Nome: _____ **Data:** _____ **Punteggio:** _____

Protezione dei dati e archiviazione aziendale Guida alla sicurezza

Mascheramento dei dati, tokenizzazione, crittografia dei dati a riposo e in transito, backup offline

PANORAMICA DI APPRENDIMENTO SULLA PROTEZIONE DEI DATI

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso gli standard e i controlli di protezione dei dati. Esplorerai la crittografia dell'intero disco, i controlli di accesso sicuri, i backup hardware, la postura di sicurezza del cloud e le tecniche di mascheramento dei dati.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/protezione-dei-dati/

Il tuo percorso di apprendimento sulla strategia di protezione dei dati

- Distingui tra le tecniche di mascheramento dei dati e di tokenizzazione.
- Implementa la crittografia dei dati a riposo per le unità di archiviazione e la crittografia in transito tramite TLS.
- Progetta sistemi di backup offline e isolati dalla rete per la protezione dal ransomware.

ISTRUZIONI DELLA GUIDA ALLA PROTEZIONE DEI DATI

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze alla protezione dei dati. Concludi con l'attività bonus Pensa veloce.

PROTEZIONE DEI DATI E SICUREZZA DELLO STORAGE AZIENDALE (INTRODUZIONE)

La protezione dei dati salvaguarda gli asset di dati aziendali tramite mascheramento, tokenizzazione, crittografia dei database a riposo e protocolli di transito sicuri. Progettare backup isolati dalla rete aiuta a garantire che i database principali possano essere ripristinati in caso di intrusione attiva.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Qual è lo scopo principale del data masking?

- A. Sostituire gli identificatori sensibili con caratteri fittizi ma realistici per proteggere la privacy
- B. Comprimere grandi file di database per risparmiare spazio di archiviazione fisico del server
- C. Eliminare le vecchie email di contatto dei clienti dai sistemi di backup di archivio
- D. Nascondere l'indirizzo IP pubblico del server del database dalle scansioni di internet

2. Quale meccanismo cifra i file archiviati sul disco rigido di un server di database?

- A. Cifratura dell'intero disco a riposo
- B. Protocolli di handshake della sessione TLS in transito
- C. Regole di inoltro dei nameserver DNS dinamico
- D. Autenticazione a più fattori con chiavi hardware

3. Che cosa rappresentano i dati in transito?

- A. Pacchetti di dati che si spostano attraverso router e switch di rete
- B. Log delle transazioni del database archiviati su un'unità di backup offline
- C. File utente archiviati salvati in un caveau cloud isolato
- D. File di configurazione di sistema statici su un archivio desktop locale

4. Perché un backup offline regolare è fondamentale per la protezione dal ransomware?

- A. Fornisce una copia pulita offline per ripristinare i file senza pagare un riscatto
- B. Impedisce agli hacker di scansionare le configurazioni delle porte aperte
- C. Aumenta la velocità di trasmissione della banda della rete locale
- D. Automatizza i log di consenso ai cookie nei browser

5. Che cosa fa la tokenizzazione dei dati?

- A. Sostituisce i numeri di carta sensibili con token casuali non sensibili
- B. Instrada il traffico web attraverso più nodi onion sicuri
- C. Analizza le directory di sistema alla ricerca di malware basato su firme
- D. Controlla gli orari delle sessioni di accesso degli amministratori del database

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Il mascheramento dei dati modifica in modo permanente i record del database negli ambienti di produzione.

Vero Falso

7 Domanda 7

7. I backup offsite devono essere isolati dalla rete aziendale principale per evitare la propagazione del ransomware.

Vero Falso

8 Domanda 8

8. I certificati SSL/TLS proteggono i database crittografando i dati archiviati a riposo sui supporti fisici.

Vero Falso

9 Domanda 9

9. Lo Zero Trust Network Access (ZTNA) verifica l'identità di ogni utente prima di concedere l'accesso al database.

Vero Falso

10 Domanda 10

10. La tokenizzazione basata su vault conserva i valori originali delle carte in un vault di token centrale e sicuro.

Vero Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Sostituire i nomi personali con segnaposto realistici si chiama _____ dei dati.
2. Cifrare i blocchi di archiviazione fisica protegge le risorse del database _____ .
3. I protocolli TLS cifrano i pacchetti di dati attivi che si spostano in _____ .
4. I permessi basati sui ruoli limitano gli utenti che possono ottenere l' _____ al database.
5. Ripristinare file aziendali puliti dopo una violazione richiede un _____ offline sicuro.
6. La verifica delle configurazioni cloud valuta la _____ di sicurezza di un'organizzazione.

BANCA DELLE PAROLE DEL VOCABOLARIO

A RIPOSO ACCESSO BACKUP CRITTOGRAFIA MASCHERAMENTO MINIMIZZAZIONE POSTURA TRANSITO

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

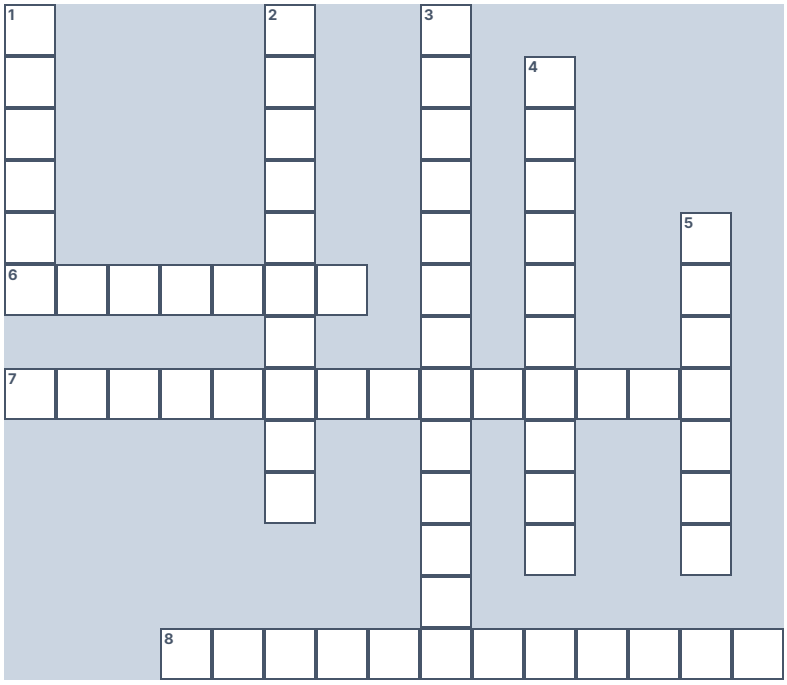
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. CRITTOGRAFIA	A	Creare copie sicure dei dati all'esterno per ripristinarli in caso di guasti del sistema.
☐	2. BACKUP	B	Trasformare il testo in chiaro in testo cifrato illeggibile in modo che i dati intercettati restino privati.
☐	3. MINIMIZZAZIONE	C	Lo stato di sicurezza complessivo e la prontezza difensiva del cloud di un'organizzazione.
☐	4. ACCESSO	D	Rispettare gli standard normativi come GDPR o CCPA per la gestione delle informazioni private degli utenti.
☐	5. POSTURA DI SICUREZZA	E	Incidente di sicurezza in cui i dati protetti vengono consultati o divulgati senza autorizzazione.
☐	6. VIOLAZIONE	F	Limitazione dei permessi di lettura e scrittura del database ai ruoli utente autenticati.
☐	7. CONFORMITÀ	G	Sostituzione dei caratteri sensibili nei campi del database per proteggere le identità personali.
☐	8. MASCHERAMENTO	H	Limitare la raccolta di dati personali al minimo assoluto necessario per le operazioni.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

6. Lo stato complessivo di sicurezza e la prontezza di difesa del cloud di un'organizzazione. (7)

7. Limitare la raccolta di dati personali al minimo indispensabile per le operazioni. (14)

8. Trasformare il testo in chiaro in testo cifrato illeggibile in modo che i dati intercettati restino privati (12)

VERTICALI

1. Creare copie sicure dei dati fuori sede da ripristinare in caso di guasti del sistema. (6)

2. Rispettare standard normativi come GDPR o CCPA nella gestione delle informazioni private degli utenti. (10)

3. Sostituire i caratteri sensibili nei campi del database per proteggere le identità personali. (13)

4. Incidente di sicurezza in cui i dati protetti vengono consultati o divulgati senza autorizzazione (10)

5. Limitare i permessi di lettura e scrittura del database ai ruoli utente autenticati. (7)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

6 orizzontale: Lo stato complessivo di sicurezza e la prontezza di difesa del cloud di un'organizzazione. (7 lettere):

7 orizzontale: Limitare la raccolta di dati personali al minimo indispensabile per le operazioni. (14 lettere):

8 orizzontale: Trasformare il testo in chiaro in testo cifrato illeggibile in modo che i dati intercettati restino privati (12 lettere):

VERTICALI

1 verticale: Creare copie sicure dei dati fuori sede da ripristinare in caso di guasti del sistema. (6 lettere):

2 verticale: Rispettare standard normativi come GDPR o CCPA nella gestione delle informazioni private degli utenti. (10 lettere):

3 verticale: Sostituire i caratteri sensibili nei campi del database per proteggere le identità personali. (13 lettere):

4 verticale: Incidente di sicurezza in cui i dati protetti vengono consultati o divulgati senza autorizzazione (10 lettere):

5 verticale: Limitare i permessi di lettura e scrittura del database ai ruoli utente autenticati. (7 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

O K T S V R Z E H E S C A L Q

T C E N O I Z A L O I V Z P A

N M K V B A C K U P R U O C A

E S W J M M H H N H R S C F K

M T L R W H B U F Y T E O Y W

A S H T X A P U N U S N Z O I

R Q T I P V U O R S U U K A E

E P M K A N V A O G G P Q X Y

H J K V J Y W Y P J I Z I J N

C A A T I M R O F N O C E I A

S M I N I M I Z Z A Z I O N E

A S A J F W E K Z K E K Q N J

M A C R I T T O G R A F I A F

O K N D N C D H I B A P R L P

W T I Y F Y S G X W H F R T N

ELENCO DELLE PAROLE DEL VOCABOLARIO

CRITTOGRAFIA BACKUP MINIMIZZAZIONE ACCESSO POSTURA VIOLAZIONE CONFORMITÀ MASCHERAMENTO

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO

- **A. CRITTOGRAFIA**
- **B. BACKUP**
- **C. MINIMIZZAZIONE**
- **D. ACCESSO**
- **E. POSTURA**
- **F. VIOLAZIONE**
- **G. CONFORMITÀ**
- **H. MASCHERAMENTO**

DEFINIZIONI E CAMPI DI ABBINAMENTO

_____ 1. Incidente di sicurezza in cui i dati protetti vengono consultati o divulgati senza autorizzazione.

_____ 2. Sostituire i caratteri sensibili nei campi del database per proteggere le identità personali.

_____ 3. Limitare i permessi di lettura e scrittura del database ai ruoli utente autenticati.

_____ 4. Lo stato complessivo di sicurezza e la prontezza di difesa del cloud di un'organizzazione.

_____ 5. Rispettare standard normativi come GDPR o CCPA nella gestione delle informazioni private degli utenti.

_____ 6. Limitare la raccolta di dati personali al minimo indispensabile per le operazioni.

_____ 7. Trasformare il testo in chiaro in testo cifrato illeggibile in modo che i dati intercettati restino privati.

_____ 8. Creare copie sicure dei dati fuori sede da ripristinare in caso di guasti del sistema.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. AORTRGFCIIAT
2. MIINZNMOZEZIAI
3. TPUASRO
4. RTOAFIMCON
5. KCPBUA
6. SCSAEOC
7. ILVIZONEAO
8. MSHENAOMRATEC

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Cose di cui fai il backup			
2	Parole legate alla sicurezza informatica			
3	Persone autorizzate a vedere dati sensibili			
4	Modi per eliminare i dati in modo sicuro			
5	Luoghi in cui vengono conservati i dati			
6	Cose che dovrebbero essere cifrate			
7	Dati che un ospedale deve proteggere			
8	Tipi di backup			
9	Informazioni che non dovresti mai condividere			
10	Segnali di allarme in un'email			
11	Buone abitudini sicure che puoi iniziare oggi			
12	Persone a cui puoi chiedere aiuto per l'IT			
13	Dispositivi che possono essere hackerati			
14	Modi per proteggere i dati			
15	Cose che possono distruggere i dati			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: AGGIORNAMENTO DELLA CRITTOGRAFIA A RIPOSO DEL DATABASE AZIENDALE

👷

Scenario: Un rivenditore online conserva i database delle transazioni su un archivio cloud senza cifratura dell'intero disco. Un recente audit di conformità lo ha segnalato come un grave rischio per la sicurezza dei dati ai sensi del CCPA. Progetta un'architettura di ripristino.

Domanda di discussione: Analizza i rischi di conformità al CCPA e proponi una strategia di cifratura dei dati a riposo.

CASO DI STUDIO 2: CONTENIMENTO DEL RANSOMWARE E RIPRISTINO DEI DATI

👷

Scenario: Un attacco ransomware in corso sta cifrando le unità di rete di una rete locale aziendale. L'amministratore ha rilevato l'infezione tempestivamente. Pianifica i passaggi di contenimento e ripristino.

Domanda di discussione: Descrivi nel dettaglio le azioni di contenimento immediate e pianifica un processo di ripristino sicuro.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

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 7 9 9 4 1 20 9

16 18 9 22 1 20 9 3 15 14 3 15 14 20 18 15 12 12 9

19 9 3 21 18 9

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Che cos'è la protezione dei dati?

È il processo di protezione dei dati personali e aziendali da accessi non autorizzati, perdita o corruzione tramite controlli tecnici.

Q2: Perché la cifratura dell'intero disco è importante?

Protegge i blocchi di dati archiviati sulle unità fisiche, impedendo a chiunque di leggere i dati se ruba fisicamente il disco rigido.

Q3: Qual è la differenza tra cifratura dei dati inattivi e dei dati in transito?

La crittografia a riposo protegge i file memorizzati sui dischi, mentre la crittografia in transito protegge i pacchetti di rete attivi che si spostano attraverso i router.

Q4: Cos'è il data masking?

Sostituisce i dettagli sensibili (come i numeri di carta di credito) con dati fittizi ma realistici per i test, senza esporre record reali.

Q5: Perché il backup offline è importante?

Conserva una copia pulita dei tuoi file isolata dalla rete, il che aiuta a proteggere i tuoi backup dalla cifratura da parte del ransomware.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Cos'è un vault di tokenizzazione dei dati?

Un database sicuro e isolato che associa token casuali ai loro valori sensibili originali (come i numeri principali delle carte di credito).

Q7: Cosa significa accesso al database Zero Trust?

Significa verificare l'identità e lo stato del dispositivo di ogni utente a ogni accesso, anziché fidarsi di chiunque si trovi all'interno della rete.

Q8: Come protegge i dati in transito TLS?

TLS crittografa il payload della sessione TCP, impedendo ad attori malevoli sulle reti pubbliche di intercettare o modificare i pacchetti in transito.

Q9: Cos'è l'auditing degli accessi al database?

La registrazione continua delle query al database e degli accessi per rilevare schemi di accesso non autorizzato o anomalie di sicurezza.

Q10: Che cos'è un audit della postura di sicurezza del cloud?

Un processo che analizza le configurazioni cloud per individuare porte aperte, regole di accesso configurate in modo errato e lacune nella conformità alla sicurezza.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come funziona la crittografia a busta?

Cifra i dati con una chiave dati, poi cifra quella chiave dati con una chiave master, semplificando l'archiviazione e la rotazione delle chiavi.

Q2: Che cos'è la crittografia omomorfica?

Un metodo avanzato di cifratura che consente di eseguire operazioni direttamente sui dati cifrati senza prima decifrarli.

Q3: Perché si usa la cifratura a livello di colonna nei database?

Cifra singolarmente specifiche colonne sensibili (come gli SSN), proteggendole anche se gli amministratori ottengono l'accesso generale in lettura alla tabella.

Q4: Cos'è la prevenzione della perdita di dati (DLP)?

Software che monitora i punti di uscita della rete per rilevare e bloccare i trasferimenti in uscita non autorizzati di file sensibili.

Q5: Come proteggono dal ransomware i backup WORM (write-once-read-many)?

I backup WORM impediscono che i file vengano eliminati o modificati per una durata stabilita, evitando che il ransomware crittografi i backup esistenti.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: Qual è il rischio del riutilizzo delle chiavi?

Riutilizzare la stessa chiave crittografica su database diversi significa che la compromissione di una sola chiave espone tutti i database.

Q7: Come migliora la conformità al CCPA la tokenizzazione del database?

I token pseudonimizzano i record nei sistemi non di produzione e limitano l'esposizione in caso di violazione, ma i dati tokenizzati possono comunque essere informazioni personali.

Q8: Perché la classificazione dei dati è fondamentale?

Classifica i file in base al livello di sensibilità, aiutando le organizzazioni ad applicare la crittografia e i controlli di accesso più forti ai dati ad alto rischio.

Q9: Qual è il ruolo della rotazione delle chiavi?

Aggiornare regolarmente le chiavi di crittografia limita la quantità di dati storici esposti se una singola chiave viene prima o poi violata.

Q10: Come proteggono le enclave sicure le query al database in memoria?

Le enclave sicure isolano le operazioni di query in blocchi di memoria protetti dalla CPU, impedendo agli amministratori dell'host di vedere il testo in chiaro nella RAM.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

Il regolamento GDPR è entrato in vigore a maggio 2018, cambiando il modo in cui i siti globali gestiscono i consensi ai cookie e i registri dei dati personali.

2. APPROFONDIMENTO SULLA SICUREZZA

Una sanzione per violazione del GDPR può arrivare a 20 milioni di euro o al 4% del fatturato globale, il che rappresenta un'esposizione legale notevole. [4]

3. APPROFONDIMENTO SULLA SICUREZZA

Il CCPA è entrato in vigore nel gennaio 2020, stabilendo diritti pionieristici dei consumatori in materia di privacy digitale negli Stati Uniti.

4. APPROFONDIMENTO SULLA SICUREZZA

La minimizzazione dei dati riduce lo spazio occupato dal database, abbassando i costi operativi dei server e diminuendo l'impatto delle violazioni.

5. APPROFONDIMENTO SULLA SICUREZZA

La distruzione crittografica risolve il problema dell'eliminazione dai backup eliminando le chiavi invece di modificare i file storici dei nastri di backup.

6. APPROFONDIMENTO SULLA SICUREZZA

Oggi la maggior parte dei paesi del mondo ha adottato leggi sulla protezione dei dati personali per tutelare i diritti alla privacy dei consumatori.

7. APPROFONDIMENTO SULLA SICUREZZA

I moduli di consenso opt-in con caselle preselezionate sono espressamente vietati dalle definizioni normative europee sulla privacy dei dati.

8. APPROFONDIMENTO SULLA SICUREZZA

Il GDPR richiede di notificare le violazioni dei dati personali all'autorità di controllo entro 72 ore dalla scoperta, ove possibile. [3]

9. APPROFONDIMENTO SULLA SICUREZZA

L'hashing delle password con algoritmi lenti come bcrypt o Argon2 rende molto più difficile il cracking offline degli hash rubati. [6]

10. APPROFONDIMENTO SULLA SICUREZZA

I dati a riposo sono i file di database salvati, mentre i dati in transito sono i pacchetti che si spostano attivamente attraverso i router di rete.

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1 — **Risposta corretta: A**

NOTA DIDATTICA

Qual è lo scopo principale del data masking? → Sostituire gli identificatori sensibili con caratteri fittizi ma realistici per proteggere la privacy

2 Domanda 2 — **Risposta corretta: A**

NOTA DIDATTICA

Quale meccanismo cifra i file archiviati sul disco rigido di un server di database? → Cifratura dell'intero disco a riposo

3 Domanda 3 — **Risposta corretta: A**

NOTA DIDATTICA

Che cosa rappresentano i dati in transito? → Pacchetti di dati che si spostano attraverso router e switch di rete

4 Domanda 4 — **Risposta corretta: A**

NOTA DIDATTICA

Perché un backup offline regolare è fondamentale per la protezione dal ransomware? → Fornisce una copia pulita offline per ripristinare i file senza pagare un riscatto

5 Domanda 5 — **Risposta corretta: A**

NOTA DIDATTICA

Che cosa fa la tokenizzazione dei dati? → Sostituisce i numeri di carta sensibili con token casuali non sensibili

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Falso**

NOTA DIDATTICA

Il masking altera le copie di test o nasconde i valori al momento della query; i record di produzione restano invariati.

7 **Domanda 7** — **Risposta corretta: Vero**

NOTA DIDATTICA

I backup offsite devono essere isolati dalla rete aziendale principale per evitare la propagazione del ransomware.

8 **Domanda 8** — **Risposta corretta: Falso**

NOTA DIDATTICA

I certificati TLS proteggono i dati in transito; i dati a riposo richiedono la cifratura di disco, file o database.

9 **Domanda 9** — **Risposta corretta: Vero**

NOTA DIDATTICA

Lo Zero Trust Network Access (ZTNA) verifica l'identità di ogni utente prima di concedere l'accesso al database.

10 **Domanda 10** — **Risposta corretta: Vero**

NOTA DIDATTICA

La tokenizzazione basata su vault conserva i valori originali in un vault di token sicuro che associa ogni token ai suoi dati.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

B 1. CRITTOGRAFIA	A 2. BACKUP	H 3. MINIMIZZAZIONE	F 4. ACCESSO
C 5. POSTURA DI SICUREZZA	E 6. VIOLAZIONE	D 7. CONFORMITÀ	G 8. MASCHERAMENTO

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 MASCHERAMENTO	2 A RIPOSO	3 TRANSITO	4 ACCESSO
5 BACKUP	6 POSTURA		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 F – VIOLAZIONE	2 H – MASCHERAMENTO	3 D – ACCESSO	4 E – POSTURA
5 G – CONFORMITÀ	6 C – MINIMIZZAZIONE	7 A – CRITTOGRAFIA	8 B – BACKUP

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare CRITTOGRAFIA, BACKUP e MINIMIZZAZIONE con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

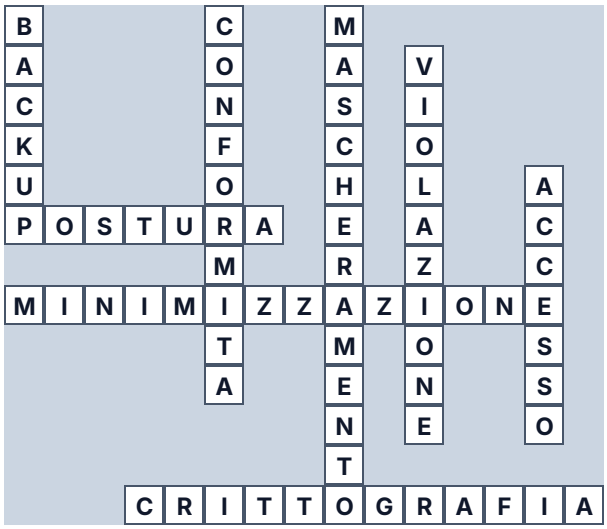
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

6 orizzontale: POSTURA Lo stato complessivo di sicurezza e la prontezza di difesa del cloud di un'organizzazione. (7 lettere)

7 orizzontale: MINIMIZZAZIONE Limitare la raccolta di dati personali al minimo indispensabile per le operazioni. (14 lettere)

8 orizzontale: CRITTOGRAFIA Trasformare il testo in chiaro in testo cifrato illeggibile in modo che i dati intercettati restino privati (12 lettere)

VERTICALI

1 verticale: BACKUP Creare copie sicure dei dati fuori sede da ripristinare in caso di guasti del sistema. (6 lettere)

2 verticale: CONFORMITÀ Rispettare standard normativi come GDPR o CCPA nella gestione delle informazioni private degli utenti. (10 lettere)

3 verticale: MASCHERAMENTO Sostituire i caratteri sensibili nei campi del database per proteggere le identità personali. (13 lettere)

4 verticale: VIOLAZIONE Incidente di sicurezza in cui i dati protetti vengono consultati o divulgati senza autorizzazione (10 lettere)

5 verticale: ACCESSO Limitare i permessi di lettura e scrittura del database ai ruoli utente autenticati. (7 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. AORTRGFCIIAT — **CRITTOGRAFIA**
2. MIINZNMOZEZIAI — **MINIMIZZAZIONE**
3. TPUASRO — **POSTURA**
4. RTOAFIMCON — **CONFORMITÀ**
5. KCPBUA — **BACKUP**
6. SCSAEOC — **ACCESSO**
7. ILVIZONEAO — **VIOLAZIONE**
8. MSHENAOMRATEC — **MASCHERAMENTO**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"PROTEGGI I DATI PRIVATI CON CONTROLLI SICURI"

Soluzioni dei casi di studio

A Caso di studio 1: aggiornamento della crittografia a riposo del database aziendale

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un rivenditore online archivia i database delle transazioni su un cloud storage senza crittografia dell'intero disco. Un recente audit di conformità lo ha segnalato come un grave rischio per la sicurezza dei dati ai sensi del CCPA. Progetta un'architettura di ripristino.
- Strategia e soluzione consigliate: Implementa la crittografia dell'intero disco AES-256 a riposo su tutti i file system. Usa un servizio di gestione delle chiavi (KMS) centralizzato con rotazione automatica e applica criteri IAM rigorosi per controllare l'accesso alla decrittografia.

B Caso di studio 2: Contenimento del ransomware e ripristino dei dati

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un attacco ransomware attivo sta crittografando le unità di rete di una rete locale aziendale. L'amministratore ha rilevato l'infezione in anticipo. Pianifica i passaggi di contenimento e di ripristino.
- Strategia e soluzione consigliate: Isola subito il segmento compromesso. Formatta gli endpoint interessati e ripristina dal più recente backup offline write-once-read-many (WORM). Verifica l'integrità del backup prima di ricollegare i sistemi.