Nome: _____ Data: _____ Pontuação: _____

Arquitetura e segurança Zero Trust

Verificação contínua, microssegmentação de rede, gestão de identidades e acessos, privilégio mínimo e verificações de postura.

VISÃO GERAL DA APRENDIZAGEM SOBRE SEGURANÇA ZERO TRUST

PROTEGIDO

ENCRIPTAÇÃO DE DADOS

Norma AES de 256 bits

CONFORME

NORMAS GLOBAIS

Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST

POLÍTICA DE ACESSO

Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pela arquitetura e segurança Zero Trust. Vais explorar a verificação contínua, a microssegmentação de rede, a gestão de identidades e acessos (IAM), o privilégio mínimo e a auditoria de sessões.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/ciberseguranca-zero-trust/

O teu roteiro de aprendizagem sobre a estratégia Zero Trust

- Compreender o princípio central da verificação contínua.
- Implementa a microssegmentação da rede e o acesso com privilégio mínimo.
- Configura verificações de postura dos dispositivos e auditoria de sessões ativas.

INSTRUÇÕES DO GUIA DE SEGURANÇA ZERO TRUST

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à arquitetura Zero Trust. Termina com a atividade bónus Pensa rápido.

ARQUITETURA E SEGURANÇA ZERO TRUST (INTRODUÇÃO)

A segurança Zero Trust substitui os antigos modelos de perímetro de rede por uma política rigorosa de «nunca confiar, verificar sempre». Implementar microssegmentação, gestão de identidades e acessos (IAM), direitos de privilégio mínimo e verificações de postura bloqueia o movimento lateral das ameaças.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é o princípio fundamental da segurança Zero Trust?

- A. Nunca confiar, verificar sempre cada pedido de acesso, independentemente da origem
- B. Presumir que todo o tráfego dentro da firewall corporativa é seguro
- C. Armazenar ficheiros de bases de dados sem encriptação para melhorar a velocidade
- D. Impor a autenticação de e-mail usando apenas registos SPF

2. O que é a microssegmentação de rede?

- A. Dividir redes em zonas pequenas e isoladas para conter o movimento lateral
- B. Encriptar as placas de rede durante o trânsito de dados
- C. Ligar todos os servidores locais a um único endereço IP público
- D. Monitorizar as teclas premidas pelo utilizador em sessões do navegador

3. O que é o princípio do privilégio mínimo?

- A. Restringir as permissões de acesso do utilizador apenas ao que é necessário para o seu trabalho
- B. Dar por predefinição todos os privilégios do sistema a todos os utilizadores
- C. Permitir inícios de sessão anónimos em servidores de bases de dados corporativas
- D. Configurar routers Wi-Fi públicos sem palavras-passe

4. O que é a gestão de identidades e acessos (IAM)?

- A. Estruturas que gerem identidades digitais e controlam os privilégios do sistema
- B. Utilitários antivírus que analisam diretórios de ficheiros locais
- C. Um sistema de armazenamento de cópias de segurança que usa suportes isolados da rede (air-gapped)
- D. Um protocolo de gateway de e-mail que rejeita domínios falsificados

5. O que significa autenticação contínua?

- A. Verificar repetidamente a identidade do utilizador e a postura do dispositivo durante uma sessão ativa
- B. Alterar a palavra-passe principal a cada 10 minutos
- C. Aplicar hash a registos de bases de dados com vários algoritmos
- D. Encriptar pacotes de rede em trânsito com chaves TLS

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. O Zero Trust assume que todo o tráfego dentro da firewall da empresa é seguro.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. A microssegmentação limita a capacidade de os atacantes se moverem lateralmente entre servidores internos.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. O privilégio mínimo concede acesso a todos os ficheiros da base de dados por predefinição.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. A verificação contínua valida o estado do dispositivo e as credenciais durante toda a sessão de início de sessão.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. A implementação do Zero Trust reduz o impacto de credenciais empresariais comprometidas.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Exigir credenciais em cada ponto de acesso é a _____ contínua.
2. Dividir a rede corporativa em pequenas zonas é a micro- _____ .
3. Configurar identidades digitais e controlo de acesso recorre a um sistema de _____ .
4. Restringir as permissões dos utilizadores aplica o princípio do menor _____ .
5. Avaliar o estado de saúde dos dispositivos ligados analisa a _____ do dispositivo.
6. Registar e rever as sessões ativas é a _____ de segurança.

BANCO DE PALAVRAS DE VOCABULÁRIO

AUDITORIA FIREWALL GESTÃO IAM POSTURA PRIVILÉGIO ROUTER SEGMENTAÇÃO VERIFICAÇÃO

Escreve aqui as tuas respostas:

1.
2.
3.
4.
5.
6.

Ponto de controlo 4: Associação de conceitos de segurança

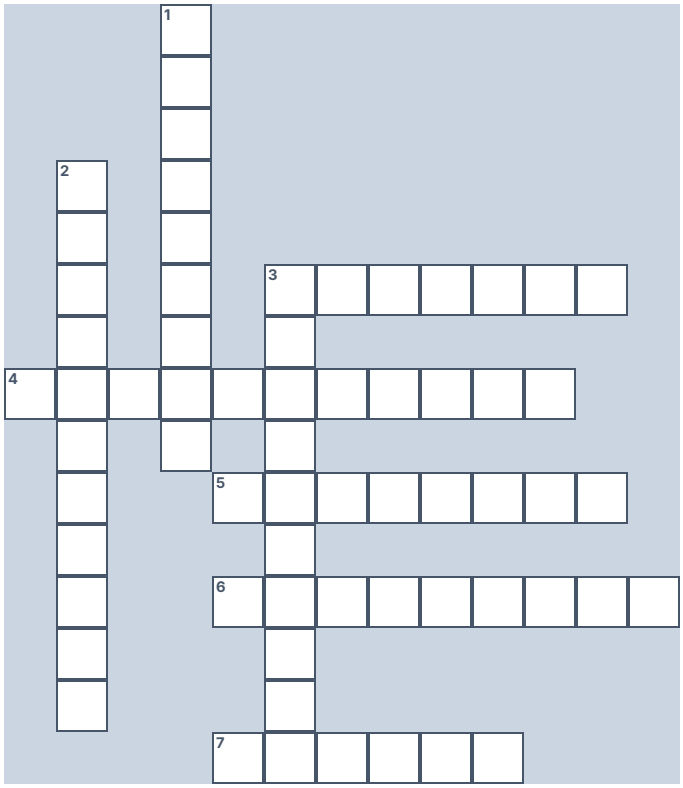
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. VERIFICAÇÃO	A	Gerir o acesso às credenciais dos utilizadores.
☐	2. SEGMENTAÇÃO	B	Princípio do menor direito de acesso.
☐	3. IAM	C	Encaminhamento do tráfego de pacotes de rede.
☐	4. PRIVILÉGIO	D	Proteção de barreira de rede externa.
☐	5. POSTURA	E	Rever as sessões de acesso registadas.
☐	6. AUDITORIA	F	Dividir as zonas da rede interna.
☐	7. FIREWALL	G	Verificar sempre as credenciais do utilizador.
☐	8. ROUTER	H	Avaliar o estado de saúde do dispositivo.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

3. Avaliação do estado de saúde dos dispositivos. (7)

4. Verificar sempre as credenciais do utilizador. (11)

5. Proteção da barreira externa da rede. (8)

6. Gestão do acesso às credenciais dos utilizadores. (9)

7. Encaminhamento do tráfego de pacotes da rede. (6)

VERTICAIS

1. Revisão das sessões de acesso registadas. (9)

2. Divisão das zonas internas da rede. (11)

3. Princípio dos direitos de acesso mínimos. (10)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

3 horizontal: Avaliação do estado de saúde dos dispositivos. (7 letras):

4 horizontal: Verificar sempre as credenciais do utilizador. (11 letras):

5 horizontal: Proteção da barreira externa da rede. (8 letras):

6 horizontal: Gestão do acesso às credenciais dos utilizadores. (9 letras):

7 horizontal: Encaminhamento do tráfego de pacotes da rede. (6 letras):

VERTICAIS

1 vertical: Revisão das sessões de acesso registadas. (9 letras):

2 vertical: Divisão das zonas internas da rede. (11 letras):

3 vertical: Princípio dos direitos de acesso mínimos. (10 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

C R I G N R M A P X Q O C U S
O T E L J B A U B C P P X L K
A Y K X T K D D Q M O J D I N
C L L A W E R I F N S K Q P G
A M M Q R V S T T T T G C P S
T Q O H S E B O W D U S Z R V
N C Z W F R K R G H R Z D I N
E D Q X P I C I E U A B A V Z
M N D K A F D A S O D F H I I
G D R Q M I R E T I R Z S L F
E Q V F A C O A A Q O N P E T
S X Q K R A U U O S D N Y G B
F S X W J C T A I R Z Y Y I L
G I M R J A E M A L T O H O Q
Q H Z A O O R V M G U B Y R Y

LISTA DE PALAVRAS DE VOCABULÁRIO

VERIFICACAO SEGMENTACAO GESTAOIAM PRIVILEGIO POSTURA AUDITORIA FIREWALL ROUTER

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO	DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO
A. VERIFICACAO	_____ 1. Proteção da barreira externa da rede.
B. SEGMENTACAO	_____ 2. Revisão das sessões de acesso registadas.
C. GESTAOIAM	_____ 3. Princípio dos direitos de acesso mínimos.
D. PRIVILEGIO	_____ 4. Divisão das zonas internas da rede.
E. POSTURA	_____ 5. Encaminhamento do tráfego de pacotes da rede.
F. AUDITORIA	_____ 6. Avaliação do estado de saúde dos dispositivos.
G. FIREWALL	_____ 7. Gestão do acesso às credenciais dos utilizadores.
H. ROUTER	_____ 8. Verificar sempre as credenciais do utilizador.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. **FCAEIAVCROI** _____
2. **MGATEOIAS** _____
3. **TPUASRO** _____
4. **ELLAWFIR** _____
5. **CEATGOENSAM** _____
6. **IIVEGPRLOI** _____
7. **OAIARIUTD** _____
8. **URRETO** _____

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Informações que nunca deves partilhar			
2	Hábitos seguros que podes começar hoje			
3	Coisas verificadas num dispositivo			
4	Coisas que ficam registadas			
5	Palavras relacionadas com cibersegurança			
6	Coisas que o Zero Trust verifica			
7	Locais onde mostras a identificação no dia a dia			
8	Formas de provar que és mesmo tu			
9	Coisas a fazer depois de uma fuga de dados			
10	Sinais de que um computador está infetado			
11	Razões para atualizar o software			
12	Níveis de acesso numa empresa			
13	Ferramentas de segurança que conheces			
14	Zonas em que uma rede pode ser dividida			
15	Ditados sobre confiança			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: TRANSIÇÃO PARA UMA ARQUITETURA DE REDE ZERO TRUST

👷

Cenário: Uma grande empresa usa atualmente uma rede interna plana onde qualquer dispositivo da rede local pode aceder a todos os servidores e bases de dados da empresa.

Questão para debate: Cria uma estratégia de microssegmentação de rede para limitar o movimento lateral.

ESTUDO DE CASO 2: IMPLEMENTAR CONTROLOS DE ACESSO DE PRIVILÉGIO MÍNIMO

👷

Cenário: Os registos de auditoria revelam que utilizadores temporários de bases de dados e colaboradores de nível básico têm permissões globais de leitura e escrita em bases de dados de contabilidade críticas.

Questão para debate: Audita e restringe os privilégios IAM da base de dados para impor o privilégio mínimo.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

22 5 18 9 6 9 3 1 19 5 13 16 18 5 3 15 13 1

1 18 17 21 9 20 5 20 21 18 1 26 5 18 15

20 18 21 19 20

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é o Zero Trust?

O Zero Trust é uma estrutura de segurança que assume que existem ameaças tanto fora como dentro do perímetro da rede, exigindo verificação para cada pedido. [1]

Q2: Qual é a regra central do Zero Trust?

Nunca confiar, verificar sempre.

Q3: O que é a microssegmentação?

Divisão de uma rede em pequenos segmentos lógicos seguros para controlar o tráfego e conter violações.

Q4: O que é o privilégio mínimo?

Conceder aos utilizadores apenas os direitos de acesso mínimos necessários para realizar as suas tarefas específicas. [2]

Q5: O que significa IAM?

Gestão de identidades e acessos.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: Como ajuda a verificação de postura do dispositivo?

Verifica se um dispositivo está atualizado, tem antivírus ativo e é seguro antes de permitir o acesso.

Q7: O que é o movimento lateral?

O processo que os atacantes utilizam para se deslocarem numa rede, de um nó inicialmente comprometido para sistemas de maior valor.

Q8: O Zero Trust substitui as firewalls?

Não, melhora-os ao acrescentar verificações centradas na identidade e firewalls de segmentação interna.

Q9: O que é a autenticação contínua?

Verificação contínua da identidade do utilizador durante uma sessão ativa, e não apenas no início de sessão.

Q10: Porque é perigosa uma rede plana?

Em redes planas, um único nó comprometido permite aos atacantes aceder facilmente a qualquer base de dados da rede.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como responde o Zero Trust ao modelo de perímetro?

Substitui o modelo ultrapassado de «castelo e fosso», deslocando a defesa das redes de fronteira para identidades e recursos específicos de utilizadores.

Q2: O que é um ponto de decisão de políticas (PDP)?

O componente do sistema que avalia pedidos de autorização face às regras de segurança para decidir se o acesso deve ser concedido.

Q3: O que é um ponto de aplicação de políticas (PEP)?

O nó do sistema (como um gateway ou proxy) que permite ou bloqueia fisicamente os pedidos de ligação com base na decisão do PDP.

Q4: Como apoia o controlo de acesso baseado em funções (RBAC) o Zero Trust?

O RBAC agrupa permissões em funções específicas, ajudando a evitar que os utilizadores herdem privilégios administrativos excessivos.

Q5: O que é o controlo de acesso contextual?

Avaliar os pedidos de início de sessão com pistas secundárias, como a localização geográfica, a postura do dispositivo e a hora de início de sessão, para avaliar o risco.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: Em que difere a microssegmentação das VLAN normais?

As VLAN dividem as redes em segmentos lógicos amplos na camada 2, enquanto a microssegmentação usa políticas de software para isolar cargas de trabalho individuais.

Q7: O que é o acesso just-in-time (JIT)?

Conceder temporariamente permissões administrativas elevadas e revogá-las automaticamente quando a tarefa termina.

Q8: Como se protegem as API numa framework Zero Trust?

Exigindo tokens OAuth assinados criptograficamente e auditando as assinaturas dos pedidos em cada gateway de API.

Q9: O que é um cliente de acesso à rede Zero Trust (ZTNA)?

Um agente de software que estabelece ligações de saída seguras e encriptadas a aplicações específicas, em vez de sub-redes de rede em bruto.

Q10: Como é que a auditoria de registos ajuda o Zero Trust?

O registo contínuo permite que as ferramentas automatizadas de análise de segurança detetem anomalias e suspendam de imediato inícios de sessão não autorizados.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

As arquiteturas Zero Trust substituem o modelo tradicional de castelo e fosso por regras de verificação centradas na identidade.

2. PERSPETIVA SOBRE SEGURANÇA

A microssegmentação de rede reduz a área que o software malicioso pode alcançar, isolando as cargas de trabalho em pequenas zonas protegidas.

3. PERSPETIVA SOBRE SEGURANÇA

O Zero Trust centra-se na proteção de recursos como ativos, serviços e contas, e não de segmentos de rede. [1]

4. PERSPETIVA SOBRE SEGURANÇA

As políticas de acesso com privilégio mínimo reduzem o risco de saída de dados das bases de dados centrais por ameaças internas.

5. PERSPETIVA SOBRE SEGURANÇA

A validação da postura do dispositivo verifica em tempo real os níveis de atualização do sistema operativo e o estado do antivírus ativo.

6. PERSPETIVA SOBRE SEGURANÇA

Os intermediários de Zero Trust Network Access (ZTNA) podem substituir ou complementar as VPN empresariais para restringir o âmbito de acesso dos utilizadores.

7. PERSPETIVA SOBRE SEGURANÇA

A delegação de privilégios administrativos Just-in-Time (JIT) reduz o risco de roubo de credenciais em controladores de domínio.

8. PERSPETIVA SOBRE SEGURANÇA

A validação contínua regista e audita o comportamento da sessão, suspendendo utilizadores que apresentem padrões anómalos de execução de scripts.

9. PERSPETIVA SOBRE SEGURANÇA

As defesas de perímetro tradicionais não conseguem bloquear ataques laterais depois de uma credencial administrativa ser divulgada.

10. PERSPETIVA SOBRE SEGURANÇA

A Publicação Especial NIST 800-207 (2020) apresenta uma definição abstrata da arquitetura Zero Trust, com modelos de implementação. [1]

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Qual é o princípio fundamental da segurança Zero Trust? → Nunca confiar, verificar sempre cada pedido de acesso, independentemente da origem

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

O que é a microssegmentação de rede? → Dividir redes em zonas pequenas e isoladas para conter o movimento lateral

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

O que é o princípio do privilégio mínimo? → Restringir as permissões de acesso do utilizador apenas ao que é necessário para o seu trabalho

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

O que é a gestão de identidades e acessos (IAM)? → Estruturas que gerem identidades digitais e controlam os privilégios do sistema

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que significa autenticação contínua? → Verificar repetidamente a identidade do utilizador e a postura do dispositivo durante uma sessão ativa

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Falso: o Zero Trust não concede confiança implícita com base na localização na rede, dentro ou fora dela.

7 **Pergunta 7** **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Verdadeiro: pequenas zonas isoladas limitam a distância a que um intruso se pode mover entre servidores.

8 **Pergunta 8** **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Falso: o privilégio mínimo concede apenas o acesso mínimo de que cada função precisa.

9 **Pergunta 9** **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A verificação contínua valida o estado do dispositivo e as credenciais durante toda a sessão de início de sessão.

10 **Pergunta 10** **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A implementação do Zero Trust reduz o impacto de credenciais empresariais comprometidas.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

G 1. VERIFICAÇÃO	F 2. SEGMENTAÇÃO	A 3. IAM	B 4. PRIVILÉGIO
H 5. POSTURA	E 6. AUDITORIA	D 7. FIREWALL	C 8. ROUTER

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 VERIFICAÇÃO	2 SEGMENTAÇÃO	3 GESTÃO IAM	4 PRIVILÉGIO
5 POSTURA	6 AUDITORIA		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 G – FIREWALL	2 F – AUDITORIA	3 D – PRIVILEGIO	4 B – SEGMENTACAO
5 H – ROUTER	6 E – POSTURA	7 C – GESTAOIAM	8 A – VERIFICACAO

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar VERIFICAÇÃO, SEGMENTAÇÃO e IAM por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

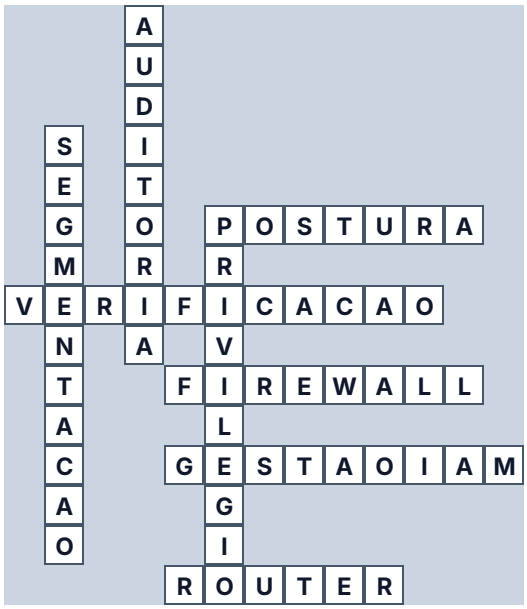
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

C	R	I	G	N	R	M	A	P	X	Q	O	C	U	S
O	T	E	L	J	B	A	U	B	C	P	P	X	L	K
A	Y	K	X	T	K	D	D	Q	M	O	J	D	I	N
C	L	L	A	W	E	R	I	F	N	S	K	Q	P	G
A	M	M	Q	R	V	S	T	T	T	T	G	C	P	S
T	Q	O	H	S	E	B	O	W	D	U	S	Z	R	V
N	C	Z	W	F	R	K	R	G	H	R	Z	D	I	N
E	D	Q	X	P	I	C	I	E	U	A	B	A	V	Z
M	N	D	K	A	F	D	A	S	O	D	F	H	I	I
G	D	R	Q	M	I	R	E	T	I	R	Z	S	L	F
E	Q	V	F	A	C	O	A	A	Q	O	N	P	E	T
S	X	Q	K	R	A	U	U	O	S	D	N	Y	G	B
F	S	X	W	J	C	T	A	I	R	Z	Y	Y	I	L
G	I	M	R	J	A	E	M	A	L	T	O	H	O	Q
Q	H	Z	A	O	O	R	V	M	G	U	B	Y	R	Y

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

3 horizontal: POSTURA Avaliação do estado de saúde dos dispositivos. (7 letras)

4 horizontal: VERIFICACAO Verificar sempre as credenciais do utilizador. (11 letras)

5 horizontal: FIREWALL Proteção da barreira externa da rede. (8 letras)

6 horizontal: GESTAOIAM Gestão do acesso às credenciais dos utilizadores. (9 letras)

7 horizontal: ROUTER Encaminhamento do tráfego de pacotes da rede. (6 letras)

VERTICAIS

1 vertical: AUDITORIA Revisão das sessões de acesso registadas. (9 letras)

2 vertical: SEGMENTACAO Divisão das zonas internas da rede. (11 letras)

3 vertical: PRIVILEGIO Princípio dos direitos de acesso mínimos. (10 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. F C A E I A V C R O I — **VERIFICACAO**
2. M G A T E O I A S — **GESTAOIAM**
3. T P U A S R O — **POSTURA**
4. E L L A W F I R — **FIREWALL**
5. C E A T G O E N S A M — **SEGMENTACAO**
6. I I V E G P R L O I — **PRIVILEGIO**
7. O A I A R I U T D — **AUDITORIA**
8. U R R E T O — **ROUTER**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"VERIFICA SEMPRE COM A ARQUITETURA ZERO TRUST"

Soluções dos estudos de caso

A Estudo de caso 1: Transição para uma arquitetura de rede Zero Trust

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Uma grande empresa usa atualmente uma rede interna plana em que qualquer dispositivo da rede local pode aceder a todos os servidores e bases de dados da empresa.
- Estratégia e solução recomendadas: Segmentar a rede plana em zonas departamentais isoladas. Instalar firewalls internas para controlar o tráfego entre zonas e exigir validação de tokens de ligação para todos os acessos.

B Estudo de caso 2: Implementar controlos de acesso de privilégio mínimo

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Os registos de auditoria revelam que utilizadores temporários da base de dados e funcionários de nível inferior têm permissões globais de leitura e escrita em bases de dados contabilísticas críticas.
- Estratégia e solução recomendadas: Revogar todos os privilégios administrativos globais. Implementar o Controlo de Acesso Baseado em Funções (RBAC) para corresponder exatamente às funções profissionais e estabelecer revisões semanais automatizadas de permissões.