Nombre: _____ **Fecha:** _____ **Puntuación:** _____

Filtraciones de contraseñas y seguridad de las credenciales

Relleno de credenciales, filtraciones de datos, algoritmos de hash, autenticación multifactor y seguridad de las contraseñas.

RESUMEN DE APRENDIZAJE: FILTRACIONES DE CONTRASEÑAS

PROTEGIDO
CIFRADO DE DATOS
Estándar AES de 256 bits

CONFORME
ESTÁNDARES GLOBALES
Marcos del RGPD (GDPR) y la CCPA

CONFIANZA CERO
POLÍTICA DE ACCESO
Autenticación multifactor

¡Hola! Este paquete de actividades te guía por las filtraciones de contraseñas y la seguridad de las credenciales. Explorarás el relleno de credenciales (credential stuffing), las brechas de datos, los algoritmos de hash, la autenticación multifactor y los gestores de contraseñas.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina la ciberseguridad y la prevención de amenazas.**
- [ ] **Partes 5-7: Resuelve crucigramas y sopas de letras.**
- [ ] **Partes 8-9: Resuelve casos prácticos y el reto de cifrado.**
- [ ] **Parte 10: Repasa las páginas de preguntas frecuentes básicas y avanzadas.**
- [ ] **Parte 11: Explora 10 datos reales interesantes.**
- [ ] **Extra: reto Piensa rápido.**

Abre la guía de ciberseguridad de VPN.com

URL: https://www.vpn.com/es/ciberseguridad/filtracion-contrasenas/

Tu hoja de ruta de aprendizaje sobre seguridad de contraseñas

- Comprende los riesgos de exposición de credenciales en los foros de la dark web.
- Implantar la autenticación multifactor (MFA) y la supervisión de credenciales comprometidas.
- Diseña defensas de seguridad corporativas contra estafas dirigidas de ingeniería social.

INSTRUCCIONES DE LA GUÍA SOBRE FILTRACIONES DE CONTRASEÑAS

Responde a las preguntas de opción múltiple y de verdadero/falso, completa las frases con huecos usando el banco de palabras, relaciona las definiciones y resuelve el crucigrama y la sopa de letras. Aplica tus conocimientos a la protección de credenciales. Termina con la actividad extra Piensa rápido.

FILTRACIONES DE CONTRASEÑAS Y SEGURIDAD DE LAS CREDENCIALES (INTRODUCCIÓN)

Las filtraciones de contraseñas exponen las credenciales de los usuarios en sitios públicos y de la dark web. Las contraseñas únicas de un gestor de contraseñas, la comprobación de contraseñas filtradas y la autenticación multifactor (MFA) reducen el riesgo de relleno de credenciales, mientras que un hash de contraseñas lento y con sal limita el daño si se roba una base de datos de contraseñas.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA RESPUESTA CORRECTA.

Punto de control 1: Reto de opción múltiple

1. ¿Qué es el relleno de credenciales (credential stuffing)?

- A. Usar la automatización para probar combinaciones filtradas de usuario y contraseña en varios sitios
- B. Cifrar los archivos de almacenamiento de la base de datos local
- C. Saturar servidores web con peticiones de tráfico de red
- D. Supervisar en secreto lo que se escribe con el teclado

2. ¿Qué algoritmo recomienda OWASP actualmente como primera opción para almacenar contraseñas?

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. ¿Cómo mitiga la autenticación multifactor (MFA) el riesgo de filtración de contraseñas?

- A. Exige un factor de verificación adicional, por lo que una contraseña robada por sí sola no basta
- B. Cambia la contraseña automáticamente cada hora
- C. Cifra el nombre de usuario durante la transmisión
- D. Avisa a la agencia de crédito de las solicitudes fraudulentas

4. ¿Qué es un volcado de una filtración de datos?

- A. Una recopilación de credenciales de usuarios filtradas que se publica en internet o se vende en foros de hackers
- B. Una copia de seguridad de los archivos de la base de datos almacenada fuera de las instalaciones
- C. Una caché temporal de los registros del servidor web
- D. Una herramienta administrativa para restablecer las contraseñas de los usuarios

5. ¿Qué función cumple un gestor de contraseñas?

- A. Generar y guardar contraseñas únicas y seguras para cada cuenta
- B. Supervisar el tráfico de red en busca de filtraciones de contraseñas
- C. Bloquear ataques automatizados de fuerza bruta en la pasarela
- D. Analizar los bloques de almacenamiento de la base de datos en busca de contraseñas sin cifrar

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Reutilizar contraseñas en varias cuentas aumenta el riesgo de relleno de credenciales (credential stuffing).

- ◯ Verdadero
- ◯ Falso

7 Pregunta 7

7. SHA-1 es una función hash recomendada para almacenar contraseñas hoy en día.

- ◯ Verdadero
- ◯ Falso

8 Pregunta 8

8. Exigir solo contraseñas complejas (sin MFA) detiene por completo el relleno de credenciales.

- ◯ Verdadero
- ◯ Falso

9 Pregunta 9

9. Las herramientas de supervisión de la dark web rastrean internet en busca de credenciales corporativas comprometidas.

- ◯ Verdadero
- ◯ Falso

10 Pregunta 10

10. Los hash con sal añaden datos aleatorios únicos a las contraseñas antes de aplicar el hash para frustrar los ataques con tablas arcoíris.

- ◯ Verdadero
- ◯ Falso

Punto de control 3: Inserción de términos clave

Lee cada una de las frases siguientes y rellena el espacio en blanco con el término correcto del banco de palabras.

1. Probar credenciales filtradas en muchas aplicaciones web se denomina _____ de credenciales.

2. Un algoritmo de hash de contraseñas lento y adaptativo que OWASP todavía acepta es _____ .

3. La exposición en internet de archivos confidenciales de una base de datos es una _____ de datos.

4. Añadir valores aleatorios a las contraseñas antes de aplicarles el hash se denomina _____ .

5. Una base de datos local y segura para las credenciales de usuario es un _____ de contraseñas.

6. Añadir un segundo paso de verificación al iniciar sesión utiliza la autenticación _____ .

BANCO DE PALABRAS DE VOCABULARIO

ARCOÍRIS BCRYPT BRECHA GESTOR MULTIFACTOR PHISHING RELLENO SALADO

Escribe aquí tus respuestas:

1. | **2.**

3. | **4.**

5. | **6.**

Punto de control 4: Relación de conceptos de seguridad

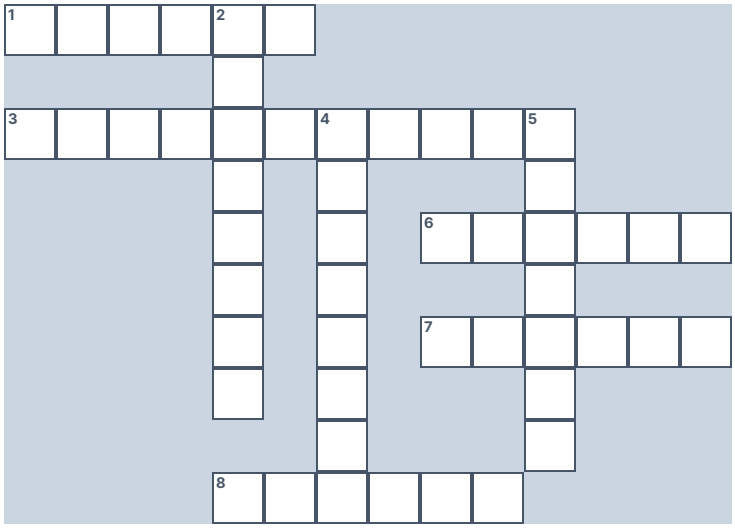
RELACIÓN DE DEFINICIONES

Relaciona cada término de vocabulario de la izquierda con su definición correcta de la derecha escribiendo la letra correspondiente (A-H) en la casilla rellenable.

☐	1. RELLENO DE CREDENCIALES	A	Tabla precalculada de hashes de contraseñas.
☐	2. BCRYPT	B	Verificación de inicio de sesión multifactor.
☐	3. BRECHA	C	Herramienta para guardar credenciales.
☐	4. SALADO	D	Exposición no autorizada de una base de datos.
☐	5. GESTOR	E	Ingeniería social para robar credenciales de acceso.
☐	6. MFA	F	Probar credenciales filtradas.
☐	7. ARCOÍRIS	G	Añadir sal aleatoria al hash de la contraseña.
☐	8. PHISHING	H	Algoritmo lento de hash de contraseñas.

Punto de control 5: Crucigrama

Resuelve el crucigrama escribiendo letras en las casillas blancas activas. Los números corresponden a las pistas de abajo.



HORIZONTALES

1. Algoritmo lento de hash de contraseñas. (6)

3. Comprobación de inicio de sesión con varios factores (MFA). (11)

6. Adición de una sal aleatoria al hash de una contraseña. (6)

7. Exposición no autorizada de una base de datos. (6)

8. Herramienta para almacenar credenciales. (6)

VERTICALES

2. Ingeniería social para robar datos de acceso. (8)

4. Tabla precalculada de hashes de contraseñas. (8)

5. Prueba de credenciales filtradas (___ de credenciales). (7)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

Los usuarios de lectores de pantalla y de teclado pueden escribir las respuestas del crucigrama directamente en los campos de texto de abajo.

HORIZONTALES

1 horizontal: Algoritmo lento de hash de contraseñas. (6 letras):

3 horizontal: Comprobación de inicio de sesión con varios factores (MFA). (11 letras):

6 horizontal: Adición de una sal aleatoria al hash de una contraseña. (6 letras):

7 horizontal: Exposición no autorizada de una base de datos. (6 letras):

8 horizontal: Herramienta para almacenar credenciales. (6 letras):

VERTICALES

2 vertical: Ingeniería social para robar datos de acceso. (8 letras):

4 vertical: Tabla precalculada de hashes de contraseñas. (8 letras):

5 vertical: Prueba de credenciales filtradas (___ de credenciales). (7 letras):

Punto de control 6: Sopa de letras

Encuentra los 8 términos clave del vocabulario ocultos en la cuadrícula de abajo. Las palabras pueden estar en horizontal, en vertical o en diagonal.

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

LISTA DE PALABRAS DE VOCABULARIO

RELLENO BCRYPT BRECHA SALADO GESTOR MULTIFACTOR ARCOIRIS PHISHING

Punto de control 6, alternativa: Relación de vocabulario accesible

Relaciona cada uno de los 8 términos de vocabulario de la sopa de letras con su definición correcta escribiendo la letra (A-H) en el espacio en blanco.

TÉRMINOS DE VOCABULARIO
A. RELLENO
B. BCRYPT
C. BRECHA
D. SALADO
E. GESTOR
F. MULTIFACTOR
G. ARCOIRIS
H. PHISHING

DEFINICIONES Y CAMPOS DE RELACIÓN

1. Ingeniería social para robar datos de acceso.
2. Exposición no autorizada de una base de datos.
3. Algoritmo lento de hash de contraseñas.
4. Tabla precalculada de hashes de contraseñas.
5. Prueba de credenciales filtradas (___ de credenciales).
6. Adición de una sal aleatoria al hash de una contraseña.
7. Herramienta para almacenar credenciales.
8. Comprobación de inicio de sesión con varios factores (MFA).

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos y términos clave de ciberseguridad. Escribe tus respuestas en los campos proporcionados.

1. LNREOLE
2. ABEHCR
3. GSTROE
4. OISRIARC
5. YRTBPC
6. DASLOA
7. CIMUARTOLFT
8. SHHGPNII

Actividad extra: Piensa rápido

3 RESPUESTAS POR CATEGORÍA. GANA QUIEN COMPLETE PRIMERO LA LISTA.

1	Hábitos seguros que puedes empezar hoy			
2	Normas para una contraseña segura			
3	Gestores de contraseñas que conoces			
4	Herramientas de seguridad que conoces			
5	Señales de alerta en un correo electrónico			
6	Palabras divertidas para una frase de contraseña larga			
7	Formas de iniciar sesión sin contraseña			
8	Información que nunca deberías compartir			
9	Razones para actualizar el software			
10	Cosas que hacer cuando se filtra una contraseña			
11	Cuentas que necesitan MFA			
12	Lugares donde nunca deberían guardarse las contraseñas			
13	Señales de que un ordenador está infectado			
14	Malas contraseñas que usa la gente			
15	Cosas de las que haces copia de seguridad			

Punto de control 8: Casos prácticos de ciberseguridad

Aplica los conceptos que has aprendido para resolver los escenarios reales que aparecen a continuación.

CASO PRÁCTICO 1: SOLUCIÓN A UNA FUGA DE CREDENCIALES EMPRESARIALES

👷

Escenario: Un servicio de monitorización de la dark web avisa a una organización de que se ha publicado en internet un volcado de base de datos que contiene contraseñas de administradores de sistemas de la empresa.

Pregunta de debate: Analiza los riesgos de la filtración de credenciales y propón una estrategia de restablecimiento administrativo.

CASO PRÁCTICO 2: IMPLANTAR ESTÁNDARES DE HASH DE CONTRASEÑAS

👷

Escenario: La base de datos de una empresa almacena actualmente las contraseñas de los usuarios con hashes MD5 obsoletos y sin sal criptográfica, lo que las hace vulnerables a una extracción rápida.

Pregunta de debate: Diseña una estrategia de migración para actualizar el algoritmo de hash de la base de datos.

Punto de control 9: Descifrar el código

Un profesional de la ciberseguridad protege los activos de la red frente a los actores de amenazas en línea. Usa la clave de letras y números de abajo para descifrar el mensaje escribiendo las letras correspondientes en los espacios en blanco.

CLAVE DE CIFRADO DE LETRAS A 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 Ñ=15 O=16 P=17 Q=18
R=19 S=20 T=21 U=22 V=23 W=24 X=25 Y=26 Z=27

17	19	16	21	5	7	5		21	22	20		3	12	1	23	5	20
6	9	12	21	19	1	4	1	20		3	16	14					
13	22	12	21	9	6	1	3	21	16	19							

Mensaje descifrado:

CONSEJO: CADA NÚMERO REPRESENTA LA POSICIÓN DE ESA LETRA EN EL ALFABETO (P. EJ., 1 = A, 2 = B, 27 = Z).

Punto de control 10: Preguntas frecuentes básicas sobre ciberseguridad (Parte A)

Repasa preguntas y respuestas habituales sobre la mitigación de amenazas en línea.

Q1: ¿Qué es una filtración de contraseñas?

Una filtración de contraseñas se produce cuando las credenciales de inicio de sesión de los usuarios quedan expuestas por brechas de datos o errores de configuración de los servidores.

Q2: ¿Cómo encuentran los hackers las contraseñas filtradas?

Los hackers rastrean foros de la dark web, volcados públicos de bases de datos y sitios de pegado (paste sites) donde se publican datos de filtraciones [8].

Q3: ¿Es peligroso reutilizar contraseñas?

Sí, porque si un sitio se ve comprometido, los hackers pueden probar las mismas credenciales en miles de otras plataformas [3].

Q4: ¿Qué es una sal criptográfica?

Una sal (salt) son datos aleatorios que se añaden a una contraseña antes de aplicarle el hash, lo que inutiliza los ataques con tablas precalculadas [2].

Q5: ¿Por qué MD5 está obsoleto?

MD5 es un hash de uso general rápido y obsoleto, por lo que los atacantes pueden probar contraseñas a gran velocidad, sobre todo cuando los hashes no tienen sal [2].

Punto de control 10: Preguntas frecuentes básicas sobre ciberseguridad (Parte B)

Repasa preguntas y respuestas habituales sobre la mitigación de amenazas en línea.

Q6: ¿Cómo protege un gestor de contraseñas a los usuarios?

Genera automáticamente credenciales complejas y únicas para cada sitio, lo que reduce los errores de memoria humana y la reutilización.

Q7: ¿Qué es un ataque de fuerza bruta?

Un ataque que prueba sistemáticamente todas las combinaciones de caracteres posibles hasta dar con la contraseña correcta [4].

Q8: ¿Cómo ayuda el bloqueo de cuentas?

El bloqueo o la limitación de intentos ralentiza los intentos repetidos de adivinar contraseñas en línea y, junto con la supervisión y la MFA, reduce el riesgo de ataques de fuerza bruta [4].

Q9: ¿Son seguras las contraseñas maestras?

Son seguras si son frases de contraseña de alta entropía que nunca se reutilizan en otros sistemas web.

Q10: ¿Deben cambiarse las contraseñas con regularidad?

El NIST recomienda no forzar cambios periódicos; cámbialas cuando haya indicios de que se han visto comprometidas y prioriza la longitud, las listas de bloqueo y la MFA [1].

Punto de control 10: Preguntas frecuentes avanzadas sobre seguridad (Parte C)

Explora aspectos técnicos avanzados de los marcos de seguridad, el análisis de malware y el cumplimiento normativo de los datos.

Q1: ¿Cómo se compara Argon2 con bcrypt?

OWASP sitúa Argon2id como su primera opción; su configuración de uso intensivo de memoria resiste el descifrado con GPU y ASIC mejor que bcrypt [2].

Q2: ¿Qué es el estiramiento de claves?

Una técnica que repite un algoritmo de hash miles de veces para ralentizar la verificación de contraseñas y encarecer su descifrado [2].

Q3: ¿Cómo funcionan las tablas arcoíris?

Son tablas de búsqueda precalculadas que relacionan contraseñas en texto plano con sus hashes y que se usan para revertir rápidamente hashes sin sal [2].

Q4: ¿Qué es el reciclaje de credenciales?

Reutilizar pares de usuario y contraseña robados en una filtración para intentar acceder a otros servicios, sobre todo cuando las personas han reutilizado contraseñas [3].

Q5: ¿Se pueden hackear los gestores de contraseñas?

Sí. Muchos usan cifrado de conocimiento cero, de modo que una brecha en el servidor solo expone bóvedas cifradas, pero las contraseñas maestras débiles aún pueden descifrarse sin conexión.

Punto de control 10: Preguntas frecuentes avanzadas sobre seguridad (Parte D)

Explora aspectos técnicos avanzados de los marcos de seguridad, el análisis de malware y el cumplimiento normativo de los datos.

Q6: ¿Qué es un ataque de diccionario?

Una variante de la fuerza bruta que prueba palabras y frases comunes y contraseñas filtradas en el pasado, en lugar de letras al azar.

Q7: ¿Por qué se prefieren las frases de contraseña?

Las frases de contraseña usan varias palabras aleatorias, lo que genera una entropía alta, fácil de recordar para las personas pero costosa de descifrar computacionalmente [1].

Q8: ¿Cómo afecta el inicio de sesión único (SSO) a las filtraciones de contraseñas?

El SSO reduce la proliferación de contraseñas, pero el proveedor de identidad se convierte en un objetivo muy valioso que necesita una MFA sólida, preferiblemente resistente al phishing [6].

Q9: ¿Qué es el secuestro de sesión?

Un atacante obtiene o usa indebidamente un token de sesión válido para suplantar a un usuario que ha iniciado sesión sin necesidad de volver a introducir la contraseña [5].

Q10: ¿Cómo se detecta la pulverización de contraseñas?

Buscando las mismas pocas contraseñas probadas en muchas cuentas, a menudo lentamente para no superar los umbrales de bloqueo [7].

Parte 11: 10 datos reales sobre ciberseguridad y su aplicación

Repasa datos reales sobre filtraciones de seguridad, mecanismos de defensa y normas de cumplimiento.

1. PERSPECTIVA SOBRE SEGURIDAD

La norma NIST SP 800-63B exige comprobar las contraseñas nuevas con listas de bloqueo de contraseñas comunes y comprometidas [1].

2. PERSPECTIVA SOBRE SEGURIDAD

El volcado 'Collection #1' de 2019 reunió datos de muchas filtraciones anteriores en un enorme archivo de pares de correo y contraseña [8].

3. PERSPECTIVA SOBRE SEGURIDAD

El NIST exige ahora que las contraseñas usadas como único factor de autenticación tengan al menos 15 caracteres [1].

4. PERSPECTIVA SOBRE SEGURIDAD

El hardware ASIC puede calcular miles de millones de hashes SHA-256 por segundo, lo que hace que el hash SHA simple no sea seguro para las contraseñas de los usuarios [2].

5. PERSPECTIVA SOBRE SEGURIDAD

Las sales únicas hacen que dos usuarios con exactamente la misma contraseña obtengan hashes distintos en la base de datos [2].

6. PERSPECTIVA SOBRE SEGURIDAD

Muchos gestores de contraseñas cifran localmente los datos de la bóveda con criptografía sólida derivada de la contraseña maestra del usuario.

7. PERSPECTIVA SOBRE SEGURIDAD

El relleno de credenciales funciona porque mucha gente reutiliza la misma contraseña en sus cuentas de comercio electrónico, banca y correo electrónico [3].

8. PERSPECTIVA SOBRE SEGURIDAD

La norma NIST SP 800-63B establece que los verificadores no deben exigir cambios periódicos de contraseña, solo cambios cuando haya indicios de que se ha visto comprometida [1].

9. PERSPECTIVA SOBRE SEGURIDAD

Añadir una sola letra mayúscula y un símbolo a una contraseña corta no detiene los ataques de diccionario automatizados modernos con GPU [1].

10. PERSPECTIVA SOBRE SEGURIDAD

La MFA puede bloquear muchos intentos de relleno de credenciales incluso después de que se filtre una contraseña; la MFA resistente al phishing es más sólida que los códigos SMS [3].

Referencias técnicas y fuentes

La guía de estudio y los pasatiempos interactivos se han elaborado a partir de los estándares internacionales del NIST, de OWASP y de cumplimiento en materia de privacidad de datos.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1 — **Respuesta correcta: A**

NOTA PARA DOCENTES

El relleno de credenciales usa la automatización para probar pares de usuario y contraseña filtrados en otros sitios [3].

2 Pregunta 2 — **Respuesta correcta: A**

NOTA PARA DOCENTES

OWASP recomienda Argon2id en primer lugar; bcrypt es sobre todo para sistemas heredados en los que Argon2id o scrypt no están disponibles [2].

3 Pregunta 3 — **Respuesta correcta: A**

NOTA PARA DOCENTES

La MFA exige un factor adicional, por lo que una contraseña robada por sí sola no puede desbloquear la cuenta [3].

4 Pregunta 4 — **Respuesta correcta: A**

NOTA PARA DOCENTES

Los volcados de filtraciones son colecciones de credenciales filtradas, como la recopilación Collection #1 de 2019 [8].

5 Pregunta 5 — **Respuesta correcta: A**

NOTA PARA DOCENTES

Un gestor de contraseñas genera y guarda una contraseña única y segura para cada cuenta, lo que evita su reutilización [3].

Clave de respuestas: Punto de control 2 – Verdadero o falso

6 Pregunta 6

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Verdadero: las contraseñas reutilizadas permiten a los atacantes reutilizar en otros sitios las credenciales filtradas de uno [3].

7 Pregunta 7

Respuesta correcta: Falso

NOTA PARA DOCENTES

Falso: SHA-1 es un hash rápido; OWASP recomienda en su lugar Argon2id, scrypt, bcrypt o PBKDF2 [2].

8 Pregunta 8

Respuesta correcta: Falso

NOTA PARA DOCENTES

Falso: las reglas de complejidad por sí solas no pueden detener el relleno con contraseñas filtradas reutilizadas; se necesita MFA [3].

9 Pregunta 9

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Verdadero: los servicios de monitorización buscan credenciales expuestas en volcados de filtraciones y fuentes de la dark web [8].

10 Pregunta 10

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Verdadero: una sal única por contraseña hace ineficaces las tablas arcoíris precalculadas [2].

Claves de vocabulario y rúbrica de calificación

Rúbrica de calificación para docentes: concede 1 punto por cada relación correcta (8 puntos en total) y por cada término de contexto (6 puntos en total).

PUNTO DE CONTROL 4: SOLUCIÓN DE LA RELACIÓN DE CONCEPTOS

F 1. RELLENO DE CREDENCIALES	H 2. BCRYPT	D 3. BRECHA	G 4. SALADO
C 5. GESTOR	B 6. MFA	A 7. ARCOÍRIS	E 8. PHISHING

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 RELLENO	2 BCRYPT	3 BRECHA	4 SALADO
5 GESTOR	6 MULTIFACTOR		

PUNTO DE CONTROL 6, ALTERNATIVA: SOLUCIÓN DE LA RELACIÓN DE PALABRAS

1 H – PHISHING	2 C – BRECHA	3 B – BCRYPT	4 G – ARCOIRIS
5 A – RELLENO	6 D – SALADO	7 E – GESTOR	8 F – MULTIFACTOR

NOTAS DE DEBATE PARA DOCENTES

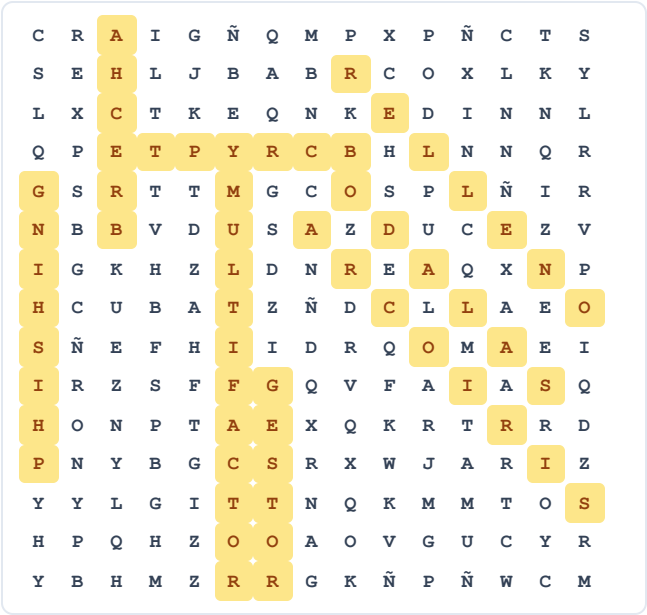
Términos clave:
Comprueba que los estudiantes saben explicar RELLENO DE CREDENCIALES, BCRYPT y BRECHA con sus propias palabras y dar un ejemplo de cada uno.

Casos prácticos:
Pide a los estudiantes que justifiquen sus recomendaciones con datos de la hoja de trabajo y no con suposiciones.

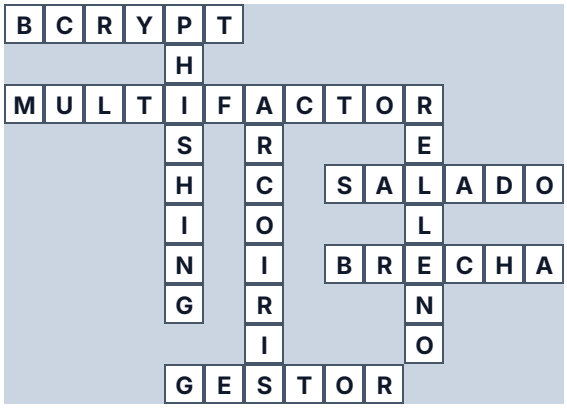
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS



SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

1 horizontal: BCRYPT Algoritmo lento de hash de contraseñas. (6 letras)

3 horizontal: MULTIFACTOR Comprobación de inicio de sesión con varios factores (MFA). (11 letras)

6 horizontal: SALADO Adición de una sal aleatoria al hash de una contraseña. (6 letras)

7 horizontal: BRECHA Exposición no autorizada de una base de datos. (6 letras)

8 horizontal: GESTOR Herramienta para almacenar credenciales. (6 letras)

VERTICALES

2 vertical: PHISHING Ingeniería social para robar datos de acceso. (8 letras)

4 vertical: ARCOIRIS Tabla precalculada de hashes de contraseñas. (8 letras)

5 vertical: RELLENO Prueba de credenciales filtradas (___ de credenciales). (7 letras)

Clave de soluciones de palabras desordenadas y del cifrado

Clave de calificación de la actividad de ordenar letras del vocabulario y del Reto del código secreto.

CLAVE DE LAS PALABRAS DESORDENADAS

1.	L N R E O L E	RELLENO	5.	Y R T B P C	BCRYPT
2.	A B E H C R	BRECHA	6.	D A S L O A	SALADO
3.	G S T R O E	GESTOR	7.	C I M U A R T O L F T	MULTIFACTOR
4.	O I S R I A R C	ARCOIRIS	8.	S H H G P N I I	PHISHING

CLAVE DEL RETO DEL CÓDIGO SECRETO

"PROTEGE TUS CLAVES FILTRADAS CON MULTIFACTOR"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Solución a una fuga de credenciales empresariales

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un servicio de vigilancia de la web oscura avisa a una organización de que se ha publicado en internet un volcado de base de datos con contraseñas de los administradores de sistemas de la empresa.
- Estrategia y solución recomendadas: revocar todas las sesiones de administrador activas y restablecer las credenciales con un generador de alta entropía. Imponer MFA resistente al phishing en los portales de administración [6], rotar las claves de API afectadas, revisar los registros de inicio de sesión, localizar la exposición inicial y comprobar las demás cuentas con privilegios.

B Caso práctico 2: Implantar estándares de hash de contraseñas

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: La base de datos de una empresa almacena actualmente las contraseñas de los usuarios con hashes MD5 obsoletos sin sal criptográfica, lo que las hace vulnerables a una extracción rápida.
- Estrategia y solución recomendadas: adoptar Argon2id (o bcrypt en sistemas heredados) con una sal única por usuario [2]. Envolver ahora los hashes MD5 existentes en el nuevo algoritmo, volver a generar el hash directamente en el siguiente inicio de sesión de cada usuario y forzar un restablecimiento en las cuentas inactivas durante mucho tiempo.