

Taller Formativo

**Gestiona tus contraseñas de forma segura y
protege tus cuentas de usuario**



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



ÍNDICE

1. Objeto del documento.....	4
2. Organización y estructura	5
3. Objetivo	6
4. Metodología y recursos	7
5. Contenidos.....	8
5.1. Diapositiva 1. Presentación del taller	8
5.2. Diapositiva 2. Índice	8
5.3. Diapositiva 3. Introducción	8
5.4. Diapositiva 4. Las contraseñas, ¿cómo nos protegen?.....	8
5.5. Diapositiva 5. Principales amenazas sobre nuestras contraseñas	9
5.6. Diapositiva 6. Principales amenazas sobre nuestras contraseñas. Ataques a nuestras contraseñas.....	9
5.7. Diapositiva 7. Principales amenazas sobre nuestras contraseñas. Típicos errores que cometemos	10
5.8. Diapositiva 8. Una contraseña robusta es sinónimo de seguridad.....	10
5.9. Diapositiva 9. Una contraseña robusta es sinónimo de seguridad. Cómo crear contraseñas robustas.....	10
5.10. Diapositiva 10. Una contraseña robusta es sinónimo de seguridad. Reglas nemotécnicas.....	11
5.11. Diapositiva 11. Actividad 1	12
5.12. Diapositiva 12. Medidas de protección adicionales.....	12
5.13. Diapositiva 13-14. Medidas de protección adicionales. Verificación en dos pasos.....	12
5.14. Diapositiva 15-16. Medidas de protección adicionales. Gestores de contraseñas: cómo utilizarlos	13
5.15. Diapositiva 17. Comprobación de cuentas comprometidas	15
5.16. Diapositiva 18. Actividad 2	15
5.17. Diapositiva 19. Cuestionario de evaluación 1	15
5.18. Diapositiva 20. Cuestionario de evaluación 2	16
5.19. Diapositiva 21. Cuestionario de evaluación 3	16
5.20. Diapositiva 22. Cuestionario de evaluación 4	16
5.21. Diapositiva 23. Cuestionario de evaluación 5	16
5.22. Diapositiva 24. Cuestionario de evaluación 6	16
5.23. Diapositiva 25. Cuestionario de evaluación 7	16
5.24. Diapositiva 26. Cuestionario de evaluación 8	17
5.25. Diapositiva 27. Cuestionario de evaluación 9	17
5.26. Diapositiva 28. Cuestionario de evaluación 10.....	17
5.27. Diapositiva 29. Final del taller	17
5.28. Diapositiva 30. Licencia de contenidos	17
6. Recursos de evaluación	19
6.1. Cuestionario de evaluación	20
ANEXO	22
Recursos para ampliar	22

1. OBJETO DEL DOCUMENTO

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **Taller formativo de ‘Gestiona tus contraseñas de forma segura y protege tus cuentas de usuario’**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 5 temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. Las contraseñas, ¿cómo nos protegen?
2. Una contraseña robusta es sinónimo de seguridad.
 - a. Cómo crear contraseñas robustas.
 - b. Reglas nemotécnicas.
3. Medidas de protección adicionales:
 - a. Verificación en dos pasos.
 - b. Gestores de contraseñas: cómo utilizarlos.
4. Principales amenazas sobre nuestras contraseñas
 - a. Ataques a nuestras contraseñas.
 - b. Típicos errores que cometemos.
5. Comprobación de cuentas comprometidas.

3. OBJETIVO

Este taller tiene como objetivo principal **proporcionar a los alumnos las herramientas y conocimientos necesarios para crear y gestionar sus contraseñas de forma segura y mejorar la seguridad de sus cuentas personales**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

4. METODOLOGÍA Y RECURSOS

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual:** las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa:** el alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
 - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en Power Point.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades.** Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.
- **Cuestionario de evaluación.** Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

5. CONTENIDOS

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

5.1. Diapositiva 1. Presentación del taller

Presentación del taller 'Aprende a contrastar la información'. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017, al igual que los nuevos canales chats de WhatsApp y Telegram para contactar con él.

5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Las contraseñas, ¿cómo nos protegen?
2. Una contraseña robusta es sinónimo de seguridad.
 - a. Cómo crear contraseñas robustas.
 - b. Reglas nemotécnicas.
3. Medidas de protección adicionales:
 - a. Verificación en dos pasos: tipos, ejemplos y configuración.
 - b. Gestores de contraseñas: cómo utilizarlos.
4. Principales amenazas sobre nuestras contraseñas
 - a. Ataques a nuestras contraseñas.
 - b. Típicos errores que cometemos.
5. Comprobación de cuentas comprometidas.

5.3. Diapositiva 3. Introducción

Nuestra información personal, especialmente aquella que está alojada en Internet, es un objetivo muy atractivo para los ciberdelincuentes. Nuestra principal protección contra ellos son nuestras **contraseñas**, aunque no siempre les prestamos la atención que se merecen y pueden ser la causa de brechas de seguridad que provoquen que esta información termine en malas manos.

A lo largo de este taller, aprenderemos a diferenciar una contraseña débil de una robusta y a **gestionar de forma fácil y segura todas nuestras claves para no tener que recurrir a malas prácticas que faciliten a los ciberdelincuentes acceder a nuestras cuentas**.

5.4. Diapositiva 4. 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**. También existen métodos de autenticación adicionales, como la biometría, que nos permite utilizar nuestro rostro o nuestra huella digital, aunque no serán el objetivo de este taller.

Esta información nos permite iniciar sesión, identificarnos y disfrutar de nuestras cuentas de correo, en redes sociales, cuentas con el banco y mucho más.

Además, son el **principal mecanismo de protección que tenemos contra los ataques de suplantación de identidad** y todo tipo de estafas y fraudes que estén relacionados con

el acceso a la información que se almacena en una cuenta de cualquier servicio, ya que evitan que terceros puedan acceder a toda esta información. Sin embargo, también pueden presentar vulnerabilidades, especialmente cuando no tenemos claro qué es una contraseña robusta o cómo podemos gestionarlas de forma segura.

5.5. Diapositiva 5. Principales amenazas sobre nuestras contraseñas

Nuestras contraseñas son una de las primeras defensas para proteger nuestras cuentas personales y dispositivos. Por esto, están en el punto de mira de los ciberdelincuentes que cuentan con un amplio abanico de técnicas contra nuestras contraseñas.

Podemos clasificar estas amenazas en:

- **Ataques a nuestras contraseñas:** herramientas informáticas y técnicas empleadas por los ciberdelincuentes para adivinar nuestras contraseñas o explotar alguna vulnerabilidad del servicio para obtener acceso a nuestra cuenta.
- **Ataques basados en ingeniería social:** son un conjunto de técnicas de engaño con el objetivo de suplantar la identidad de una entidad o servicio de confianza para conseguir que compartamos nuestro usuario y contraseña con el ciberdelincuente.

5.6. Diapositiva 6. 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. A continuación, vamos a ver los diferentes [tipos de ataques](#) que existen:

- **Fuerza bruta:** es el método más básico y, por lo tanto, el menos efectivo. Los atacantes realizan pruebas de ensayo y error, realizando combinaciones al azar, conjugando nombres, letras y números hasta dar con el patrón correcto.
- **Ataques de diccionario:** utilizan un programa malicioso que trata de adivinar la contraseña de una cuenta de forma automática realizando combinaciones de letras cada vez más complejas hasta dar con la correcta.
- **Ataques Keylogger:** son ataques donde se utiliza un tipo de [malware](#) conocido como Keylogger. Los ciberdelincuentes consiguen instalar este [malware](#) en el dispositivo de sus víctimas por medio de diferentes técnicas, como el *phishing*. Una vez instalado, este programa malicioso recopilará todas las pulsaciones que el usuario haga sobre su teclado, incluidos usuarios y contraseñas, y luego las compartirá con el atacante.
Algunas modalidades permiten realizar capturas de pantalla e incluso realizar grabaciones de vídeo y audio.
- **Ataques 'Spidering' o de araña:** estos ataques se basan en buscar toda la información posible sobre la víctima en Internet para luego realizar pruebas con combinaciones de palabras sobre su vida personal, como fechas de cumpleaños, nombre y apellidos o nombres de la mascota.
- **Ataques de ingeniería social:** estos ataques son los más comunes y existen una amplia variedad de ellos, como el *phishing*, *smishing*, *vishing*... En conjunto, se tratan de técnicas de engaño donde los ciberdelincuentes consiguen que sus víctimas les faciliten el usuario y la contraseña de sus cuentas, pensando que se

trata de una persona o entidad de confianza, como nuestro banco o personal del servicio técnico de nuestro equipo.

5.7. Diapositiva 7. Principales amenazas sobre nuestras contraseñas. Típicos errores que cometemos

Ya sea por comodidad o desconocimiento, muchos de nosotros, solemos emplear malas prácticas con respecto a nuestras contraseñas. Por ejemplo, utilizar la misma contraseña en diferentes cuentas, utilizando claves muy fáciles de adivinar o dejarlas escritas en sitios accesibles por otras personas. El riesgo de este tipo de prácticas es muy alto y puede poner en peligro toda nuestra seguridad y privacidad.

Para evitar seguir cometiéndolos, vamos a hacer un repaso de algunas de las prácticas más comunes y peligrosas:

- **Reciclar contraseñas:** un error muy frecuente es utilizar la misma clave para múltiples cuentas o aplicaciones.
- **Memorizar contraseñas en función del teclado:** muchos usuarios usan el teclado como guía para recordar contraseñas fácilmente (ej.: “123456” o ‘qwerty’).
- **Usar expresiones hechas:** entre otro de los errores más comunes es el uso como contraseñas de frases como ‘teamo’, ‘iloveyou’, ‘teodio’, etc.
- **Utilizar información personal:** algunos usuarios suelen emplear datos personales para crear sus claves, como su cumpleaños, fecha de aniversario, nombre y apellidos, nombre de la mascota o equipo favorito.
- **Apuntarlas en notas:** aunque se haya creado una clave robusta, nunca se debe dejar por escrito y mucho menos a la vista de cualquiera.
- **Hacer uso de patrones sencillos:** como que la primera letra esté en mayúscula seguida de 4 o 5 en minúscula o usar uno o dos números y finalizar con un carácter especial como un punto o signo de exclamación (Ej.: Perro26!).

5.8. Diapositiva 8. Una contraseña robusta es sinónimo de seguridad

¿Sabes cuánto tardaría un ciberdelincuente en adivinar una contraseña como ‘1234567890?’ La respuesta es en segundos. Hoy en día, los ciberdelinquentes cuentan con numerosas herramientas que permiten descifrar las contraseñas más sencillas en cuestión de segundos.

Para evitarlo, cada vez son más los servicios que nos solicitan la creación de contraseñas con unas características especiales que las hagan más robustas y difíciles de adivinar. Un ejemplo de este tipo de contraseñas robustas podría ser: 0SiSegur1dad!

5.9. Diapositiva 9. 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. A continuación, vamos a ver una serie de pasos que podemos seguir para crear todas ellas:

1. Pensemos en dos palabras que no tengan nada que ver entre ellas, aunque también puede ser una frase de un libro que hayamos leído recientemente. También,

podemos utilizar palabras que nos vengan a la mente al pensar en el servicio para el que estamos creando la contraseña. Por ejemplo: **mejora tu seguridad**.

2. Ahora, vamos a incluir algunas **mayúsculas y minúsculas** en esta frase para realizar la siguiente combinación: **MejoraTuSeguridad**.
3. Después, vamos a incluir algunos **números**. Un truco es sustituir algunas letras por un número concreto. Por ejemplo: **M3joraTuS3guridad**.
4. El siguiente paso será añadir **caracteres especiales** que añadan un poco más de complejidad. Podemos sustituir alguna letra o añadirlos en un extremo de nuestra clave: **M3joraTuS3guridad!**.
5. Finalmente, podemos personalizarlas para cada uno de nuestros servicios, de modo que no tengamos que repetir la misma contraseña en todos ellos.
 - Por ejemplo, si vamos a crear la contraseña para nuestro correo electrónico, podemos utilizar **CEM3joraTuS3guridad!**.
 - Mientras que, para nuestra cuenta de Facebook: **FBM3joraTuS3guridad!**.

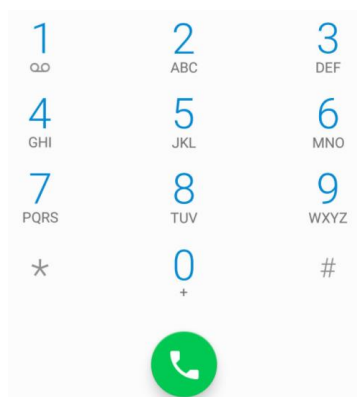
5.10. Diapositiva 10. Una contraseña robusta es sinónimo de seguridad. Reglas nemotécnicas

A todos nos preocupa que se nos olvide una contraseña, especialmente cuando utilizamos contraseñas robustas más complejas que sus versiones menos seguras. Por suerte, podemos recurrir a nuestras propias reglas para ayudarnos a recordar estas contraseñas.

Las **reglas nemotécnicas** nos ayudan a asociar información que ya formen parte de nuestra memoria, de modo que podamos recordar una contraseña larga asociando sus partes con algún concepto o evento de nuestra memoria.

Veamos algunos ejemplos:

1. **Patrones de teclado numérico.** Todos los teléfonos móviles cuentan con un sistema de letras asociado a números, especialmente los teléfonos más antiguos. Con ellos, podemos convertir una palabra en un conjunto de números. Por ejemplo: 'OSI', sería '**674**'. Para hacerla más compleja, podríamos utilizar palabras más largas y alternar entre letras y números, como 'Contraseña' que sería '**C6n8R2s3Ñ2**'.



2. **Elementos distintivos por cuenta.** Otra alternativa es memorizar una contraseña robusta y variarla entre cuentas añadiendo alguna palabra o letras relacionadas con la cuenta. Por ejemplo, nuestra contraseña de correo electrónico puede ser '**Cc0ntr4señA!E**' y la de nuestra red social '**Rc0ntr4señAL**'.

3. **Frase como base de la contraseña.** Podemos utilizar una frase larga que nos recuerde la contraseña que hemos utilizado, como 'Esta es mi contraseña de correo electrónico en 2021' para construir '**EsMcDcEe21!**'.
4. **Mezclar dos palabras.** Si mezclamos 'calor' con 'manga' obtendremos 'cmaalnogra' que podremos completar con alguna mayúscula, números y un carácter especial: '**Cmaaln0gra!**'

5.11. Diapositiva 11. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

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 servirtte de este [recurso](#) para ello.

5.12. Diapositiva 12. Medidas de protección adicionales

Una contraseña robusta nos asegurará que la mayoría de ciberdelincuentes desistan a la hora de intentar atacar nuestra seguridad. Sin embargo, no podemos dar por hecho que nuestras cuentas sean totalmente impenetrables. Ataques basados en ingeniería social, es decir, técnicas de engaño para manipularnos y conseguir que, sin que seamos conscientes de ello, seamos nosotros quienes facilitemos nuestra contraseña.

Un correo con un enlace malicioso o la descarga por error de un virus puede afectar a nuestra seguridad independientemente de lo robusta que sea nuestra contraseña.

Por ello, debemos tener en cuenta el uso de otras medidas de protección adicionales, especialmente en aquellas cuentas personales que contengan información sensible, como nuestro banco o el correo electrónico, por ejemplo.

5.13. Diapositiva 13-14. 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. Al activarla, además de un usuario y una contraseña, será necesario facilitar otro código para autenticarnos.

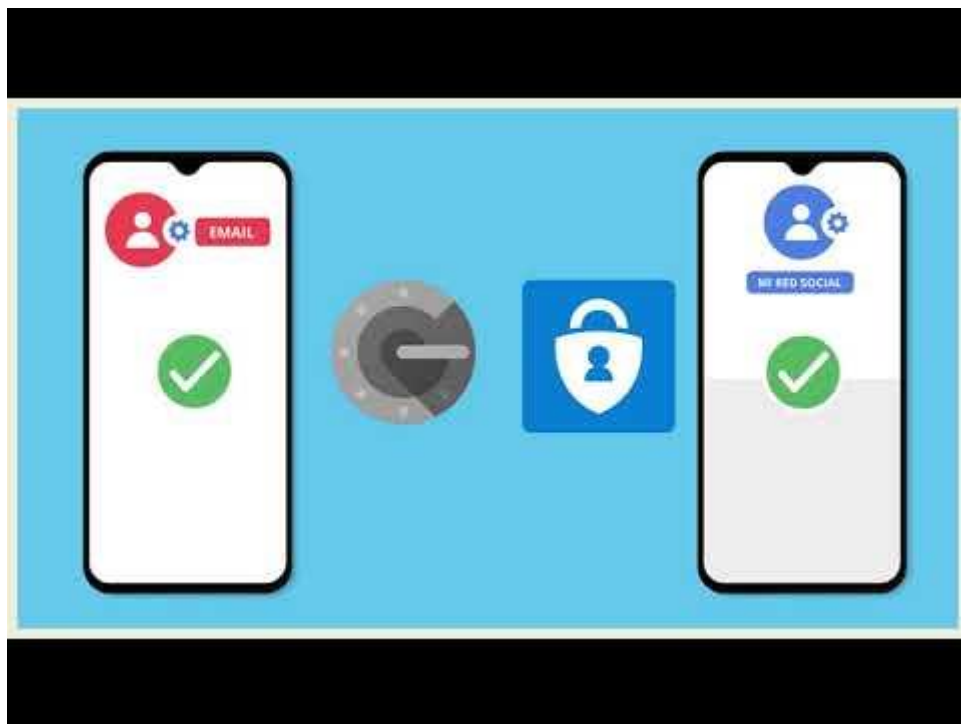
Este código suele enviarse a otro dispositivo, como puede ser nuestro móvil, aunque existen diversos métodos:

- Verificación por SMS.

- Verificación por correo electrónico.
- Verificación con pregunta de seguridad: algunos servicios utilizan preguntas de seguridad como medida de seguridad extra.
- Verificación a través de una aplicación: aplicaciones que se vinculan a nuestras cuentas y que sirven de intermediario para verificar nuestra identidad al compartírnos el código de validación.
- Verificación por códigos temporales proporcionados por la propia app o servicio: algunos servicios expiden códigos temporales a modo de verificación.
- Verificación mediante llave de seguridad (USB, NFC, Bluetooth...): un dispositivo externo que al conectarlo o vincularlo verifica nuestra identidad.
- Verificación con biometría: nuestro rostro o huella dactilar puede servir para identificarnos y como medida de seguridad extra.
- Verificación con códigos de recuperación: se trata de códigos que debemos guardar o imprimir y que podemos utilizar en caso de emergencia a modo de llave maestra.

De este modo, para acceder a nuestra cuenta se necesita, además de nuestro usuario y contraseña, tener acceso a nuestro dispositivo personal, lo que minimiza las posibilidades de que un atacante nos robe la cuenta.

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 de grandes empresas como Google y su 'Google Authenticator' o Microsoft con 'Microsoft Authenticator'. Estas aplicaciones se pueden descargar en Google Play y App Store para nuestras cuentas de Gmail, Amazon, Facebook, Outlook, PayPal, Dropbox, Twitter...



5.14. Diapositiva 15-16. Medidas de protección adicionales. Gestores de contraseñas: cómo utilizarlos

Los gestores de contraseñas son herramientas que nos permiten guardar nuestras contraseñas de forma cifrada, de modo que un tercero no puede tener acceso a ellas a menos que conozca una contraseña maestra que sirve, precisamente, para cifrarlas. Además, suelen incluir otras funciones como la creación automática de contraseñas fuertes o alertas para actualizar nuestras claves cada cierto tiempo o que nos avisan si utilizamos contraseñas muy similares entre sí.

En el mercado existe una gran variedad de aplicaciones con esta función, tanto para dispositivos móviles, ordenadores Windows o macOS y navegadores. A continuación, vamos a ver los pasos a seguir para configurar nuestras contraseñas desde el gestor LastPass.

1. Lo primero será [descargar la aplicación](#) y crearnos una cuenta. Este paso es idéntico en todos los gestores, y nos requerirá el uso de una dirección de correo electrónico y una contraseña maestra.



The image shows the LastPass login interface. At the top, the LastPass logo is displayed. Below it, there are two links: 'INICIAR SESIÓN' and 'O CREE UNA CUENTA'. The 'INICIAR SESIÓN' link is highlighted. Below the links, there are two input fields: 'Dirección de e-mail' and 'Contraseña maestra'. Both fields have placeholder text: 'introduzca una dirección de e-mail válida' and 'introduzca una contraseña' respectively. Below the input fields, there is a red button labeled 'INICIAR SESIÓN'. Below the button, there is a link '¿HA OLVIDADO LA CONTRASEÑA?' and a link 'Opciones avanzadas' with a dropdown arrow.

Vamos a crear su contraseña maestra

Elija una que no suela utilizar en ningún otro sitio. No podrá restablecerla, así que utilice algo que pueda recordar.

Contraseña maestra



Confirmar contraseña maestra



Indicio de contraseña (opcional)

ESTABLECER MI CONTRASEÑA

2. Una vez entremos en la aplicación, deberemos **agregar nuevos elementos** para nuestras cuentas (correo electrónico, redes sociales, cuenta bancaria). Como mínimo nos pedirán la URL o servicio para el que será utilizado, el nombre de usuario, la contraseña y algún comentario o nota que queramos añadir.
3. Ahora, siempre que necesitemos acceder a una de nuestras cuentas, podremos consultar esta herramienta. Además, muchos de los gestores incluyen **funciones adicionales** para ayudarnos a crear contraseñas robustas, recordatorios para cambiar las contraseñas y medidas para recuperar nuestra clave maestra en caso de que la olvidemos.

5.15. Diapositiva 17. Comprobación de cuentas comprometidas

En ocasiones, los ciberdelincuentes realizan ataques a empresas de servicio, como plataformas de compras online, redes sociales u otro tipo de servicios online donde tenemos cuenta. Cuando esto ocurre, la seguridad de nuestras cuentas puede verse afectada y es recomendable realizar una comprobación para cambiar nuestras contraseñas en aquellas cuentas afectadas.

Para comprobarlo, podemos hacer uso de la web [Have i Been Pwned](#).

- Una vez dentro, nos pedirá que ingresemos nuestro email y la herramienta vinculará ese correo con los datos recogidos de las filtraciones de datos que se han publicado en Internet.
- Luego, nos informará si existe una coincidencia y, además, sabremos si nuestro correo electrónico, afectado por una de estas filtraciones, se ha utilizado en algún servicio que no conocíamos o que habíamos olvidado debido al poco uso.

5.16. Diapositiva 18. Actividad 2

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

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](#).

5.17. Diapositiva 19. Cuestionario de evaluación 1

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

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

5.18. Diapositiva 20. Cuestionario de evaluación 2

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

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

5.19. Diapositiva 21. Cuestionario de evaluación 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.

5.20. Diapositiva 22. Cuestionario de evaluación 4

El primer paso para construir una contraseña robusta debe ser:

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

5.21. Diapositiva 23. Cuestionario de evaluación 5

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

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

5.22. Diapositiva 24. Cuestionario de evaluación 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.

5.23. Diapositiva 25. Cuestionario de evaluación 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.

5.24. Diapositiva 26. Cuestionario de evaluación 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.

5.25. Diapositiva 27. Cuestionario de evaluación 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.

5.26. Diapositiva 28. Cuestionario de evaluación 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.

5.27. Diapositiva 29. Final del taller

¡Gracias por vuestra atención!

5.28. Diapositiva 30. Licencia de contenidos

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

[Imagen licencia de contenidos BY-NC-SA]

6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller.** La participación del alumnado mediante dudas u otro tipo de aportaciones resulta de un gran valor evaluativo (10% de la evaluación final).
2. **Actividades.** Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u *feedback* directo sobre la evolución del alumnado (25% de la evaluación final).

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.
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 .

3. **Cuestionario de evaluación.** Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación

6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test 'opción múltiple' (3 opciones). La respuesta correcta está destacada en color verde.

1	Cuando un programa se dedica a recopilar lo que escribimos, hablamos de un:	Keylogger
		Ransomware
		Ataque de diccionario
	Feedback: los <i>Keyloggers</i> son programas maliciosos que una vez instalados recopilan todo lo que escribimos, hasta realizan capturas de pantalla de nuestro dispositivo y lo comparten con el ciberdelincuente.	
2	El principal riesgo de utilizar una contraseña sencilla como 'contraseña' es:	Ataques por diccionario.
		Ataques de araña.
		Keylogger.
	Feedback: un ciberdelincuente solo necesitaría unos segundos para descifrar una contraseña. Por lo tanto, mediante el ataque por diccionario, realizará varias combinaciones de palabras hasta dar con la clave.	
3	¿Cuál de las siguientes prácticas es insegura y peligrosa para la seguridad de nuestras cuentas?	Todas las opciones son inseguras.
		Apuntarlas en un papel.
		Reciclar contraseñas.
	Feedback: ambas opciones son peligrosas, ya que un papel puede estar a la vista de todo el mundo y al reciclar las contraseñas, ponemos en peligro más de una cuenta.	
4	El primer paso para construir una contraseña robusta debe ser:	Unir dos palabras aleatorias.
		Utilizar información personal.
		Usar expresiones hechas.
	Feedback: una contraseña robusta empieza por elegir una combinación de palabras que no tengan nada que ver entre ellas, ni con nosotros, para luego aplicarle modificaciones, como números, mayúsculas, minúsculas y caracteres especiales.	
5	De entre las siguientes opciones, ¿cuáles podríamos considerar una contraseña robusta?	M4resDelMund0!
		12345678
		MiguelHernandez1972
	Feedback: una clave demasiado corta o con información personal, como nuestro nombre y fecha de nacimiento jamás podrá protegernos de los ataques a las contraseñas.	
6	La verificación en dos pasos es un método de protección que mejora la seguridad de nuestras cuentas al:	Enviar un código de confirmación al iniciar sesión.
		Obligar a utilizar una clave robusta.
		Utilizar dos contraseñas en lugar de 1.
	Feedback: al activarla, cada vez que queramos iniciar sesión en nuestra cuenta, tendremos que introducir un código que nos habrá sido enviado por otro canal,	

	como un SMS o un correo electrónico. Sin este código, no podremos iniciar sesión, evitando que terceros puedan acceder incluso aunque tuviesen nuestra contraseña.	
7	Un gestor de contraseñas es una herramienta muy útil, ya que nos ayuda a:	<p>Ambas opciones son correctas.</p> <p>Proteger todas nuestras contraseñas.</p> <p>Construir contraseñas robustas.</p>
	Feedback: los gestores de contraseñas nos ayudan a controlar todas nuestras contraseñas, protegerlas mediante un cifrado y nos echan una mano para construir claves robustas, avisarnos cuando son demasiado sencillas y cuando debemos cambiarlas.	
8	En lo referente a nuestras contraseñas, ¿cuál sería la práctica más recomendada?	<p>Utilizar la verificación en dos pasos, un gestor de contraseñas y contraseñas robustas.</p> <p>Utilizar un gestor de contraseñas con contraseñas robustas, la verificación es opcional.</p> <p>Utilizar solo contraseñas robustas.</p>
	Feedback: la mejor forma de proteger nuestras cuentas es utilizar todas las herramientas que están a nuestra disposición, como un gestor de contraseñas, la verificación en dos pasos, siempre que sea posible y el servicio lo permita, y el uso de contraseñas robustas.	
9	La biometría es una tecnología que nos permite identificarnos por medio de:	<p>Nuestra huella o rostro.</p> <p>Un código enviado al teléfono móvil.</p> <p>Una palabra o pregunta clave.</p>
	Feedback: la biometría es una tecnología con la que podemos identificarnos y demostrar que somos quienes decimos ser mediante el uso de nuestra huella, el rostro e incluso nuestro iris.	
10	En caso de una fuga de información de un servicio online que utilizamos, lo primero que debemos hacer es:	<p>Comprobar la seguridad de nuestras cuentas.</p> <p>Cambiar la contraseña de la cuenta que tengamos en el servicio afectado.</p> <p>Nada, solo afecta al servicio, no a mi cuenta.</p>
	Feedback: ante una fuga de información que haya podido afectar a alguna de nuestras cuentas, lo más seguro es comprobar la seguridad de todas ellas mediante el servicio Have i Been Pwned , por ejemplo. Así nos aseguramos de que ninguna de ellas corre peligro.	

ANEXO

RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- [¡Me han secuestrado mi cuenta!](#)
- [¿Cuánto tardarían en averiguar mis contraseñas?](#)
- [¿Cuentas comprometidas? Compruébalo](#)
- [¿Sabías que el 90% de las contraseñas son vulnerables?](#)
- [Ataques a las contraseñas](#)
- [Cómo proteger las cuentas de juegos online](#)
- [Conoce a fondo qué es el *phishing*](#)
- [Crea tu contraseña segura paso a paso](#)
- [El camino seguro](#)
- [El factor de autenticación doble y múltiple](#)
- [Gestores de contraseñas: ¿cómo funcionan?](#)
- [Guía de privacidad y seguridad en Internet](#)
- [Me robaron la cuenta, ¿qué hago?](#)
- [Mejora tus contraseñas](#)
- [Registrarte con tu cuenta de Google, Facebook o Twitter: ventajas e inconvenientes](#)
- [Típicos errores que cometemos al usar nuestras contraseñas, y cómo corregirlos](#)
- [Una contraseña fácil, ¿pero cuántas cuentas comprometidas?](#)