Nome: _____ **Data:** _____ **Pontuação:** _____

Noções básicas de cibersegurança e ameaças online Prevenção

Ameaças de cibersegurança, firewalls de rede, autenticação multifator, quadros de segurança

VISÃO GERAL DE APRENDIZAGEM SOBRE NOÇÕES BÁSICAS DE CIBERSEGURANÇA

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 pelos princípios fundamentais da cibersegurança e da prevenção de ameaças online. Vais explorar ameaças de software malicioso, autenticação multifator, firewalls de rede e estruturas de resposta a incidentes.

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/

O teu roteiro de aprendizagem sobre os fundamentos da cibersegurança

- Identifica vetores comuns de software malicioso, phishing e intrusão em redes empresariais.
- Implementa controlos de cibersegurança padrão, incluindo MFA, firewalls e defesa de dispositivos terminais.
- Avalia procedimentos de resposta a incidentes para atenuar o impacto de violações de dados.
- Analisa os fatores de risco organizacional e o alinhamento de segurança segundo as diretrizes do NIST.
- Configura práticas de higiene de segurança para mitigar o credential stuffing automatizado.

INSTRUÇÕES DO GUIA DE CIBERSEGURANÇA

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 prevenção de ameaças. Termina com a atividade bónus Pensa rápido.

NOÇÕES BÁSICAS DE CIBERSEGURANÇA E PREVENÇÃO DE AMEAÇAS (INTRODUÇÃO)

A cibersegurança protege redes, sistemas e dados contra ataques digitais não autorizados. Desenvolver hábitos de segurança sólidos, configurar firewalls, exigir autenticação multifator e formar o pessoal no reconhecimento de ameaças são componentes essenciais da defesa de redes empresariais.

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 principal objetivo de um ataque de phishing?

- A. Roubar credenciais e dados sensíveis dos utilizadores
- B. Melhorar a visibilidade do site nos motores de busca
- C. Aumentar a capacidade de largura de banda da rede
- D. Gerir a replicação de centros de dados de cópia de segurança

2. Que mecanismo oferece a proteção de conta mais forte?

- A. Autenticação multifator com chaves de hardware
- B. Palavras-passe complexas atualizadas a cada trinta dias
- C. Restringir o início de sessão na conta ao horário de expediente
- D. Ocultar o nome de utilizador da conta nos diretórios públicos

3. O que define a carga de uma infeção por ransomware?

- A. Encriptar ficheiros do sistema e exigir pagamento
- B. Registar silenciosamente as teclas premidas em servidores remotos
- C. Injetar publicidade não autorizada nos navegadores
- D. Usar recursos do CPU local para minerar criptomoedas

4. De que forma afeta uma exploração de dia zero as defesas de segurança?

- A. Visa vulnerabilidades desconhecidas e sem correção
- B. Desativa automaticamente a firewall corporativa
- C. Obriga o sistema a efetuar um reinício forçado
- D. Não requer qualquer orçamento para ser corrigido

5. Que enquadramento rege os controlos de segurança empresariais?

- A. Diretrizes do NIST Cybersecurity Framework
- B. Especificações do esquema de documentos HTML5 do W3C
- C. Manuais de instalação de controladores de impressora
- D. Definições do protocolo de encaminhamento do IETF

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta (verdadeiro/falso) 6

6. Os ataques de phishing visam apenas contas de e-mail pessoais.

Verdadeiro Falso

7 Pergunta (verdadeiro/falso) 7

7. A autenticação multifator ajuda a bloquear ataques de credential stuffing.

Verdadeiro Falso

8 Pergunta (verdadeiro/falso) 8

8. As firewalls inspecionam o tráfego de rede para bloquear o acesso não autorizado a portas.

Verdadeiro Falso

9 Pergunta (verdadeiro/falso) 9

9. A correção de explorações zero-day exige atualizações normais das definições do antivírus.

Verdadeiro Falso

10 Pergunta (verdadeiro/falso) 10

10. Um honeypot é um servidor isco usado para atrair cibercriminosos.

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. Os administradores de rede instalam uma _____ para filtrar o tráfego de entrada.

2. Um atacante usa um _____ para contornar as correções do sistema.

3. Os atacantes enviam emails falsificados para realizar campanhas de _____ contra os funcionários.

4. O ransomware é uma forma destrutiva de _____ que bloqueia os dados do utilizador.

5. Estabelecer uma boa _____ de palavras-passe reduz os riscos de roubo de credenciais.

6. Para proteger comunicações sensíveis, os utilizadores aplicam protocolos de _____ .

BANCO DE PALAVRAS DE VOCABULÁRIO

ENCRIPTAÇÃO EXPLOIT ZERO-DAY FIREWALL HIGIENE HONEYPOT MALWARE MULTIFATOR PHISHING

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de segurança

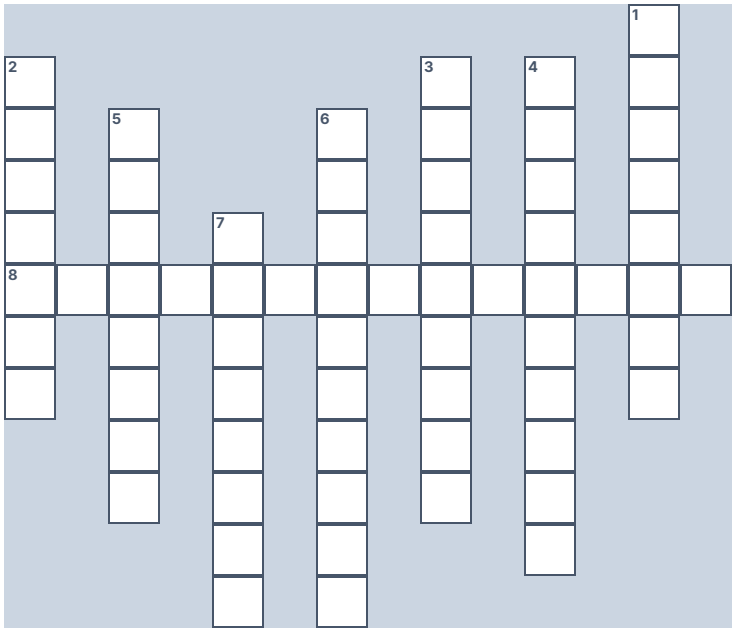
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. Ameaça de ransomware	A	Diretrizes estruturadas, como as do NIST, usadas para gerir ciber-riscos.
☐	2. Autenticação multifator	B	Plano estruturado para tratar e mitigar violações de segurança.
☐	3. Exploração de dia zero	C	Barreira de rede que filtra o tráfego com base em regras de segurança.
☐	4. Honeypot isco	D	Software malicioso que encripta dados e exige um pagamento para a desencriptação.
☐	5. Firewall de intrusão	E	Exploração de uma vulnerabilidade antes de o fabricante lançar uma correção.
☐	6. Resposta a incidentes	F	Boas práticas para gerir credenciais e chaves de autenticação.
☐	7. Higiene das palavras-passe	G	Validação de segurança que exige dois ou mais fatores de autenticação.
☐	8. Quadro de segurança	H	Sistema isco criado para atrair e analisar agentes maliciosos.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

8. Exploração de uma vulnerabilidade antes de o fabricante lançar uma correção (14)

VERTICAIS

1. Barreira de rede que filtra o tráfego com base em regras de segurança (8)

2. Boas práticas para gerir credenciais e chaves de autenticação (7)

3. Diretrizes estruturadas, como as do NIST, usadas para gerir ciber-riscos (9)

4. Malware que encripta dados e exige um pagamento para os desencriptar (10)

5. Plano estruturado para tratar e atenuar violações de segurança (8)

6. Validação de segurança que exige dois ou mais fatores de autenticação (10)

7. Sistema isco montado para atrair e analisar agentes maliciosos (8)

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

8 horizontal: Exploração de uma vulnerabilidade antes de o fabricante lançar uma correção (14 letras):

VERTICAIS

1 vertical: Barreira de rede que filtra o tráfego com base em regras de segurança (8 letras):

2 vertical: Boas práticas para gerir credenciais e chaves de autenticação (7 letras):

3 vertical: Diretrizes estruturadas, como as do NIST, usadas para gerir ciber-riscos (9 letras):

4 vertical: Malware que encripta dados e exige um pagamento para os desencriptar (10 letras):

5 vertical: Plano estruturado para tratar e atenuar violações de segurança (8 letras):

6 vertical: Validação de segurança que exige dois ou mais fatores de autenticação (10 letras):

7 vertical: Sistema isco montado para atrair e analisar agentes maliciosos (8 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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

RANSOMWARE MULTIFATOR EXPLOITZERODAY HONEYPOT FIREWALL
RESPOSTA HIGIENE FRAMEWORK

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
A. RANSOMWARE
B. MULTIFATOR
C. EXPLOITZERODAY
D. HONEYPOT
E. FIREWALL
F. RESPOSTA
G. HIGIENE
H. FRAMEWORK

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

1. Barreira de rede que filtra o tráfego com base em regras de segurança.
2. Plano estruturado para tratar e atenuar violações de segurança.
3. Malware que encripta dados e exige um pagamento para os desencriptar.
4. Validação de segurança que exige dois ou mais fatores de autenticação.
5. Boas práticas para gerir credenciais e chaves de autenticação.
6. Diretrizes estruturadas, como as do NIST, usadas para gerir ciber-riscos.
7. Exploração de uma vulnerabilidade antes de o fabricante lançar uma correção.
8. Sistema isco montado para atrair e analisar agentes maliciosos.

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. RWMOARAESN
2. OXIPTAEDZY ROEL
3. EIFWALLR
4. EIEINHG
5. TFRUTAIMOL
6. OTEPHYON
7. RAOSTEPS
8. KERFMRWOA

Atividade bónus: Pensa rápido

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

1	Profissões em cibersegurança			
2	Razões para atualizar o software			
3	Coisas que uma firewall pode bloquear			
4	Sinais de alerta num email			
5	Coisas de que fazes cópia de segurança			
6	Tipos conhecidos de ciberataque			
7	Coisas que um honeypot pode atrair			
8	Informações que nunca deves partilhar			
9	Sinais de que um computador está infetado			
10	Filmes ou séries sobre hackers			
11	Camadas de segurança que podes criar			
12	Coisas a praticar num exercício de segurança			
13	Ferramentas de segurança que conheces			
14	Pessoas a quem podes pedir ajuda de TI			
15	Palavras que começam por "ciber"			

Ponto de controlo 8: Estudos de caso de cibersegurança

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

ESTUDO DE CASO 1: ESTRATÉGIA DE RECUPERAÇÃO DE RANSOMWARE

👷

Cenário: Uma rede empresarial é infetada com ransomware, que bloqueia bases de dados críticas. Os atacantes exigem um pagamento de 100 000 $ em criptomoeda. A empresa tem cópias de segurança offline de há 24 horas.

Questão para debate: Analisa os riscos de pagar e avalia a estratégia de recuperação.

ESTUDO DE CASO 2: DEFESAS CONTRA CREDENTIAL STUFFING

👷

Cenário: Um serviço online sofre um ataque de credential stuffing, com hackers a testar milhões de pares de nome de utilizador e palavra-passe roubados de outros sites.

Questão para debate: Detalha o mecanismo deste ataque e descreve dois sistemas de defesa.

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

16 18 15 20 5 7 5 15 19 9 19 20 5 13 1 3 15 13

1 21 20 5 14 20 9 3 1 3 1 15

13 21 12 20 9 6 1 20 15 18

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: Qual é o principal objetivo da cibersegurança?

O objetivo principal é proteger redes, dispositivos e dados contra o acesso não autorizado, ataques e danos acidentais.

Q2: Em que difere o phishing do spear phishing?

O phishing é uma campanha de e-mail ampla dirigida a utilizadores aleatórios, enquanto o spear phishing visa indivíduos específicos usando dados personalizados.

Q3: O que é uma firewall de rede?

Uma firewall é um sistema de segurança de rede que monitoriza e filtra o tráfego de entrada e de saída com base em regras de segurança predefinidas.

Q4: Porque é que a autenticação multifator (MFA) é necessária?

A MFA acrescenta uma camada de defesa essencial, impedindo o acesso mesmo que os atacantes roubem ou descubram as credenciais da palavra-passe principal.

Q5: O que define um vírus informático?

Um vírus é software malicioso autorreplicante que se anexa a ficheiros limpos e se propaga pelos sistemas depois de executado.

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

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

Q6: Como bloqueia o ransomware os dados locais?

O ransomware utiliza algoritmos criptográficos para encriptar os ficheiros dos utilizadores, tornando-os ilegíveis até ser aplicada uma chave de desencriptação.

Q7: O que é uma vulnerabilidade de dia zero?

Uma zero-day é uma falha de segurança num software desconhecida do fabricante, que não deixa tempo para desenvolver um patch antes da exploração.

Q8: Qual é o papel da framework do NIST?

A estrutura do NIST fornece diretrizes e normas voluntárias para ajudar as organizações a gerir e reduzir os riscos de cibersegurança.

Q9: O que é um plano de resposta a incidentes de segurança?

É um conjunto documentado de procedimentos para detetar, conter e recuperar de violações de segurança e de comprometimentos da rede.

Q10: Como é que a engenharia social explora os utilizadores?

A engenharia social usa a manipulação psicológica para levar os funcionários a revelar palavras-passe ou a transferir ficheiros maliciosos.

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 é que um ataque DDoS sobrecarrega os servidores web?

Um ataque DDoS coordena milhões de dispositivos comprometidos de uma botnet para inundar um servidor com tráfego, esgotando os limites de largura de banda e de CPU.

Q2: Qual é a diferença entre encriptação simétrica e assimétrica?

A encriptação simétrica usa uma única chave para encriptar e desencriptar, enquanto a encriptação assimétrica usa um par de chaves pública e privada.

Q3: Como executam os hackers ataques de injeção de SQL?

Os atacantes introduzem comandos SQL maliciosos em campos de formulários, levando a base de dados do backend a divulgar registos de utilizadores não autorizados.

Q4: O que é o movimento lateral em intrusões de rede?

É a técnica em que os atacantes exploram o acesso inicial a um servidor para comprometer outros sistemas interligados na rede interna.

Q5: Como redireciona a falsificação de DNS o tráfego Web?

A falsificação de DNS altera os registos da cache dos servidores de nomes, encaminhando utilizadores legítimos para sites maliciosos semelhantes em vez dos domínios de destino.

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: O que é um token de segurança de hardware?

É um dispositivo físico (como uma YubiKey) que gera provas criptográficas de autenticação, oferecendo a máxima defesa contra o phishing remoto.

Q7: Como usam as equipas de segurança honeypots de isco?

As equipas implementam servidores isca fora de produção para detetar intrusões cedo e analisar os padrões de ataque de agentes não autorizados.

Q8: O que é o princípio do privilégio mínimo?

É a norma de segurança que restringe os direitos de acesso dos utilizadores ao mínimo absolutamente necessário para desempenharem as suas funções.

Q9: Como explora um ataque Man-in-the-Middle as ligações?

Um atacante interceta e altera as comunicações entre dois dispositivos em redes não encriptadas, roubando tokens de sessão e credenciais.

Q10: O que são indicadores de comprometimento (IOC)?

Os IOC são pistas forenses de dados, como modificações invulgares do registo ou tráfego de IP não autorizado, que mostram que um sistema foi violado.

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

Os atacantes procuram constantemente servidores vulneráveis na internet e enviam emails de phishing para as caixas de entrada dos funcionários.

2. PERSPETIVA SOBRE SEGURANÇA

O erro humano, como clicar em ligações de phishing, é um fator comum nas violações de dados, razão pela qual a formação é importante.

3. PERSPETIVA SOBRE SEGURANÇA

Os custos de uma violação de dados incluem coimas, perda de clientes, investigação e reparação, e podem chegar a milhões de dólares.

4. PERSPETIVA SOBRE SEGURANÇA

A MFA resistente a phishing, como as chaves de segurança de hardware, é o tipo de MFA mais forte e o padrão que a CISA recomenda. [2]

5. PERSPETIVA SOBRE SEGURANÇA

O ransomware continua a ser uma ameaça importante para as redes empresariais, e a CISA recomenda cópias de segurança offline e encriptadas como defesa essencial. [4]

6. PERSPETIVA SOBRE SEGURANÇA

A Estrutura de Cibersegurança 2.0 do NIST (2024) tem seis funções essenciais: Governar, Identificar, Proteger, Detetar, Responder, Recuperar. [1]

7. PERSPETIVA SOBRE SEGURANÇA

Os bots de credential stuffing testam, em grande escala, pares de nome de utilizador e palavra-passe divulgados contra portais de início de sessão bancários e de comércio eletrónico.

8. PERSPETIVA SOBRE SEGURANÇA

Existem mercados de exploits zero-day em todo o mundo, onde vulnerabilidades de elevada gravidade podem ser vendidas por grandes quantias antes de serem corrigidas.

9. PERSPETIVA SOBRE SEGURANÇA

Um sistema isco (honeypot) comunica de imediato alertas de intrusão, uma vez que os utilizadores legítimos não têm razão para lhe aceder.

10. PERSPETIVA SOBRE SEGURANÇA

O Transport Layer Security (TLS) encripta as sessões do navegador, impedindo a captura de pacotes (packet sniffing) em redes Wi-Fi públicas.

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. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

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

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Soluções: Ponto de controlo 1 - Escolha múltipla

1 **Ataques de phishing** PHISHING — **Resposta correta: A**

NOTA PARA O PROFESSOR

As campanhas de phishing tentam roubar credenciais e dados sensíveis dos utilizadores através de e-mails falsificados. Citação: OWASP Secure Configuration.

2 **Proteção da conta** CHAVE MFA — **Resposta correta: A**

NOTA PARA O PROFESSOR

A autenticação multifator (MFA) com tokens de hardware proporciona a defesa mais forte do acesso às contas. Citação: NIST Digital Identity.

3 **Ameaça de ransomware** RANSOMWARE — **Resposta correta: A**

NOTA PARA O PROFESSOR

O ransomware encripta sistemas e dados críticos, exigindo o pagamento em criptomoedas pelas chaves de desencriptação. Fonte: Center for Internet Security (CIS).

4 **Vulnerabilidade zero-day** ZERO-DAY — **Resposta correta: A**

NOTA PARA O PROFESSOR

As ameaças zero-day exploram falhas de segurança desconhecidas e sem correção antes de o fabricante disponibilizar uma atualização. Citação: OWASP Secure Configuration.

5 **Quadros de segurança** ESTRUTURAS — **Resposta correta: A**

NOTA PARA O PROFESSOR

Referenciais como o NIST fornecem orientações estruturadas para ajudar as organizações a gerir e reduzir os riscos cibernéticos. Citação: NIST Digital Identity.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Phishing direcionado** PHISHING — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os ataques de phishing visam tanto redes empresariais como contas pessoais para ampliar os vetores de exploração. Citação: OWASP Secure Configuration.

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

NOTA PARA O PROFESSOR

A MFA exige um segundo fator, pelo que uma palavra-passe roubada, por si só, normalmente não basta para iniciar sessão.

8 **Firewall de tráfego** FIREWALL — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

As firewalls inspecionam e bloqueiam o tráfego em portas de rede específicas para filtrar ligações não autorizadas. Citação: Center for Internet Security (CIS).

9 **Resposta a zero-day** ZERO-DAY — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Corrigir falhas zero-day exige correções de código e filtragem por WAF, uma vez que ainda não existem assinaturas. Citação: OWASP Secure Configuration.

10 **Honeypots de engodo** HONEYPOT — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os honeypots são servidores de engodo usados pelas equipas de segurança para atrair, alertar e estudar agentes maliciosos. Citação: Center for Internet Security (CIS).

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

D 1. Ameaça de ransomware	G 2. Autenticação multifator	E 3. Exploração de dia zero	H 4. Honeypot isco
C 5. Firewall de intrusão	B 6. Resposta a incidentes	F 7. Higiene das palavras-passe	A 8. Quadro de segurança

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 FIREWALL	2 EXPLOIT ZERO-DAY	3 PHISHING	4 MALWARE
5 HIGIENE	6 ENCRIPTAÇÃO		

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

1 E – FIREWALL	2 F – RESPOSTA	3 A – RANSOMWARE	4 B – MULTIFATOR
5 G – HIGIENE	6 H – FRAMEWORK	7 C – EXPLOITZERODAY	8 D – HONEYPOT

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Ameaça de ransomware, Autenticação multifator e Exploração de dia zero 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.

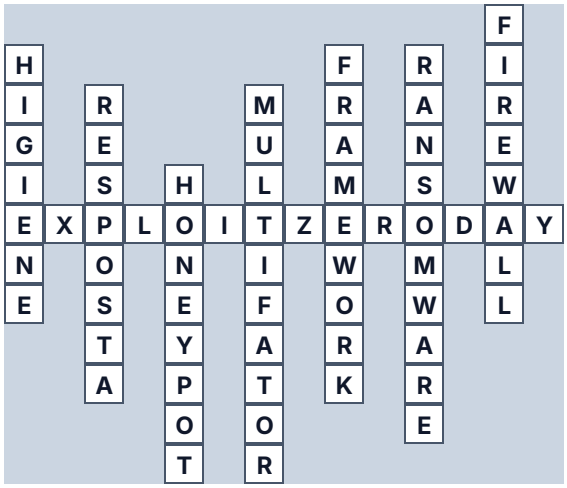
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

8 horizontal: EXPLOITZERODAY Exploração de uma vulnerabilidade antes de o fabricante lançar uma correção (14 letras)

VERTICAIS

1 vertical: FIREWALL Barreira de rede que filtra o tráfego com base em regras de segurança (8 letras)

2 vertical: HIGIENE Boas práticas para gerir credenciais e chaves de autenticação (7 letras)

3 vertical: FRAMEWORK Diretrizes estruturadas, como as do NIST, usadas para gerir ciber-riscos (9 letras)

4 vertical: RANSOMWARE Malware que encripta dados e exige um pagamento para os desencriptar (10 letras)

5 vertical: RESPOSTA Plano estruturado para tratar e atenuar violações de segurança (8 letras)

6 vertical: MULTIFATOR Validação de segurança que exige dois ou mais fatores de autenticação (10 letras)

7 vertical: HONEYPOT Sistema isco montado para atrair e analisar agentes maliciosos (8 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. RWMOARAESN — **RANSOMWARE**
2. OXIPTAEDZYROEL — **EXPLOITZERODAY**
3. EIFWALLR — **FIREWALL**
4. EIEINHG — **HIGIENE**
5. TFRUTAIMOL — **MULTIFATOR**
6. OTEPHYON — **HONEYPOT**
7. RAOSTEPS — **RESPOSTA**
8. KERFMRWOA — **FRAMEWORK**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"PROTEGE O SISTEMA COM AUTENTICACAO MULTIFATOR"

Soluções dos estudos de caso

A Estudo de caso 1: Estratégia de recuperação de ransomware

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Uma rede empresarial está infetada com ransomware, que bloqueia bases de dados críticas. Os atacantes exigem um pagamento de 100 000 $ em criptomoeda. A empresa tem cópias de segurança offline de há 24 horas.
- Estratégia e solução recomendadas: Riscos de pagar: Pagar não garante a desencriptação dos ficheiros, rotula a empresa como alvo que paga e financia atividade criminosa. Estratégia de recuperação: A equipa deve isolar os anfitriões infetados, apagar os servidores comprometidos e restaurar os dados a partir de cópias de segurança offline. Tem de corrigir o vetor de acesso inicial (phishing ou exploração de vulnerabilidade) para evitar uma reinfeção imediata.

B Estudo de caso 2: Defesas contra credential stuffing

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Um serviço online sofre um ataque de credential stuffing, em que hackers testam milhões de pares de nome de utilizador/palavra-passe roubados de outros sites.
- Estratégia e solução recomendadas: Mecanismo: Os atacantes tiram partido da reutilização de palavras-passe em vários sites, usando bots automatizados para iniciar sessão em contas de utilizadores. Defesas: 1. A autenticação multifator (MFA) bloqueia tentativas de início de sessão mesmo que a palavra-passe esteja correta. 2. Implementar limitação de taxa e CAPTCHAs bloqueia o tráfego de bots automatizados que inundam os pontos de início de sessão.