



INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Taller “Gestiona tus contraseñas de forma segura y protege tus cuentas de usuario”

---



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



TU AYUDA EN  
CIBERSEGURIDAD  
incibe\_



Oficina  
de Seguridad  
del Internauta



- ❖ **1. Las contraseñas, ¿cómo nos protegen?**
- ❖ **2. Una contraseña robusta es sinónimo de seguridad**
- ❖ **3. Medidas de protección adicionales**
- ❖ **4. Principales amenazas sobre nuestras contraseñas**
- ❖ **5. Comprobación de cuentas comprometidas**

# INTRODUCCIÓN

Nuestra principal protección contra los ciberdelincuentes son nuestras **contraseñas**, aunque no siempre les prestamos la atención que se merecen.

¿Sabemos cómo **gestionar de forma segura todas nuestras claves**?



# 1. LAS CONTRASEÑAS, ¿CÓMO NOS PROTEGEN?

En Internet, la mayoría de servicios online donde nos registramos utilizan como mecanismo para verificar nuestra identidad un **nombre de usuario (o correo electrónico) y una contraseña de acceso.**



## 2. PRINCIPALES AMENAZAS SOBRE NUESTRAS CONTRASEÑAS

Nuestras contraseñas son una de las **primeras defensas** para proteger nuestras cuentas personales y dispositivos.



Ataques a nuestras contraseñas



Ataques basados en ingeniería social

## 2. PRINCIPALES AMENAZAS SOBRE NUESTRAS CONTRASEÑAS. ATAQUES A NUESTRAS CONTRASEÑAS

Los ciberdelincuentes hacen uso de un **gran número de herramientas y estrategias** con las que conseguir adivinar nuestras contraseñas:

Fuerza bruta

Ataques *Keylogger*

Ataques de diccionario

Ataques de ingeniería social

Ataques *Spidering*



## 2. PRINCIPALES AMENAZAS SOBRE NUESTRAS CONTRASEÑAS. TÍPICOS ERRORES QUE COMETEMOS

El riesgo debido al **uso de malas prácticas** es muy alto y puede poner en peligro toda nuestra seguridad y privacidad. Veamos algunos ejemplos:



### 3. UNA CONTRASEÑA ROBUSTA ES SINÓNIMO DE SEGURIDAD

¿Sabes cuánto tardaría un ciberdelincuente en adivinar una contraseña como '1234567890'? La respuesta es: segundos.

1234567890



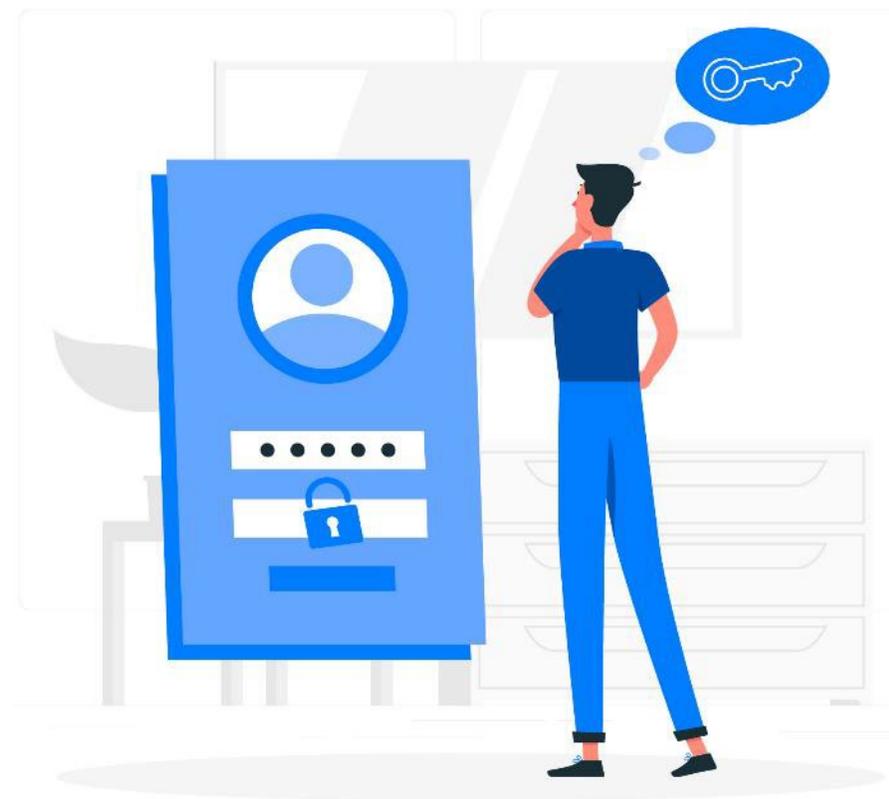
0SiSegur1dad!



### 3. UNA CONTRASEÑA ROBUSTA ES SINÓNIMO DE SEGURIDAD. CÓMO CREAR CONTRASEÑAS ROBUSTAS

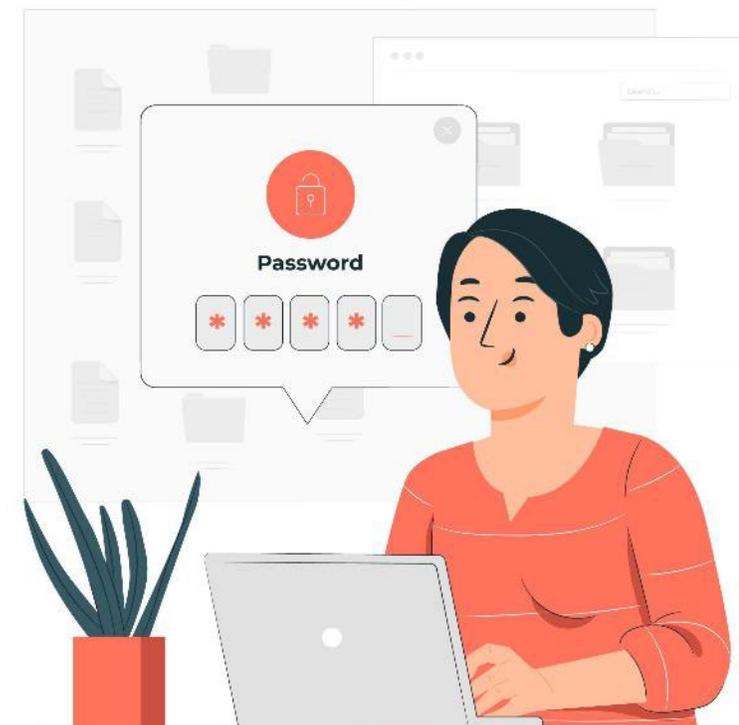
La **creación de contraseñas robustas** es un proceso que puede parecer tedioso y complejo, pero nada más lejos de la realidad:

- ❖ Piensa una frase o varias palabras.
- ❖ Incluye mayúsculas y minúsculas.
- ❖ Añade algunos números.
- ❖ Añade caracteres especiales.
- ❖ Personaliza tus contraseñas.



### 3. UNA CONTRASEÑA ROBUSTA ES SINÓNIMO DE SEGURIDAD. REGLAS NEMOTÉCNICAS

Podemos recurrir a nuestras propias reglas para ayudarnos a recordar estas contraseñas:



- ❖ Patrones de teclado numérico.
- ❖ Elementos distintivos por cuenta.
- ❖ Frase como base de la contraseña.
- ❖ Mezclar dos palabras.

# ACTIVIDAD 1



¿Utilizas contraseñas robustas? Ya hemos visto cómo se construye una clave robusta y qué características tiene.

Ahora, vamos a intentar construir una contraseña robusta para los servicios o herramientas que más utilicemos. Puedes servirte de este [recurso](#) para ello.

## 4. MEDIDAS DE PROTECCIÓN ADICIONALES

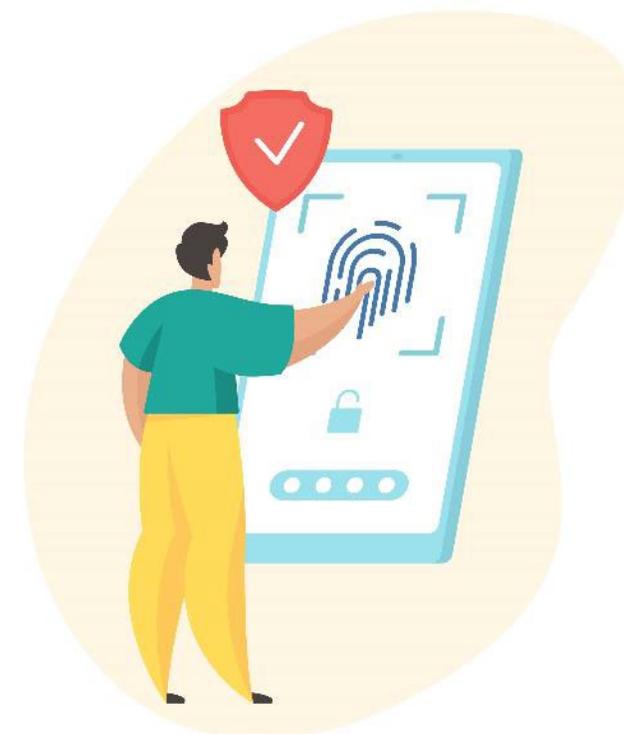
Una contraseña robusta nos asegurará que la mayoría de ciberdelincuentes desistan a la hora de intentar atacar nuestra seguridad.



## 4. MEDIDAS DE PROTECCIÓN ADICIONALES. VERIFICACIÓN EN DOS PASOS

La verificación en dos pasos es una medida de protección adicional a la contraseña con la que podemos dificultar que alguien sin autorización acceda a nuestra cuenta:

- ❖ Verificación por SMS.
- ❖ Verificación por correo electrónico.
- ❖ Verificación con pregunta de seguridad.
- ❖ Verificación a través de una aplicación.
- ❖ Verificación por códigos temporales proporcionados por la propia app o servicio.
- ❖ Verificación mediante llave de seguridad (USB, NFC, Bluetooth...).
- ❖ Verificación con biometría: Verificación con códigos de recuperación.



## 4. MEDIDAS DE PROTECCIÓN ADICIONALES. VERIFICACIÓN EN DOS PASOS

Muchos son los servicios que ya cuentan con un sistema de verificación en dos pasos propio que debemos activar si queremos disponer de esta capa de seguridad para proteger nuestras cuentas. Sin embargo, también podemos utilizar **aplicaciones externas**: <https://youtu.be/oFzKEogQEsI>



## 4. MEDIDAS DE PROTECCIÓN ADICIONALES. GESTORES DE CONTRASEÑAS: CÓMO UTILIZARLOS

Los gestores de contraseñas son herramientas que nos permiten guardar nuestras contraseñas de forma cifrada:



## 4. MEDIDAS DE PROTECCIÓN ADICIONALES. GESTORES DE CONTRASEÑAS: CÓMO UTILIZARLOS

En el mercado existe una gran variedad de aplicaciones con esta función:

- 1 Descargar la aplicación y crear una cuenta
- 2 Agregar nuevos elementos (cuentas)
- 3 Disfrutar de funciones adicionales



## 5. COMPROBACIÓN DE CUENTAS COMPROMETIDAS

Cuando los ciberdelincuentes atacan a empresas de servicio, la seguridad de nuestras cuentas puede verse afectada y es recomendable **realizar una comprobación de nuestras cuentas**.

The screenshot shows a web browser displaying the 'have i been pwned?' website. The main heading is ';-have i been pwned?' with the subtitle 'Check if your email or phone is in a data breach'. Below this is a search input field with the placeholder text 'email or phone (international format)' and a 'pwned?' button. A red box highlights the search input field and the 'pwned?' button. Below the search field, a red box highlights a message that reads: 'Oh no — pwned!' followed by 'Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)'. The browser's address bar and navigation icons are visible at the top.

## ACTIVIDAD 2



Por muy seguros que estemos de la seguridad de nuestras cuentas, es recomendable que de vez en cuando realicemos alguna comprobación.

Vamos a comprobar, por medio de nuestro correo electrónico, si nuestras cuentas son seguras ingresándolo en [\*Have i Been Pwned\*](#).

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



1. Cuando un programa se dedica a recopilar lo que escribimos, hablamos de un:

- A. *Keylogger*
- B. *Ransomware*
- C. Ataque de diccionario

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**2. El principal riesgo de utilizar una contraseña sencilla como 'contraseña' es:**

- A. Ataques de araña
- B. Ataques por diccionario
- C. *Keyloggers*

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**3. ¿Cuál de las siguientes prácticas es insegura y peligrosa para la seguridad de nuestras cuentas?:**

- A. Apuntarla en un papel
- B. Reciclar contraseñas
- C. Todas las opciones son inseguras

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**4. El primer paso para construir una contraseña robusta debe ser:**

- A. Unir dos palabras aleatorias
- B. Utilizar información personal
- C. Usar expresiones hechas

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



5. De entre las siguientes opciones, ¿cuáles podríamos considerar una contraseña robusta?:

- A. 12345678
- B. M4resDelMund0!
- C. MiguelHernandez1972

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**6. La verificación en dos pasos es un método de protección que mejora la seguridad de nuestras cuentas al:**

- A. Obligar a utilizar una clave robusta.
- B. Utilizar dos contraseñas en lugar de 1.
- C. Enviar un código de confirmación al iniciar sesión.

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**7. Un gestor de contraseñas es una herramienta muy útil, ya que nos ayuda a:**

- A. Proteger todas nuestras contraseñas.
- B. Construir contraseñas robustas.
- C. Ambas opciones son correctas.

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**8. En lo referente a nuestras contraseñas, ¿cuál sería la práctica más recomendada?:**

- A. Utilizar la verificación en dos pasos, un gestor de contraseñas y contraseñas robustas.
- B. Utilizar un gestor de contraseñas con contraseñas robustas, la verificación es opcional.
- C. Utilizar solo contraseñas robustas.

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**9. La biometría es una tecnología que nos permite identificarnos por medio de:**

- A. Un código enviado al teléfono móvil.
- B. Nuestra huella o rostro.
- C. Una palabra o pregunta clave.

# CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



**10. En caso de una fuga de información de un servicio online que utilizamos, lo primero que debemos hacer es:**

- A. Comprobar la seguridad de nuestras cuentas.
- B. Cambiar la contraseña de la cuenta que tengamos en el servicio afectado.
- C. Nada, solo afecta al servicio, no a mi cuenta.



INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Gracias por vuestra atención

---



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO

MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



TU AYUDA EN  
CIBERSEGURIDAD  
incibe\_



Oficina  
de Seguridad  
del Internauta

# LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- ❖ Reconocimiento. El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- ❖ Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- ❖ Compartir Igual. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: [https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es\\_ES](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES)



**Reconocimiento-NoComercial-CompartirIgual 4.0  
Internacional (CC BY-NC-SA 4.0)**