Custos Imputáveis à U/E/O	361,17 €	30,10 €

Custos Diretos	1 275,17 €	106,26 €
Custos Indiretos	9 754,19 €	812,85 €
Custos Imputável Entidades Externas (com alimentação)	2 485,71 €	207,14 €
Custos Imputável Entidades Externas (sem alimentação)	1 765,71 €	147,14 €

FICHA DE CUSTOS DA FORMAÇÃO

1. Código – Designação

FCF.E01912A1 - Tarefas de um analista de segurança num Centro de Operações de Segurança – Parte 2

2. Cálculo de custos com pessoal

a. Custos com formandos

FORMANDOS					
Posto/Categoria	N.º Formandos (por posto)	Remuneração (por hora)	Outras despesas (Ajudas de Custo)	Duração (em horas)	Custos
Capitão	1	18,69 €	93,43	50	1 027,72 €
Tenente	2	14,84 €	74,19	50	1 557,95 €
Alferes	1	13,39 €	66,97	50	736,70 €
Saj Ajudante	1	15,32 €	76,59	50	842,52 €
1º Sargento	3	13,39 €	66,97	50	2 076,17 €
2ºSargento	2	12,43 €	62,16	50	1 305,41 €
Furriel	1	9,07 €	45,33	50	498,59 €
Cabo Adjunto	1	9,07 €	45,33	50	498,59 €
				Total	8 543,65 €

b. Custos com formadores

FORMADORES (INTERNOS E EXTERNOS)				
Posto/Categoria	Remuneração (por hora)	Outras despesas	Horas lecionadas	Custos
Capitão	18,69 €	0,00 €	25	700,72 €
Sargento-ajudante	15,32 €	0,00 €	25	574,45 €
			Total	1 275,17 €

c. Custos com pessoal de apoio permanente

PESSOAL DE APOIO PERMANENTE				
Posto/Categoria	Função	Remuneração (por hora)	Duração (em horas)	Custos
Major	Chefe Secção Formação	21,57 €	50	30,42 €
Capitão	Diretor de Curso	18,69 €	50	26,35 €
Sargento Chefe	Adjunto do Chefe Secção Formação	17,24 €	50	24,31 €
Sargento Ajudante	Adjunto do Diretor de Curso	15,32 €	50	21,60 €
			Total	102,68 €

d. Custos com pessoal de apoio temporário

Posto/Categoria	Ação a desempenhar	N.º de elementos (por posto)	Remuneração (por hora)	Horas Despendidas	Outras despesas	Custos
					Total	

3. Amortizações

Designação dos Bens	Qtd	Valor Patrimonial	Taxa de Amortização	Horas de Afetação	Custos
Sala aula (laboratório)	1	20 000,00 €	5,00%	50	2,89 €

Camarata	1	50 000,00 €	5,00%	50	7,23 €
Computadores	13	5 000,00 €	5,00%	50	9,40 €
Projetor Multimédia	1	3 149,07 €	25,00%	50	2,28 €
Tela Projeção	1	73,74 €	12,00%	50	0,03 €
Quadro Branco	1	209,16 €	12,50%	50	0,08 €
UPS	6	2 300,00 €	12,00%	50	4,79 €
				Total	26,70 €

4. Despesas Gerais

a. Despesas com combustíveis e lubrificantes

Viatura	Consumo médio	Km a Percorrer	Preço/Litro	Custos
Nada a referir.				
			Total	

b. Despesas com munições, explosivos e artifícios

Designação da Munição	Quantidade	Preço Unitário	Custos
Nada a referir.			
		Total	

c. Despesas com Limpeza e Higiene

Encargos com Limpeza e Higiene (LH)	Efetivo Médio	N.º de Formandos	Duração (DUF)	Custos
11 247,16 €	256	12	10	14,44 €

d. Despesas com alimentação - refeições fornecidas

Designação da Refeição	Número de Refeições	Preço Refeição	Custos
1ºRefeição	120	1,00 €	120,00 €
2ºRefeição	120	2,50 €	300,00 €
3ºRefeição	120	2,50 €	300,00 €
		Total	720,00 €

e. Despesas com vestuário e artigos pessoais

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

f. Despesas com materiais de consumo

Designação do Material de Consumo	Qtd	Preço	Custos
Agrafos 24/6 (CX)	1	0,16 €	0,16 €
Clips nº4 (CX100)	1	0,16 €	0,16 €
Folhas A4 (resma de 500)	1	2,71 €	2,71 €
Marcadores para Quadro Didax	3	0,61 €	1,82 €
Esferográficas	15	0,08 €	1,27 €
Recarga para apagador quadro Didax (*pack*) de 10	1	2,54 €	2,54 €

Folha Cartolina A4 cor p/Diploma	15	0,29 €	4,36 €
Impressões (preto/branco)	250	0,02 €	5,00 €
		Total	18,01 €

g. Despesas material de consumo clínico

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

h. Despesas com prémios, condecorações e ofertas

Designação do Artigo	Qtd	Preço	Custos
Nada a referir.			
		Total	

i. Despesas com encargos das instalações

Encargos com Instalações	Efetivo médio	N.º de Formandos	Duração (DUF)	Custos
166 698,68 €	256	12	10	214,08 €

j. Despesas com conservação de bens

Encargos com Conservação de bens	Efetivo médio	N.º de Formandos	Duração (DUF)	Custos
89 260,66 €	256	12	10	114,63 €

k. Despesas com comunicações

Descrição da despesa com comunicações	Custos
Nada a referir.	
Total	

l. Despesas com transportes

Tipologia da viatura alugada	Custos
Nada a referir.	
Total	

m. Despesas com a utilização de infraestruturas de transportes

Portagens a utilizar	N.º de Utilizações	Preço	Custos
Nada a referir.			
		Total	

5. Custos por Unidade de Formação de Curta Duração

Tipologia	Global	Por Formando
Custo total	11 560,33 €	963,36 €
Custos Imputável à Direção de Formação	530,97 €	44,25 €
Custos Imputável ao Comando do Pessoal	9 921,49 €	826,79 €
Custos Imputável ao Comando da Logística	746,70 €	62,23 €
Custos Imputáveis à U/E/O	361,17 €	30,10 €

Custos Diretos	1 275,17 €	106,26 €
Custos Indiretos	9 754,19 €	812,85 €
Custos Imputável Entidades Externas (com alimentação)	2 485,71 €	207,14 €
Custos Imputável Entidades Externas (sem alimentação)	1 765,71 €	147,14 €

ANEXO (HORÁRIO TIPO) ao Referencial de Curso de *Cisco Certified Network Associate – Cybersecurity Operations*

1. Primeira semana

TF	2.ª Feira	3.ª Feira	4.ª Feira	5.ª Feira	6.ª Feira
08h30 - 09h20	Cerimónia Abertura	Treino físico	UFCD.E01911A OE.3.2	Treino físico	UFCD.E01911A OE.5.1
09h30 - 10h20	Procedimentos administrativos	Reforço Formação OA2	UFCD.E01911A OE.3.2	UFCD.E01911A OE.4.2	UFCD.E01911A OE.5.1
10h30 - 11h20	UFCD.E01911A OE.1.1	UFCD.E01911A OE.3.1	UFCD.E01911A OE.3.2	UFCD.E01911A OE.4.3	UFCD.E01911A OE.5.1
11h30 - 12h20	UFCD.E01911A OE.1.2	UFCD.E01911A OE.3.1	Reforço Formação OA3	UFCD.E01911A OE.4.3	UFCD.E01911A OE.5.1
14h00 - 14h50	Reforço Formação OA1	UFCD.E01911A OE.3.1	Reforço Formação OA3	Reforço Formação OA4	UFCD.E01911A OE.5.2
15h00 - 15h50	UFCD.E01911A OE.2.1	UFCD.E01911A OE.3.2	UFCD.E01911A OE.4.1	Reforço Formação OA4	UFCD.E01911A OE.5.2
16h00 - 16h50	UFCD.E01911A OE.2.2	UFCD.E01911A OE.3.2	UFCD.E01911A OE.4.2	UFCD.E01911A OE.5.1	UFCD.E01911A OE.5.3

2. Segunda semana

TF	2.ª Feira	3.ª Feira	4.ª Feira	5.ª Feira	6.ª Feira
08h30 - 09h20	UFCD.E01911A OE.5.3	Treino físico	UFCD.E01911A OE.5.7	Treino físico	UFCD.E01912A OE.2.1
09h30 - 10h20	UFCD.E01911A OE.5.3	UFCD.E01911A OE.5.5	UFCD.E01911A OE.5.7	UFCD.E01912A OE.1.3	UFCD.E01912A OE.2.2
10h30 - 11h20	UFCD.E01911A OE.5.4	UFCD.E01911A OE.5.5	Reforço Formação OA5	UFCD.E01912A OE.1.4	UFCD.E01912A OE.2.2
11h30 - 12h20	UFCD.E01911A OE.5.4	UFCD.E01911A OE.5.5	Reforço Formação OA5	UFCD.E01912A OE.1.4	UFCD.E01912A OE.2.3
14h00 - 14h50	UFCD.E01911A OE.5.4	UFCD.E01911A OE.5.6	UFCD.E01912A OE.1.1	Reforço Formação OA1	UFCD.E01912A OE.2.3
15h00 - 15h50	UFCD.E01911A OE.5.5	UFCD.E01911A OE.5.6	UFCD.E01912A OE.1.2	Reforço Formação OA1	UFCD.E01912A OE.2.4
16h00 - 16h50	UFCD.E01911A OE.5.5	UFCD.E01911A OE.5.7	UFCD.E01912A OE.1.2	UFCD.E01912A OE.2.1	UFCD.E01912A OE.2.4

3. Terceira semana

TF	2.ª Feira	3.ª Feira	4.ª Feira	5.ª Feira	6.ª Feira
08h30 - 09h20	UFCD.E01912A OE.2.5	Treino físico	UFCD.E01912A OE.4.1	Treino físico	UFCD.E01912A OE.5.1
09h30 - 10h20	UFCD.E01912A OE.2.5	UFCD.E01912A OE.3.1	UFCD.E01912A OE.4.1	UFCD.E01912A OE.4.3	UFCD.E01912A OE.5.1
10h30 - 11h20	UFCD.E01912A OE.2.5	UFCD.E01912A OE.3.2	UFCD.E01912A OE.4.2	UFCD.E01912A OE.4.4	UFCD.E01912A OE.5.2
11h30 - 12h20	Reforço Formação OA2	UFCD.E01912A OE.3.2	UFCD.E01912A OE.4.2	UFCD.E01912A OE.4.4	UFCD.E01912A OE.5.2
14h00 - 14h50	Reforço Formação OA2	UFCD.E01912A OE.3.2	UFCD.E01912A OE.4.2	UFCD.E01912A OE.4.4	UFCD.E01912A OE.5.2
15h00 - 15h50	UFCD.E01912A OE.3.1	UFCD.E01912A OE.3.2	UFCD.E01912A OE.4.3	Reforço Formação OA4	
16h00 - 16h50	UFCD.E01912A OE.3.1	Reforço Formação OA3	UFCD.E01912A OE.4.3	Reforço Formação OA4	

4. Quarta semana

TF	2.ª Feira	3.ª Feira	4.ª Feira	5.ª Feira	6.ª Feira
08h30 - 09h20	Reforço Formação Revisões	Treino físico	Preparação Máquinas Virtuais	Treino físico	Correção de testes
09h30 - 10h20	Preparação Máquinas Virtuais	Reforço Formação Revisões	UFCD.E01911A *Hands-on Game Mission*	Reforço Formação Revisões	Correção de testes
10h30 - 11h20	UFCD.E01911A *Cisco Practise Final Exam*	UFCD.E01911A *Cisco Final Exam*	UFCD.E01911A *Hands-on Game Mission*	UFCD.E01911A *Quiz RTm*	Procedimentos administrativos
11h30 - 12h20	UFCD.E01912A *Cisco Practise Final Exam*	UFCD.E01912A *Cisco Final Exam*	UFCD.E01912A *Hands-on Game Mission*	UFCD.E01912A *Quiz RTm*	Cerimónia Encerramento
14h00 - 14h50	UFCD.E01911A *Hands-on Skills Exam Cisco*	UFCD.E01911A *Hands-on Skills Lab Mix*	UFCD.E01911A *Hands-on Skills Exam RTm*	UFCD.E01911A Repetição de avaliações	
15h00 - 15h50	UFCD.E01911A *Hands-on Skills Exam Cisco*	UFCD.E01912A *Hands-on Skills Lab Mix*	UFCD.E01912A *Hands-on Skills Exam RTm*	UFCD.E01912A Repetição de exames	
16h00 - 16h50	UFCD.E01912A *Hands-on Skills Exam Cisco*	UFCD.E01912A *Hands-on Skills Lab Mix*	UFCD.E01912A *Hands-on Skills Exam RTm*	Desmontagem de laboratórios	