

# Módulo 1. Protege tu espacio digital

## Módulo 1. Protege tu espacio digital

---



Imagen generada con IA (DALL-E) (CC BY-NC-SA  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En un mundo cada vez más digitalizado, los **dispositivos** que utilizamos diariamente son **herramientas clave** para el trabajo y el estudio. Pero también, son **blancos potenciales de amenazas** que pueden comprometer nuestra

seguridad y privacidad. Proteger nuestro espacio digital es crucial para evitar problemas como el robo de identidad y la invasión a nuestra vida privada.

Este módulo te proporcionará las **habilidades** necesarias para **asegurar tu información** personal y profesional. A lo largo de estas lecciones, aprenderás cómo crear y gestionar **contraseñas robustas**, así como a **proteger tus dispositivos móviles y ordenadores** de amenazas comunes. Al finalizar este módulo, contarás con un conjunto de estrategias efectivas para trabajar de manera segura.

---

Obra publicada con **Licencia Creative Commons Reconocimiento No comercial Compartir igual 4.0 <<http://creativecommons.org/licenses/by-nc-sa/4.0/>>**

# Módulo 1. Protege tu espacio digital

## 1.1 Protegiendo el castillo

Imagina tu espacio digital como un castillo que alberga valiosos secretos y riquezas. Al igual que los castillos medievales dependían de murallas, fosos, y torres de vigilancia para su defensa, nuestro espacio digital requiere medidas de protección equivalentes para salvaguardar nuestra privacidad y seguridad.

Este apartado, denominado '**Protegiendo el castillo**', se centra en estrategias clave para blindar nuestro castillo digital **contra invasores y amenazas**. Exploraremos cómo dispositivos comunes, como los **USB**, pueden convertirse en **amenazas**, la **importancia del cifrado** para proteger nuestros datos y la necesidad de **fortificar** la seguridad de nuestros **dispositivos móviles**, que son puertas de entrada diarias a nuestro mundo digital.



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es) <<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>> )



**Cuando los USB se vuelven contra nosotros**



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

seguridad de tus sistemas.

Los **dispositivos USB** son herramientas cotidianas indispensables para el almacenamiento y transferencia de datos. Sin embargo, también pueden ser una de las vías más directas para **ataques maliciosos** a nuestros sistemas. Desde la propagación de **malware** hasta la ejecución de **ataques físicos**, los dispositivos USB presentan riesgos significativos para la seguridad informática.

Este apartado te enseñará a reconocer y prevenir estos **riesgos**, fortaleciendo así la

### Objetivos:

- Aprender a identificar potenciales amenazas procedentes de dispositivos USB.
- Conocer medidas para prevenir su impacto en la seguridad de nuestros dispositivos.

### Lecturas recomendadas:

- **Rubber Ducky, la amenaza camuflada** [\(INCIBE\)](https://www.incibe.es/empresas/blog/rubber-ducky-simple-memoria-usb). Explora cómo un dispositivo USB común puede convertirse en una herramienta de hacking, exponiendo los riesgos de seguridad de las tecnologías que parecen inofensivas.
- **¡SOS, batería baja! Cuidado con dónde cargas tu dispositivo** [\(INCIBE\)](https://www.incibe.es/empresas/blog/sos-bateria-baja-cuidado-con-).

[donde-cargas-tu-dispositivo>](#) (INCIBE). Aborda los peligros de cargar dispositivos en puertos públicos y ofrece consejos para prevenir ataques mientras recargas tu tecnología.

Para protegerse contra las amenazas que pueden provenir de dispositivos USB, es importante adoptar medidas de seguridad básicas. A continuación, ofrecemos **algunas acciones esenciales** que puedes implementar **para aumentar tu protección**:

- **No insertes dispositivos USB desconocidos en tu equipo.** Esta sencilla acción puede prevenir la mayoría de los ataques que se ejecutan automáticamente al conectar un dispositivo USB malicioso.
- **Deshabilita la ejecución automática.** Evita que el contenido malicioso se ejecute sin tu consentimiento al conectar un dispositivo USB. Esto reduce significativamente el riesgo de infección por malware.
  - Sistemas operativos Windows.
  - Sistemas operativos Linux.
  - Sistemas Operativos MacOS
- **Sé cauteloso al cargar dispositivos en puestos de carga gratuita.** Prioriza llevar tu propio cable. Esta es una práctica segura y recomendable. Para una protección adicional, utiliza protectores de datos USB que impiden la transferencia de datos y permiten solo la carga.



### **Actividad de reflexión (opcional): USB bajo la lupa: Concienciación y Prevención**

**Descripción:** En el foro del curso, comparte tus pensamientos sobre los artículos. ¿Habías oído hablar de estos tipos de amenazas antes? ¿Conoces algún caso cercano relacionado con estos riesgos? ¿Conoces algún otro riesgo asociado a los dispositivos USB?

Discute al menos una medida que podrías tomar para minimizar el riesgo de ser afectado por una amenaza USB.



## **El Poder del cifrado: Protegiendo nuestros datos**

Imaginemos un mundo donde los límites entre la oficina y el hogar se desvanecen, un lugar donde tu sofá se convierte en tu cubículo y tu cafetería favorita en la sala de reuniones. Este escenario no es producto de la ciencia ficción, sino una realidad impulsada por el avance tecnológico, conocida como **BYOD (Bring Your Own Device)**. Nuestros dispositivos personales se convierten en herramientas laborales, cargando **datos sensibles** junto con fotos y mensajes personales.

Sin embargo, esta conveniencia conlleva **riesgos**, un descuido podría comprometer la seguridad de nuestros datos. Para evitarnos un susto, lo mejor que podemos hacer es mantener nuestra información cifrada.

En esta sección, exploraremos cómo el **cifrado** puede integrarse en nuestra rutina diaria, ofreciendo pasos concretos para **proteger dispositivos** y datos personales.



Imagen generada con IA (DALL-E) (CC BY-NC-SA <<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>> )

## Objetivos:

- Entender la importancia del cifrado para la seguridad de los datos.
- Aprender a cifrar y proteger con contraseña la información en dispositivos y plataformas.

## Lecturas recomendadas:

- Cifrado de la información: protege tu principal activo <<https://www.incibe.es/empresas/blog/cifrado-de-la-informacion-protege-el-principal-activo-de-tu-empresa>> (INCIBE). Este artículo aborda la importancia del cifrado como una medida de protección esencial para la información corporativa, destacando métodos y prácticas recomendadas.
- Cifrado y almacenamiento seguro de ficheros paso a paso <<https://www.incibe.es/ciudadania/blog/cifrado-y-almacenamiento-seguro-de-ficheros-paso-paso>> (INCIBE). Una guía detallada sobre cómo implementar el cifrado para el almacenamiento seguro de ficheros, explicando cada paso para una protección efectiva.

**Actividad (opcional):** Cifrado y protección con contraseña de un dispositivo USB

**Descripción:** En esta actividad, aprenderás a cifrar y proteger con contraseña un dispositivo USB. Esta práctica es esencial para garantizar la seguridad de la información almacenada en dispositivos que pueden perderse o ser robados fácilmente.

**Pasos:**

A continuación, veremos, paso a paso, cómo cifrar nuestros dispositivos USB en diferentes sistemas operativos:

**1. Habilitar BitLocker en el dispositivo USB:**

- Conecta el dispositivo USB a tu ordenador.
- Haz clic derecho en el dispositivo USB y selecciona "Activar BitLocker".

**2. Elegir un método de desbloqueo:**

- Selecciona "Usar una contraseña" para crear una contraseña y confirma la contraseña.
- Selecciona "Usar un archivo de clave de recuperación" para guardar un archivo de clave de recuperación en tu ordenador o en un dispositivo de almacenamiento externo.

**3. Elegir cómo guardar la clave de recuperación:**

- Guarda la clave de recuperación en tu cuenta de Microsoft, en un archivo de texto o imprime la clave de recuperación.

#### **4. Cifrar el dispositivo USB:**

- Selecciona "Comenzar el cifrado" para cifrar el dispositivo USB.

#### **5. Desbloquear y usar el dispositivo USB:**

- Desbloquea el dispositivo USB cada vez que lo conectes a un ordenador introduciendo la contraseña o usando el archivo de clave de recuperación.

*Nota: BitLocker está disponible en las ediciones Windows Pro, Enterprise y Education de Windows 10 y Windows 11. Si estás utilizando una edición diferente de Windows, es posible que no tengas acceso a esta función. En el apartado "Para saber mas...", encontrarás sobre una herramienta alternativa, VeraCrypt.*

#### **1. Conectar el dispositivo USB:**

- Conecta el dispositivo USB a tu ordenador.

#### **2. Abrir el Administrador de Discos:**

- Busca "Discos" en el menú de aplicaciones o en el panel de control y selecciona el Administrador de Discos.

#### **3. Seleccionar el dispositivo USB:**

- Selecciona el dispositivo USB en la lista de dispositivos de almacenamiento.

#### **4. Crear una nueva partición:**

- Haz clic con el botón derecho en el dispositivo USB y selecciona "Crear nueva partición".

#### **5. Elegir el tipo de partición:**

- Selecciona "Partición primaria" o "Partición lógica" según tus preferencias.

#### **6. Elegir el tamaño de la partición:**

- Define el tamaño de la partición según tus necesidades.

#### **7. Elegir el sistema de archivos:**

- Selecciona el sistema de archivos deseado, como "ext4" o "ntfs".

#### **8. Asignar una etiqueta de volumen:**

- Asigna un nombre a la partición.

#### **9. Elegir la opción de cifrado:**

- Selecciona la opción de cifrado en el proceso de creación de la partición.

#### **10. Establecer una contraseña:**

- Establece una contraseña para el dispositivo USB cifrado.

#### **11. Confirmar la contraseña:**

- Confirma la contraseña.

#### **12. Finalizar el proceso:**

- Finaliza el proceso de creación de la partición y el cifrado del dispositivo USB.

#### **13. Desmontar y volver a montar el dispositivo USB:**

- Desmonta el dispositivo USB y vuelve a montarlo para que los cambios surtan efecto.

#### **14. Usar el dispositivo USB:**

- A partir de ahora, cada vez que conectes el dispositivo USB, se te pedirá la contraseña para acceder a su contenido.

*Nota: Los pasos descritos pueden variar ligeramente dependiendo de la distribución de Linux que estés utilizando. Si encuentras diferencias en la interfaz o en los nombres de los programas, consulta la documentación específica de tu distribución.*

#### **1. Habilitar FileVault en el dispositivo USB:**

- Conecta el dispositivo USB a tu Mac.
- Abre el Finder y selecciona el dispositivo USB.
- Haz clic derecho en el dispositivo USB y selecciona "Encrypt [Nombre del dispositivo]".
- Introduce una contraseña y confirma la contraseña.
- Opcional: Guarda la contraseña en tu iCloud Keychain.

#### **2. Elegir cómo guardar la contraseña:**

- Si guardaste la contraseña en tu iCloud Keychain, no necesitas hacer nada más.
- Si no guardaste la contraseña en tu iCloud Keychain, asegúrate de guardarla en un lugar seguro, como una nota encriptada o un gestor de contraseñas.

### **3. Cifrar el dispositivo USB:**

- Selecciona "Encrypt Disk" para comenzar el proceso de cifrado.

### **4. Desbloquear y usar el dispositivo USB:**

- Desbloquea el dispositivo USB cada vez que lo conectes a una Mac ingresando la contraseña.

*Nota: FileVault está disponible en las versiones de macOS desde OS X Lion (10.7) en adelante. Si estás utilizando una versión anterior de macOS, es posible que no tengas acceso a esta función. En el apartado "Para saber más...", encontrarás información sobre alternativas de cifrado de disco para macOS.*



Aunque en la actividad anterior nos enfocamos en el cifrado de dispositivos USB, **es posible aplicar el cifrado a una amplia gama de datos y dispositivos**. Existen numerosas herramientas de cifrado disponibles, como VeraCrypt, que se destaca por su capacidad para encriptar **archivos, carpetas y unidades de almacenamiento completo**, proporcionando una solución robusta para la seguridad de los datos.

¡Te animamos a explorar estas opciones para aumentar aún más la seguridad de tus datos!

#### **Recursos adicionales:**

- **VeraCrypt <<https://www.veracrypt.fr/en/Home.html>>** - Visita el sitio oficial para descargar la herramienta. Aquí encontrarás todas las versiones disponibles y documentación relevante.

- **Tutorial de VeraCrypt**  
<https://www.redeszone.net/tutoriales/seuridad/veracrypt-cifrar-archivos-gratis/> - Para aprender a utilizar VeraCrypt y comenzar a cifrar tus archivos y carpetas, consulta este tutorial detallado. Este recurso te guiará paso a paso a través del proceso de cifrado con ejemplos prácticos.
- 



## Blindando tus dispositivos móviles

---



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

La versatilidad de los **smartphones y tablets** nos abre un mundo de posibilidades, desde mantenernos conectados hasta gestionar aspectos cruciales de nuestra vida personal y laboral. Pero, como suele ocurrir, esta conveniencia no está exenta de riesgos. Los dispositivos pueden sufrir daños, ser sustraídos o perdidos, poniendo en peligro la valiosa información que contienen. Piensa por un momento en todo lo que tu dispositivo sabe de ti: contactos, aplicaciones usadas, lugares visitados y mucho más. La pregunta clave es: **¿qué**

**sucede si esta información cae en manos equivocadas?**

No te preocunes; en este apartado aprenderás cómo **configurar tus dispositivos móviles de manera segura**, protegiendo tu información frente a cualquier eventualidad.

**Objetivos:**

- **Reconocer y comprender** los riesgos a los que están expuestos nuestros dispositivos móviles y la información que contienen.
- **Aplicar medidas de protección** para configurar de forma segura nuestros dispositivos, preservando la privacidad y seguridad de nuestros datos personales y profesionales.

#### Lecturas recomendadas:

- **Protege tu móvil iOS y Android con 5 consejos** <<https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos>> (INCIBE). Un artículo que ofrece consejos prácticos para mejorar la seguridad y privacidad de tu dispositivo móvil.
- **Blinda tu smartphone: apps de seguridad para tu dispositivo móvil** <<https://www.incibe.es/ciudadania/blog/blinda-tu-smartphone-apps-de-seguridad-para-tu-dispositivo-movil>> (INCIBE). Explora aplicaciones útiles para fortalecer la seguridad de tus dispositivos móviles.

A continuación, presentamos acciones clave para una protección efectiva.

- **Protege el acceso a tu dispositivo:** Utiliza métodos de bloqueo robustos, como contraseñas, patrones, huella digital o reconocimiento facial, para prevenir accesos no autorizados.



*En Ajustes > Seguridad y Ubicación > Bloqueo de pantalla > Contraseña / Huella digital o Smart Lock > Reconocimiento facial.*



*En Ajustes > Touch ID/Face ID y código.*

	PIN	Contraseña alfanumérica	Patrón	Huella dactilar	Reconocimiento facial	
Android	✓	✓	✓	✓	✓	
iOS	✓	✗	✗	✓	✓	

INCIBE [<https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos>](https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos) (Dominio público)

- **Comprueba que tu dispositivo está actualizado:** Mantener el sistema operativo y las aplicaciones al día es importante para cerrar brechas de seguridad y proteger tus datos contra amenazas recientes.



*Ajustes > Sistema > Ajustes avanzados > Actualización del sistema.*



*Ajustes > General > Actualización de software > Descargar e instalar.*

INCIBE [<https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos>](https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos) (Dominio público)

- **Copias de seguridad:** Realizar copias de seguridad periódicas te permite recuperar tu información fácilmente en caso de pérdida o daño del dispositivo.



#### **COPIA DE SEGURIDAD**

*En Ajustes > Google > Hacer copia de seguridad > Crear una copia de seguridad.*

#### **CIFRADO**

El cifrado se hace por defecto, aunque podemos cifrar una memoria externa en *Ajustes > Seguridad y ubicación > Cifrar almacenamiento de tarjeta SD.*



**iOS**

#### **COPIA DE SEGURIDAD**

*En Ajustes > [nombre] > [seleccionar el dispositivo] > Copia en iCloud > Realizar copia de seguridad ahora.*

Al habilitar la opción se realizarán automáticamente.

#### **CIFRADO**

El cifrado se hace por defecto.

INCIBE [<https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos>](https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos) (Dominio público)

- **Descarga e instala las aplicaciones desde las tiendas oficiales:** Las tiendas oficiales aplican medidas de seguridad para filtrar aplicaciones maliciosas, reduciendo el riesgo de instalar software dañino.



**INCIBE**

<[https://www.incibe.es/ciudadania  
blog/protege-tu-movil-ios-y  
android-con-5-consejos](https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos)>

(Dominio público)

- **Activa el doble factor de autenticación:** Añade una capa extra de seguridad a tus cuentas, requiriendo una segunda forma de verificación además de tu contraseña.



*Ajustes > Google > Gestionar tu cuenta de Google > Seguridad > Verificación en dos pasos > Empezar.*

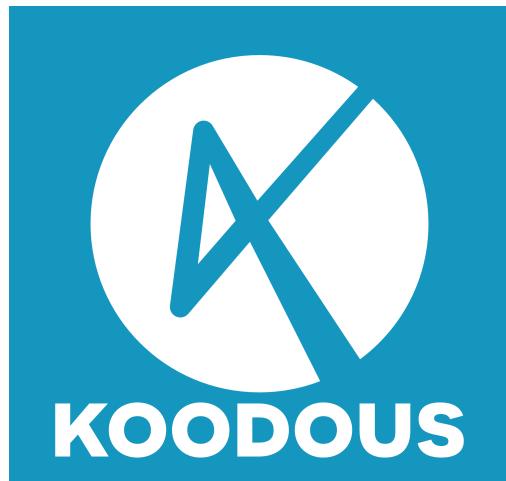


**iOS 10.3 O SUPERIOR:**  
*Ajustes > [nombre] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.*

**INCIBE**

<[https://www.incibe.es/ciudadania  
blog/protege-tu-movil-ios-y  
android-con-5-consejos](https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos)> (Dominio público)

- **Antivirus:** Instalar una aplicación antivirus puede ayudarte a detectar y eliminar malware, así como proteger tu dispositivo de otras amenazas de seguridad.



koodous <<https://koodous.com/>>  
(Dominio público)

- Algo de ayuda extra: Herramientas como Exodus Privacy <[https://play.google.com/store/apps/details?id=org.eu.exodus\\_privacy.exodusprivacy](https://play.google.com/store/apps/details?id=org.eu.exodus_privacy.exodusprivacy)> pueden ofrecer un análisis detallado del estado de seguridad de tu dispositivo, señalando aplicaciones y configuraciones peligrosas. Descarga la app <[https://play.google.com/store/apps/details?id=org.eu.exodus\\_privacy.exodusprivacy](https://play.google.com/store/apps/details?id=org.eu.exodus_privacy.exodusprivacy)> y consulta la web <<https://exodus-privacy.eu.org/en/>> de la organización Exodus para más información.



Exodus <<https://exodus-privacy.eu.org/en/>>  
(Dominio público)

## **Actividad (opcional): Análisis de privacidad y seguridad en Apps**

**Descripción:** Esta actividad tiene como objetivo aumentar la conciencia sobre las implicaciones de seguridad y privacidad de las aplicaciones que instalamos en nuestros dispositivos móviles.

### **Pasos:**

1. Lee el informe de seguridad para la aplicación de McDonald's disponible en el sitio web de Exodus Privacy en el siguiente enlace: **informe de McDonald's** <<https://reports.exodus-privacy.eu.org/es/reports/com.mcdo.mcdonalds/latest/>> . Reflexiona sobre los permisos y **rastreadores** identificados como peligrosos y considera si son adecuados para la función de la aplicación.
2. Descarga la aplicación **Exodus Privacy** <[https://play.google.com/store/apps/details?id=org.eu.exodus\\_privacy.exodusprivacy](https://play.google.com/store/apps/details?id=org.eu.exodus_privacy.exodusprivacy)> en tu dispositivo y realiza un escaneo de seguridad. Identifica aplicaciones en tu dispositivo que tengan permisos excesivos o rastreadores preocupantes.
3. Además de la aplicación, el sitio web de Exodus contiene un **buscador** <<https://reports.exodus-privacy.eu.org/es/>> para investigar informes sobre otras aplicaciones ya analizadas por ellos. Utiliza este recurso para buscar y analizar otra aplicación de tu elección, reflexionando sobre si los rastreadores y permisos son adecuados.

### **Recursos necesarios:**

- Dispositivo móvil Android.
- Acceso a Internet.

**Nota.** Si usas un dispositivo iOS, lamentablemente la aplicación Exodus Privacy no está disponible. Sin embargo, puedes utilizar el sitio web de Exodus para buscar y analizar aplicaciones. En el siguiente apartado exploraremos opciones alternativas para dispositivos iOS.



# Módulo 1. Protege tu espacio digital

## 1.2 Mantenimiento y salud digital

---

En el mundo de la tecnología, un dispositivo digital limpio y ordenado es tan importante como un cuerpo sano. El mantenimiento regular y la **higiene digital** no solo son importantes para la longevidad de nuestros dispositivos, sino también para la protección de nuestra vida digital.

En este apartado, '**Mantenimiento y salud digital**', nos sumergiremos en prácticas para prevenir la acumulación de aplicaciones , conocido como el **síndrome de Diógenes digital**. Hablaremos sobre la importancia de mantener nuestros **sistemas actualizados**, fortaleciendo así nuestros **escudos digitales** contra vulnerabilidades. Además, aprenderemos a gestionar los **permisos** que concedemos a las aplicaciones, y a elegir sabiamente nuestras descargas, priorizando la seguridad y la eficacia.

Este módulo está diseñado para equiparte con las herramientas necesarias para un mantenimiento digital que garantice la integridad y salud de tu espacio digital.



Imagen generada con IA (DALL·E) (**CC BY-NC-SA** <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es> )



**El riesgo del síndrome de Diógenes digital**

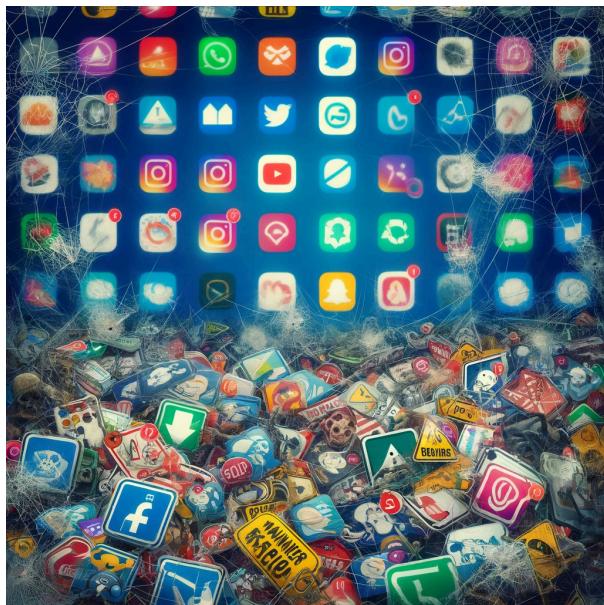


Imagen generada con IA (DALL-E) (**CC BY-NC-SA**

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es> )

uso puede ser un talón de Aquiles en la armadura digital que salvaguarda nuestra información. Es importante abordar este desorden con una estrategia de **limpieza digital** meticulosa, eliminando lo que ya no sirve.

Al igual que un armario desbordado de prendas olvidadas, nuestros dispositivos a menudo se llenan con aplicaciones rara vez utilizadas. Este exceso, lejos de ser inofensivo, conlleva el síndrome de **Diógenes digital**, una tendencia que puede abrir puertas traseras para **amenazas y vulnerabilidades** de seguridad.

Eliminar aplicaciones que no usamos, obsoletas o sospechosas no es solo una cuestión de orden; es un paso hacia la fortificación de nuestros sistemas. Cada aplicación sin

### Objetivos:

- Comprender cómo el exceso de aplicaciones puede comprometer la seguridad del dispositivo.
- Aprender a identificar y desinstalar aplicaciones innecesarias o potencialmente peligrosas.



### Actividad de reflexión (opcional): Revisión y limpieza digital

**Descripción:** Dedica un momento a revisar todas las aplicaciones instaladas en tu dispositivo. Reflexiona sobre cuándo fue la última vez que utilizaste cada una y si su presencia es justificable.

#### Pasos:

1. Enumera todas las aplicaciones que tienes instaladas.
2. Marca aquellas que no has utilizado en los últimos seis meses.
3. Desinstala las aplicaciones que hayas marcado o que consideres riesgosas.



## Actualizaciones: Escudo digital



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Tras realizar una limpieza digital exhaustiva en nuestros dispositivos, es importante entender que este esfuerzo, aunque importante, no es suficiente para asegurar una protección completa. La naturaleza dinámica de las amenazas requiere de medidas adicionales, siendo las **actualizaciones** que nos ofrecen los fabricantes de **software** una de ellas.

Las actualizaciones proporcionan **correcciones críticas** para los sistemas operativos y

aplicaciones, abarcando desde ordenadores y smartphones hasta consolas y dispositivos inteligentes. Al mantener nuestros dispositivos al día, cerramos activamente puertas a potenciales vulnerabilidades, actuando como un **escudo digital** frente a las amenazas más recientes.

### Objetivos:

- Entender la importancia de mantener actualizados nuestros dispositivos y aplicaciones.
- Aprender cómo configurar y gestionar las actualizaciones de manera efectiva.

### Lecturas recomendadas:

- **Minimiza los riesgos de un ataque: ¡actualiza el software!** <<https://www.incibe.es/empresas/blog/minimiza-los-riesgos-ataque-actualiza-el-software>> (INCIBE). Una guía sobre cómo la actualización regular del software puede ayudar a proteger tus sistemas contra amenazas de seguridad emergentes.
- **La importancia de las actualizaciones de seguridad** <<https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/actualizaciones-de-seguridad>> (INCIBE). Explica por qué es crucial mantener actualizados los dispositivos y software para la seguridad informática.

A continuación, presentamos acciones clave para una protección efectiva:

- **Vigilar el estado de actualización** de todos nuestros dispositivos y aplicaciones.

- Elegir la opción de **actualizaciones automáticas**, siempre que esté disponible.
- **No posponer la instalación de actualizaciones**, especialmente las relacionadas con sistemas operativos, navegadores y programas antivirus.

**Nota:** Mantener una aplicación actualizada no implica necesariamente usar la versión más reciente. Por ejemplo, es posible tener Windows 10 al día sin ser la última versión del sistema operativo. Los fabricantes ofrecen actualizaciones para versiones anteriores durante extensos períodos, asegurando así su seguridad y eficiencia sin obligar al salto a versiones más nuevas.

En los siguientes enlaces encontrarás una guía de cómo actualizar los diferentes sistemas operativos, navegadores y programas más conocidos:

- Cómo actualizar el sistema operativo de tus dispositivos  
[<https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-el-sistema-de-tus-dispositivos>](https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-el-sistema-de-tus-dispositivos)
- Cómo actualizar los navegadores de tus dispositivos  
[<https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-los-navegadores-de-tus-dispositivos>](https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-los-navegadores-de-tus-dispositivos)
- Cómo actualizar los programas y aplicaciones de tus dispositivos  
[<https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-los-programas-y-aplicaciones-de-tus-dispositivos>](https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/como-actualizar-los-programas-y-aplicaciones-de-tus-dispositivos)

**Actividad (opcional): ¡Actualizarse o morir!**

**Descripción:** Esta actividad consiste en realizar una revisión exhaustiva del estado de actualización de los sistemas operativos, navegadores, y programas antivirus de tus dispositivos. Procederemos a verificar y aplicar las actualizaciones pendientes siguiendo recomendaciones específicas.

**Pasos:**

1. Revisa el estado de actualización de tu sistema operativo en cada uno de tus dispositivos.
2. Actualiza tu navegador web y programas antivirus a la última versión disponible.
3. Configura las actualizaciones automáticas, si aún no lo has hecho, para garantizar que tu sistema se mantenga actualizado.
4. Y recuerda, si encuentras programas que ya no utilizas, considera desinstalarlos para reducir riesgos de seguridad.



## Permisos a tu medida



Imagen generada con IA (DALL-E) (**CC BY-NC-SA**  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Tras depurar nuestro entorno digital y actualizar sistemas y aplicaciones, surge una pregunta esencial: ¿sabemos realmente a qué información acceden las aplicaciones que usamos? La **gestión de permisos** en **aplicaciones** emerge como un paso crítico en la fortificación de nuestra privacidad digital. Este proceso nos permite no solo conocer, sino controlar el acceso que concedemos a nuestras aplicaciones, desde la ubicación hasta nuestros contactos y archivos.

En este apartado, exploraremos cómo una gestión **consciente** y **meticulosa** de permisos nos ayudará a proteger lo más valioso en el mundo digital: nuestra información personal.

### Objetivos:

- Identificar y comprender la relevancia de los permisos de aplicaciones en la protección de nuestra información personal.
- Desarrollar estrategias para una gestión eficaz de permisos que equilibre funcionalidad y privacidad.

### Lecturas recomendadas:

- **¿Por qué piden tantos permisos las apps?** <<https://www.incibe.es/ciudadania/blog/por-que-piden-tantos-permisos-las-apps>> (INCIBE). Este artículo explora las razones detrás de los extensos permisos que solicitan las aplicaciones móviles y cómo afectan la privacidad del usuario.
- **Cómo gestionar los permisos de ubicación de las aplicaciones** <<https://www.incibe.es/incibe/sala-de-prensa/gestionar-los-permisos-ubicacion-las-aplicaciones>> (INCIBE). Proporciona una guía detallada sobre cómo los usuarios pueden controlar y gestionar los permisos de ubicación en sus aplicaciones para mejorar la seguridad y privacidad.

Los permisos en tu teléfono actúan como **guardianes**. Imagina que cada app es un visitante que quiere usar diferentes partes de tu casa (teléfono). Por ejemplo, algunos pueden querer usar la cocina (micrófono) o el estudio (cámara). Los permisos son las reglas que deciden qué partes de tu casa pueden visitar estos invitados.

Si una app no tiene permiso para entrar a la cocina, no puede usar el micro. Existen muchos tipos de permisos, desde usar la cámara hasta leer tus mensajes, asegurando que solo las apps que tú elijas accedan a tus cosas importantes.

Muchas veces, las aplicaciones gratuitas solicitan permisos para acceder a funciones esenciales, como usar el micrófono para una app de grabación. Sin embargo, algunas van más allá, pidiendo acceso a tu ubicación, contactos y más, lo cual puede parecer innecesario. Este es el "**negocio**" detrás de muchas apps gratuitas: **recopilan** tu **información personal** y la utilizan con **fines publicitarios** o simplemente **venderla** al mejor postor. Y lo más sorprendente es que, al instalar estas apps y aceptar sus permisos, les damos legalmente el derecho a hacerlo.



	 Calendario	 Contactos	 Cámara/Micrófono	 Memoria	 Mensajes De texto	 Sensores Del cuerpo	 Teléfono	 Ubicación	Otros permisos
Suplantación de identidad	✓	✓	✓	✓	✓				
Robo de datos personales y confidenciales	✓			✓	✓		✓		
Publicidad dirigida	✓		✓			✓		✓	
Ataques de ingeniería social y phishing	✓	✓		✓	✓	✓	✓	✓	
Riesgo para la seguridad física	✓							✓	
Envío de spam, fraudes y malware		✓			✓		✓		
Pérdida de privacidad			✓					✓	
Extorsión/sextorsión			✓	✓					

INCIBE <<https://www.incibe.es/ciudadania/formacion/infografias/permisos-de-apps-y-riesgos-para-tu-privacidad>> (Dominio público)

A continuación, presentamos acciones clave para una protección efectiva:

- **Revisar los permisos** de cada aplicación instalada, asegurándose de que solo tengan acceso a lo estrictamente necesario.
- **Modificar los permisos que no sean necesarios** para realizar las funciones de la aplicación o que comprometan la privacidad.

- [Dispositivos Android](#)
- [Dispositivos iOS](#)
- Utilizar herramientas externas y funcionalidades de seguridad integradas en el sistema operativo, para gestionar los permisos de forma efectiva.
  - [Dispositivos Android](#)
  - [Dispositivos iOS](#)

**Nota:** Es una buena práctica revisar periódicamente los permisos de tus aplicaciones para asegurarte de que solo tienen acceso a la información necesaria y mantener tu privacidad segura.

#### **Actividad (opcional): Auditoría express de permisos**

**Descripción:** Realiza una auditoría rápida de los permisos de aplicaciones en tu dispositivo para identificar posibles riesgos a tu privacidad.

**Paso 0:** Antes de comenzar, te invitamos a "[Acepto o no acepto <https://www.incibe.es/ciudadania/formacion/actividades/acepto-no-acepto>](https://www.incibe.es/ciudadania/formacion/actividades/acepto-no-acepto)" de INCIBE, te ayudará a comenzar a identificar permisos inadecuados.

#### **Pasos:**

1. Selecciona 5 aplicaciones que uses frecuentemente en tu dispositivo.
2. Revisa y anota los permisos que cada una utiliza.
3. Trata de identificar al menos un permiso que consideres innecesario.
4. Modifica o revoca aquellos permisos que consideres innecesarios, si has encontrado alguno.

#### **Recursos necesarios:**

- Dispositivo móvil con acceso a configuración de aplicaciones.
- Hoja de notas o documento digital para registrar tus hallazgos.



## **Recursos educativos**



Imagen generada con IA (DALL-E) (CC BY-NC-SA  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es> )

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para promover el **mantenimiento y salud digital** entre nuestros estudiantes.

- **Guía para configurar dispositivos móviles:** Una guía completa que te enseñará a configurar adecuadamente los dispositivos móviles para asegurar tu privacidad y seguridad. Accede a la guía [aquí](https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles) <https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles> .
- **5 consejos de seguridad para dispositivos móviles:** Infografía con consejos para la seguridad en dispositivos móviles. [Descargar documento](https://www.incibe.es/sites/default/files/docs/osi-5-consejos-seguridad-dispositivos-moviles.pdf) <https://www.incibe.es/sites/default/files/docs/osi-5-consejos-seguridad-dispositivos-moviles.pdf> .
- **Acepto, no acepto:** Juego interactivo sobre permisos de aplicaciones. [Enlace](#) [al](#) [juego](#)

<https://www.incibe.es/ciudadania/formacion/actividades/acepto-no-acepto> .

---

Obra publicada con **Licencia Creative Commons Reconocimiento No comercial Compartir igual 4.0** <http://creativecommons.org/licenses/by-nc-sa/4.0/>

# Módulo 1. Protege tu espacio digital

## 1.3 Guardianes de contraseñas seguras

Las contraseñas actúan como los guardianes de nuestra vida digital, abriendo y cerrando el acceso a toda nuestra información. En '**Guardianes de contraseñas seguras**', exploraremos cómo fortalecer estas defensas para mantener a raya a intrusos y proteger lo que más valoramos. Desde entender el valor de una contraseña fuerte hasta adoptar prácticas que aseguren su efectividad, cada paso es vital en la protección de nuestra identidad digital.

Nos adentraremos en estrategias para **construir contraseñas sólidas**, la importancia de **gestores de contraseñas** y la exploración de capas adicionales de seguridad que van más allá de la contraseña. Con **herramientas adecuadas** y un enfoque proactivo, convertiremos nuestras credenciales en verdaderos baluartes contra las amenazas ciberneticas.



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es) [<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es) )



Evaluando nuestra primera línea de defensa



Imagen generada con IA (DALL-E) (**CC BY-NC-SA** <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

hace fuertes o débiles. Esto nos equipará con el conocimiento necesario para tomar decisiones sobre cómo **proteger nuestras cuentas en línea** de manera efectiva.

Después de haber reflexionado sobre la persistencia de contraseñas débiles y la importancia de fortalecer nuestra primera línea de defensa, es momento de llevar esa conciencia a la práctica. Ahora, daremos un paso hacia la acción: analizar la robustez de nuestras contraseñas y descubrir si han sido expuestas en alguna **brecha de seguridad** previa.

Mediante el uso de herramientas de análisis, no solo realizaremos una **evaluación de nuestras contraseñas**, sino que también aprenderemos sobre qué las

## Objetivos:

- Comprender la importancia de revisar y actualizar regularmente las medidas de seguridad.
- Identificar debilidades en la seguridad actual y planificar mejoras.

## Lecturas recomendadas:

- **La importancia de la seguridad de contraseñas y las brechas de datos** <https://www.verizon.com/business/resources/reports/dbir/> (Verizon). Destaca la importancia de la seguridad de contraseñas y aborda el impacto de las brechas de datos.
- **Las mayores brechas de datos de 2023: Cómo ocurrieron y qué significan para ti** <https://www.wired.com/story/moveit-breach-victims/> (Wired). Analiza las brechas de datos más importantes del año 2023,

explicando cómo ocurrieron y cuáles fueron sus consecuencias para los usuarios afectados.

Utilizaremos una herramienta en línea para analizar la robustez de nuestras contraseñas y entender los elementos que contribuyen a su fortaleza.

#### **Pasos:**

1. Visita **NordPass Secure Password** <<https://nordpass.com/es/secure-password/>> .
2. Introduce la contraseña que deseas evaluar.
3. Analiza el resultado, prestando atención en la solidez, tiempo estimado para descifrar la contraseña, y otros indicadores proporcionados.

**¿Te ha salido que tu contraseña es débil?** No te preocupes, en el siguiente apartado veremos como generar contraseñas seguras.

#### **Demostración práctica:**

Veamos un par de ejemplos de análisis de contraseñas en NordPass Secure Password.

- **Prueba de seguridad de una contraseña segura:**



NordPass <<https://nordpass.com/es/secure-password/>> (Dominio público)

La imagen muestra un análisis de seguridad de contraseña con cuatro áreas clave:

1. Campo para introducir la contraseña.
2. Indicador de fortaleza de la contraseña, en este caso etiquetado como "SÓLIDA"
3. Tiempo estimado para descifrar la contraseña marcado como "siglos".
4. Lista de los criterios que cumple la contraseña introducida, en este caso, todos.

- **Prueba de seguridad de una contraseña débil:**

Vamos a comprobar una de las contraseñas de las contenidas en el artículo que leímos en el apartado anterior (**Top 200 contraseñas más seguras <<https://nordpass.com/es/most-common-passwords-list/>>** ), concretamente:



Vamos a analizarla:



NordPass <<https://nordpass.com/es/secure-password/>> (Dominio público)

La imagen muestra un análisis de seguridad de contraseña con cuatro áreas clave:

1. Campo para introducir la contraseña.
2. Indicador de fortaleza de la contraseña, en este caso etiquetado como "DÉBIL"
3. Tiempo estimado para descifrar la contraseña marcado como "menos de un segundo".
4. Lista de los criterios que cumple la contraseña introducida, en este caso uno.

Como dato curioso, si volvemos al artículo, podemos ver que 302.709 usuarios/-as de la base de datos analizada por los investigadores utilizaban dicha contraseña.

En un mundo donde cada día escuchamos hablar de **ciberataques** a empresas y robos masivos de información, nos preguntamos: **¿qué buscan los ciberdelincuentes?** Más allá del dinero y la fama, los **datos** son un tesoro muy codiciado. Y entre esos datos, las **credenciales** de usuario, es decir, nuestras **contraseñas**, ocupan un lugar privilegiado.

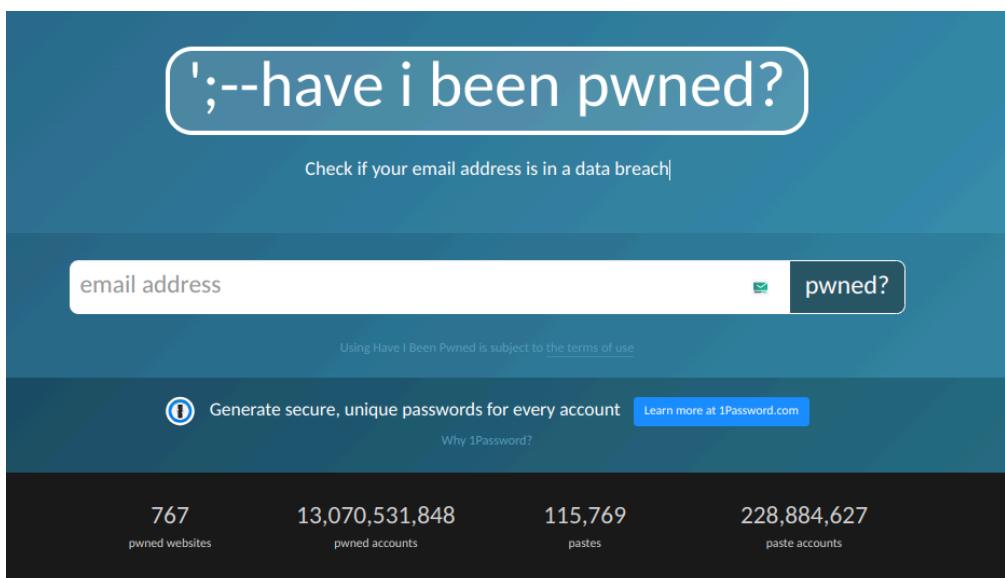
Esos datos suelen terminar en la **Deep Web**, donde se comercian en mercados clandestinos. No entra en los objetivos de este curso estudiar cómo acceder a la Deep Web, pero tampoco será necesario en este caso, ya que esos datos, después de ser vendidos, dan vueltas por internet hasta que algunos emergen a la superficie en sitios como **Pastebin**. Este sitio fue creado para compartir código entre programadores, pero también se utiliza para intercambiar **información sensible**. Allí se pueden encontrar desde números de tarjetas de crédito hasta bases de datos completas de correos y contraseñas hackeadas.

Si realizamos **búsquedas avanzadas en Google**, obtendremos resultados sorprendentes. Haz clic en los siguientes enlaces para ver las búsquedas en Google:

- Cuentas de Instagram hackeadas <<https://www.google.com/search?q=site%3Apastebin.com+instagram+hacked>>
- Cuentas de Gmail hackeadas <<https://www.google.com/search?q=site%3Apastebin.com+gmail+hacked>>
- Filtraciones de tarjetas de crédito <<https://www.google.com/search?q=site%3Apastebin.com+credit+card+leak>>

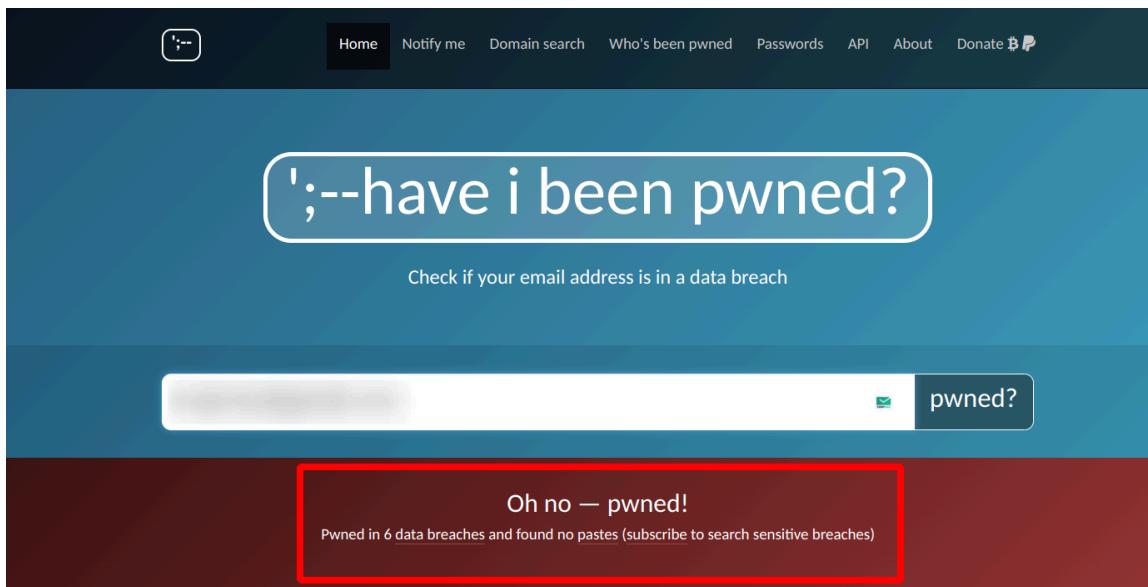
Como vemos, se nos muestra una serie de páginas dentro de Pastebin con información de dudosa procedencia. Volviendo a la pregunta inicial, **¿estás seguro de que nunca has sido hackeado?**

Existen **plataformas** que permiten a los usuarios **verificar** si sus **cuentas** han podido ser **comprometidas**. Una de estas plataformas es **Have I Been Pwned**, [<https://haveibeenpwned.com/>](https://haveibeenpwned.com/) uno de los servicios más reconocidos para este fin.



<https://haveibeenpwned.com/>      <[https://haveibeenpwned.com/>](https://haveibeenpwned.com/)  
(Dominio público)

Una vez en la web, introducimos nuestro email, y la herramienta lo cotejará con los datos recogidos de las filtraciones de datos que se han publicado en Internet y nos informará si existe una coincidencia. Simplemente introduciendo nuestro correo electrónico, podemos descubrir si nuestras credenciales figuran en alguna de las muchas bases de datos resultantes de brechas de seguridad en diversos sitios web.



[https://haveibeenpwned.com/ <https://haveibeenpwned.com/>](https://haveibeenpwned.com/) (Dominio público)

El correo proporcionado ha aparecido en fugas de datos, concretamente en 6 diferentes, sugiriendo que la contraseña asociada podría estar comprometida. Si hacemos scroll hacia abajo veremos los distintos servicios a través de los cuales nuestras cuentas fueran comprometidas.

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



**Cit0day (unverified):** In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords



**CoinMarketCap:** During October 2021, 3.1 million email addresses with accounts on the cryptocurrency market capitalisation website CoinMarketCap were discovered being traded on hacking forums. Whilst the email addresses were found to correlate with CoinMarketCap accounts, it's unclear precisely how they were obtained. CoinMarketCap has provided the following statement on the data: "CoinMarketCap has become aware that batches of data have shown up online purporting to be a list of user accounts. While the data lists we have seen are only email addresses (no passwords), we have found a correlation with our subscriber base. We have not found any evidence of a data leak from our own servers – we are actively investigating this issue and will update our subscribers as soon as we have any new information."

Compromised data: Email addresses



**Gravatar:** In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames



**Nitro:** In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Names, Passwords



**ShareThis:** In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Names, Passwords



**Terravision:** In February 2023, the European airport transfers service Terravision suffered a data breach. The breach exposed over 2M records of customer data including names, phone numbers, email addresses, salted password hashes and in some cases, date of birth and country of origin. Terravision did not respond to multiple attempts by individuals period over a period of months to report the incident.

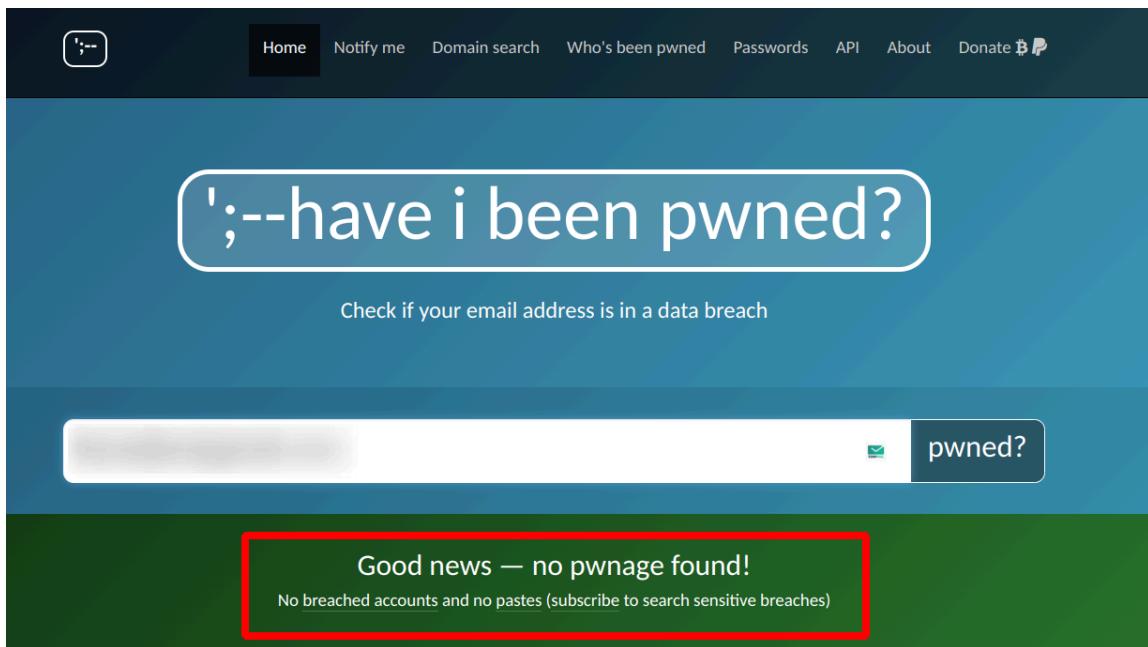
Compromised data: Dates of birth, Email addresses, Geographic locations, Names, Passwords, Phone numbers

<https://haveibeenpwned.com/>

<<https://haveibeenpwned.com/>> (Dominio público)

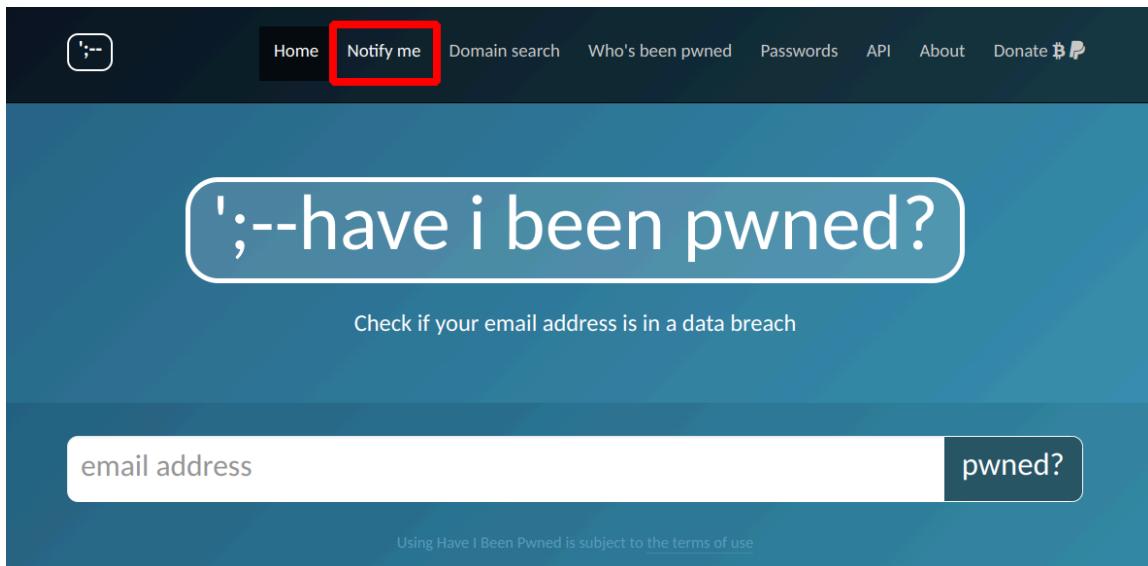
En este caso, lo primero y fundamental será cambiar las contraseñas de las cuentas de aquellos servicios que hayan sido comprometidos; y, en el caso de que dicha combinación de correo y contraseña la estemos usando en otros servicios, también deberemos cambiarlo.

A continuación vemos otro ejemplo, en el que la cuenta no ha sido comprometida:



<https://haveibeenpwned.com/> <<https://haveibeenpwned.com/>> (Dominio público)

En HaveIBeenPwned, la función "**Notify me**" nos permite registrar nuestro correo electrónico para **recibir alertas automáticas** si éste se ve implicado en una brecha de seguridad.



<https://haveibeenpwned.com> <<https://haveibeenpwned.com>> (Dominio público)

Además de esta herramienta, existen muchas otras, como **FirefoxMonitor** <<https://monitor.firefox.com/>> o **Dehashed** <<https://www.dehashed.com/>> , que ofrecen un servicio similar, y que conviene visitarlas también para verificar que no hay más filtraciones de datos.

Ver todos los sitios donde tu información está expuesta				
Filtro	Empresa	Fecha de la identificación	Estado	⋮
T	Terravision	23 abr 2023	Acción necesaria	⋮
G	Gravatar	5 dic 2021	Acción necesaria	⋮
C	CoinMarketCap	22 oct 2021	Acción necesaria	⋮
N	Nitro	19 ene 2021	Acción necesaria	⋮
S	ShareThis	3 mar 2019	Acción necesaria	⋮

<https://monitor.mozilla.org/> <<https://monitor.mozilla.org/>> (Dominio público)

The screenshot shows the homepage of Dehashed. At the top, there is a dark blue header with white text that reads "TAKE YOUR EMPLOYEE SECURITY TO THE NEXT LEVEL." To the right of the text is a graphic of a clipboard with a checklist and a red checkmark. Below the header, the word "DEHASHED" is written in large, bold, white capital letters. Underneath it, the text "14,453,524,118 COMPROMISED ASSETS" is displayed in a smaller white font. In the center of the page is a search bar with three input fields: "FIELD(S) ▾", "Search for anything...", and "SEARCH". Below the search bar, there is a small explanatory text: "Search for specific fields by adding 'fieldname:' before query or by using some premade buttons located to the left of search bar." At the bottom of the page, there is a link: "Click Here to View Our Updated Search Operators and Learn How to Utilize Regex, and the True Power of DeHashed ↗".

<https://www.dehashed.com/> <<https://www.dehashed.com/>> (Dominio público)

### **Actividad (opcional): Auditoría de seguridad de tus contraseñas**

**Descripción:** Evalúa la seguridad de tus contraseñas personales utilizando herramientas en línea para entender su robustez y si han sido expuestas.

#### **Pasos:**

1. Accede a **NordPass** <<https://nordpass.com/es/secure-password/>> y comprueba la fortaleza de tus contraseñas más usadas.
2. Visita **Have I Been Pwned** <<https://haveibeenpwned.com/>> y verifica si tus cuentas de correo han sido comprometidas.
3. Registra tu correo en la función "Notify me" de **Have I Been Pwned** <<https://haveibeenpwned.com/>> .
4. Reflexiona sobre los resultados y considera cambiar las contraseñas que resulten débiles o expuestas.

#### **Recursos necesarios:**

- Conexión a internet.
- Dispositivo con acceso a un navegador web.
- Acceso a tu cuenta de correo para confirmar la suscripción a la función "Notify me".



A pesar de que nos bombardean continuamente con consejos sobre **la seguridad de nuestras contraseñas**, las contraseñas simples como "123456" persisten, liderando listas de las más usadas. Esta preferencia por lo predecible no solo facilita el trabajo de los atacantes sino que también **expone nuestras cuentas** a riesgos innecesarios.

Te invitamos a, **reflexionar sobre nuestras prácticas actuales**, examinando las tendencias en el uso de contraseñas a través de las lecturas recomendadas.

### Lecturas Recomendadas:

- **Contraseñas más utilizadas en 2023: un vistazo a la seguridad digital** <<https://www.welivesecurity.com/es/contrasenas/contrasenas-mas-utilizadas-2023-seguridad-digital-latinoamerica/>> (WeLiveSecurity). Un análisis de las contraseñas más populares revela hábitos preocupantes que comprometen la seguridad en línea.
- **Top 200 de las contraseñas más comunes del año** <<https://nordpass.com/most-common-passwords-list/>> (NordPass). Explora la lista de contraseñas más comunes y comprende por qué representan una amenaza para la seguridad.



### Construyendo muros robustos

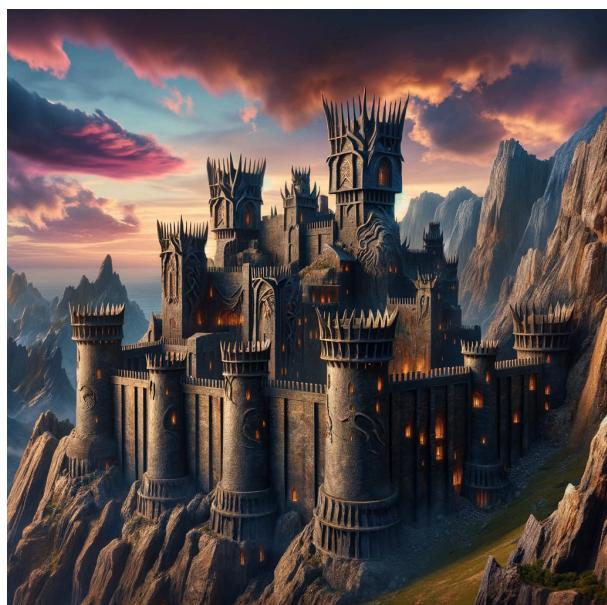


Imagen generada con IA (DALL-E) (**CC BY-NC-SA** <<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>> )

Tras haber evaluado la fortaleza de nuestras contraseñas y revisado si han sido comprometidas, es hora de avanzar al siguiente nivel: '**Construyendo muros robustos**'. Si nuestras credenciales son las llaves de nuestros castillos digitales, asegurarnos de que éstas sean indestructibles es esencial para prevenir accesos no deseados.

En este apartado, exploraremos las **características** de una **contraseña segura**: longitud adecuada, complejidad y unicidad. Además, veremos la

importancia de **evitar la repetición** de contraseñas a través de múltiples plataformas.

Acompáñanos a descubrir cómo construir muros robustos alrededor de tu información personal, asegurando que tus contraseñas no solo sean difíciles de descifrar, sino también un bastión infranqueable contra los intentos de invasión digital.

### **Objetivos:**

- Comprender los elementos que constituyen una contraseña robusta.
- Aplicar prácticas seguras en la creación y gestión de contraseñas para proteger el acceso a información personal y profesional.

### **Lecturas recomendadas:**

- **Consejos para crear contraseñas seguras y robustas** <<https://www.welivesecurity.com/la-es/2023/05/04/consejos-crear-politica-contrasenas-empresa/>> (WeLiveSecurity). Proporciona guías detalladas y estrategias efectivas para establecer políticas de contraseñas fuertes en el entorno empresarial.
- **Cómo crear una contraseña fuerte** <<https://cybernews.com/best-password-managers/how-to-create-a-strong-password/>> (CyberNews). Ofrece técnicas y consejos prácticos para generar contraseñas seguras que protejan tus cuentas digitales de manera efectiva.

Antes de sumergirnos en la creación de nuestras contraseñas, vamos a revisar las **pautas** que definen una contraseña segura y sólida:

- **Longitud mínima:** Asegúrate de que tu contraseña tenga al menos 12 caracteres.
- **Combinación de caracteres:** Utiliza una mezcla de mayúsculas, minúsculas, números y símbolos.
- **No utilices información personal:** Evita fechas de nacimiento, nombres propios o cualquier dato fácilmente asociable contigo.
- **Frases de contraseña:** Considera usar frases largas y fáciles de recordar, pero difíciles de adivinar.
- **Evita patrones comunes:** Secuencias como "1234" o "abcd" son extremadamente inseguras.
- **La regla de oro, diversificar:** No recicles contraseñas. Cada cuenta debe tener una contraseña única.
- **Cambios periódicos:** Considera actualizar tus contraseñas cada cierto tiempo para reducir el riesgo de compromiso a largo plazo.

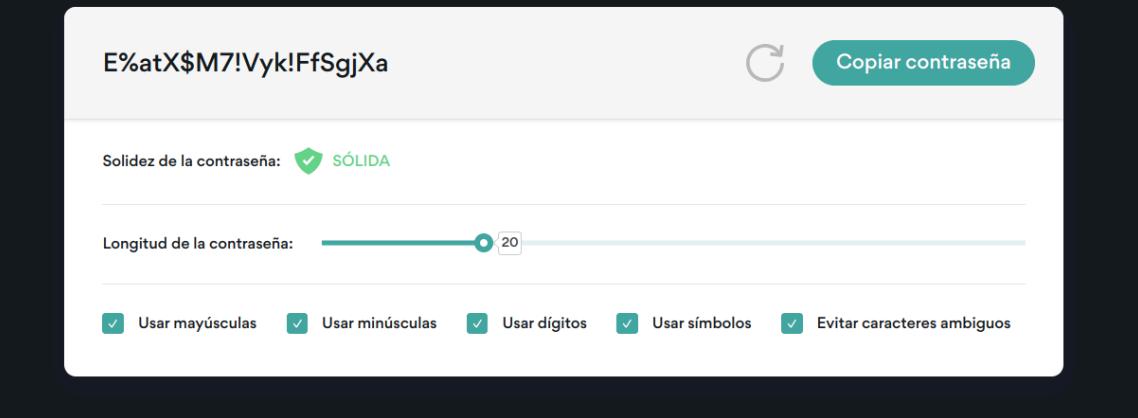
Los generadores de contraseñas son herramientas que crean contraseñas robustas y complejas. Estos generadores emplean algoritmos para fabricar contraseñas aleatorias, que superan cualquier intento de predicción o patrones comunes. La ventaja principal es su capacidad para ofrecer claves que nosotros mismos no podríamos imaginar, y que, por ende, son extremadamente difíciles de vulnerar por atacantes o programas maliciosos.

Aquí tienes **algunos generadores** que puedes usar **para reforzar tu seguridad en línea:**

- **Generador de NordPass <<https://nordpass.com/es/password-generator>>** : Define las características y obtén una contraseña sólida al instante.

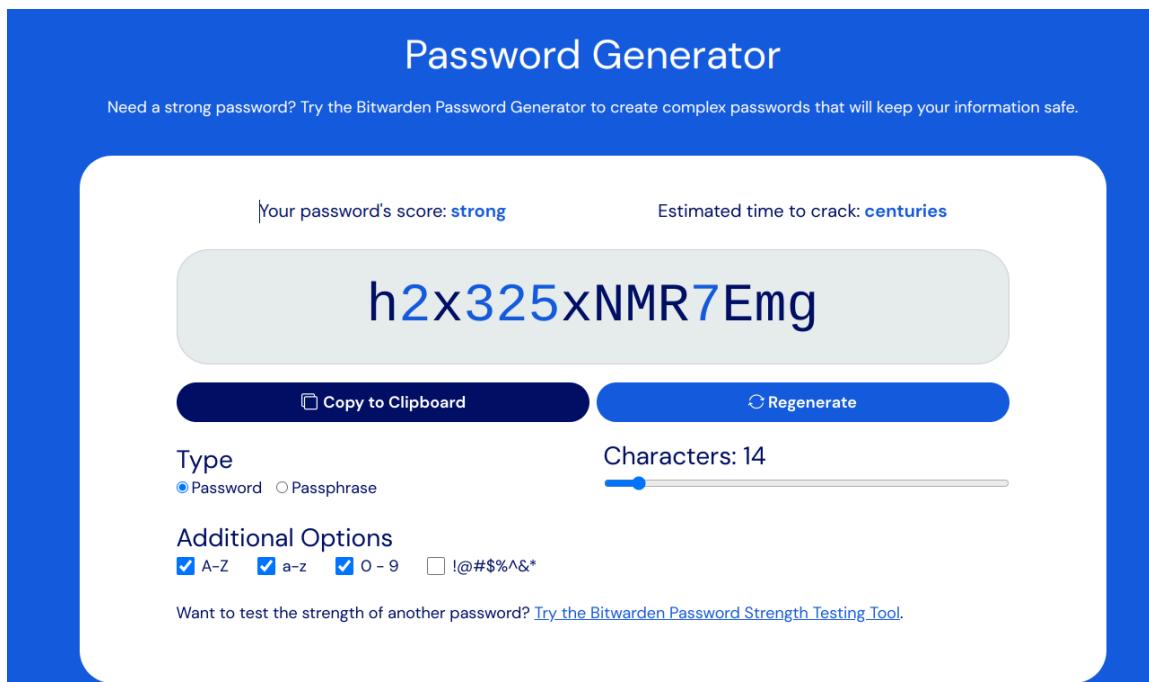
# Generador de contraseñas de NordPass

Crea contraseñas únicas y almacénalas de forma segura en NordPass.



<https://nordpass.com/es/password-generator/>  
<<https://nordpass.com/es/password-generator/>> (Dominio público)

- Generador de Bitwarden <<https://bitwarden.com/password-generator/#password-generator>> : Personaliza tu contraseña con múltiples opciones de seguridad.



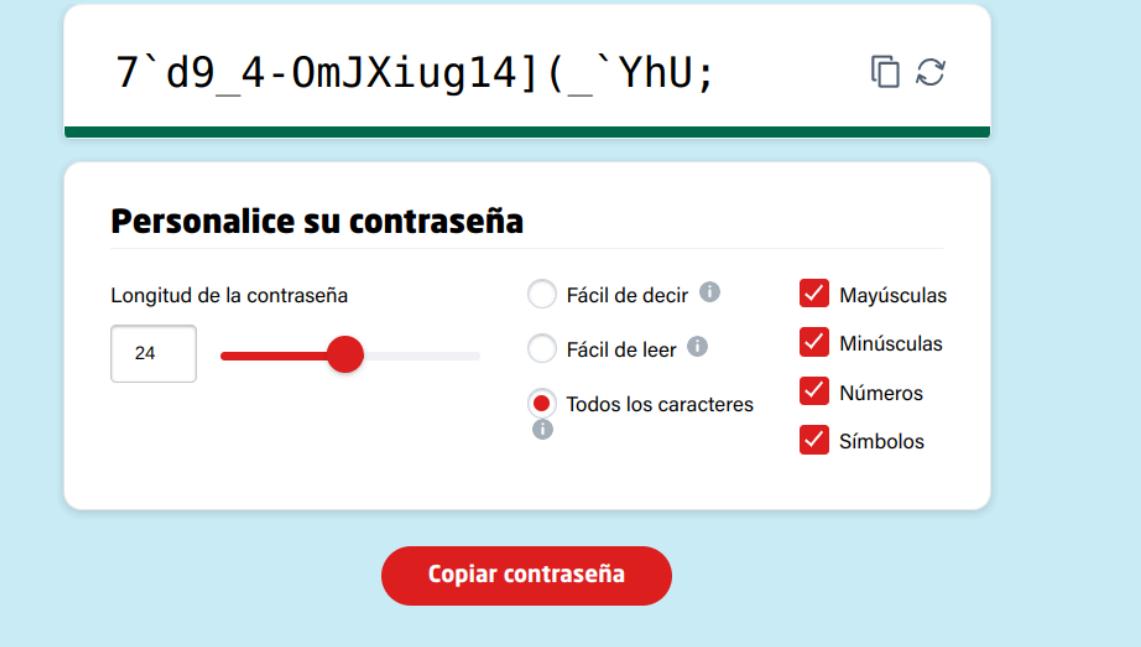
<https://bitwarden.com/password-generator/#password-generator>  
<<https://bitwarden.com/password-generator/#password-generator>> (Dominio

público)

- Generador de **LastPass** <<https://www.lastpass.com/es/features/password-generator#generatorTool>> : Opción dual, genera automáticamente o escribe tú la contraseña y ajústala hasta alcanzar el nivel óptimo de seguridad.

## Genere una contraseña aleatoria y segura al instante con la herramienta online de LastPass

Vaya más allá de los generadores de contraseñas con [LastPass Premium](#). Con independencia del dispositivo o la aplicación que utilice, todas sus contraseñas se crearán, guardarán y sincronizarán de manera automática. Esté donde esté.



[<https://www.lastpass.com/es/features/password-generator#generatorTool>](https://www.lastpass.com/es/features/password-generator#generatorTool)  
(Dominio público)

**Actividad opcional:** Construyendo el arsenal perfecto

**Descripción:** Experimenta con diferentes generadores de contraseñas para crear una clave robusta y evalúa su fortaleza con herramientas

especializadas.

#### Pasos:

1. Selecciona tres generadores de contraseñas online diferentes (de entre los vistos u otros que encuentres).
2. Crea una contraseña con cada uno, siguiendo las recomendaciones de robustez (mínimo 12 caracteres, uso de mayúsculas, minúsculas, números y símbolos).
3. Utiliza [<https://password.es/comprobador/>](https://password.es) para comprobar la fortaleza de cada contraseña generada.
4. Reflexiona sobre la diversidad y complejidad de las contraseñas creadas y la importancia de estas características para la seguridad.

#### Recursos necesarios:

- Acceso a internet y navegador web.
- Enlaces a generadores de contraseñas como **NordPass** [<https://nordpass.com/es/password-generator/>](https://nordpass.com/es/password-generator), **Bitwarden** [<https://bitwarden.com/password-generator/#password-generator>](https://bitwarden.com/password-generator/#password-generator), y **LastPass** [<https://www.lastpass.com/es/features/password-generator#generatorTool>](https://www.lastpass.com/es/features/password-generator#generatorTool).
- Acceso a [<https://password.es/comprobador/>](https://password.es) para evaluar las contraseñas.



Pensar en **memorizar contraseñas largas y complejas** para cada cuenta puede parecer tan desalentador como **subir una montaña con los bolsillos llenos de piedras**. ¡Pero tranquilo! A continuación veremos una solución para esto...



## Tu cofre forte digital

---



Imagen generada con IA (DALL-E) ([CC BY-NC-SA](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

necesario, fusionando seguridad con conveniencia. En este apartado, exploraremos cómo los gestores de contraseñas se convierten en un elemento esencial de nuestra ciberseguridad, **reforzando la protección de nuestras credenciales.**

Llegados a este punto, nos enfrentamos a una paradoja de la era digital: cuanto más complejas y seguras hacemos nuestras contraseñas, más nos cuesta recordarlas y administrarlas. Aquí es donde entran en juego los **gestores de contraseñas**, verdaderos cofres digitales que nos liberan de la carga de memorizar incontables claves.

Estas herramientas no solo **almacenan** nuestras contraseñas de manera segura, sino que también las crean y autocompletan cuando es

### Objetivos:

- Comprender el funcionamiento y beneficios de un gestor de contraseñas.
- Aprender a implementar prácticas de seguridad que mejoren la gestión de tus accesos en línea.

### Lecturas recomendadas:

- Gestores de contraseñas <<https://www.incibe.es/node/499093>> (INCIBE). Un recurso detallado que proporciona información esencial sobre el uso y beneficios de los gestores de contraseñas para mejorar la seguridad en línea.
- Gestores de contraseñas gratuitos <[https://www.incibe.es/ciudadania/filtro/herramientas?tid=303607&tid\\_1>All&tid\\_2>All&tid\\_3>All](https://www.incibe.es/ciudadania/filtro/herramientas?tid=303607&tid_1>All&tid_2>All&tid_3>All)> (INCIBE). Explora diferentes opciones de gestores de contraseñas gratuitos disponibles, ayudando a los usuarios a seleccionar uno que se adapte a sus necesidades específicas.

Los **gestores de contraseñas** son aplicaciones diseñadas para **guardar nuestras credenciales**, como usuarios y contraseñas, vinculadas a los sitios web que utilizamos. Todo se almacena en una base de datos segura, cifrada a través de una contraseña maestra. Esto nos permite administrar una variedad de cuentas y claves desde una única plataforma, reduciendo la carga de tener que recordar múltiples contraseñas; solo necesitamos recordar una clave maestra.

Las características del gestor, dependerán del proveedor, pero generalmente incluyen:

- **Compatibilidad con múltiples dispositivos**, disponibles para ordenadores, móviles y tabletas. Esto te permite acceder a tus contraseñas de forma segura desde cualquier dispositivo con acceso a internet.
- **Almacenamiento seguro**, mediante técnicas de cifrado robustas para proteger tus contraseñas y datos confidenciales.
- **Generadores de contraseñas automáticos**, eliminando el esfuerzo de crear contraseñas robustas y únicas para cada servicio.
- **Plugins para navegadores y funciones de autocompletado**, que simplifican la gestión de accesos a servicios web.
- **Alertas de vulnerabilidad**, para advertirnos sobre contraseñas débiles, repetidas o servicios que han sufrido brechas de seguridad.

¿**Las ventajas?** Primero, la **seguridad**. Cada contraseña es única y compleja, un enigma para los ciberdelincuentes. Segundo, la **comodidad**. Olvídate de memorizar o escribir contraseñas; tu gestor lo hace por ti. Y tercero, la **eficiencia**. Con todas tus claves en un solo lugar, gestionar tus cuentas es más rápido y sencillo.

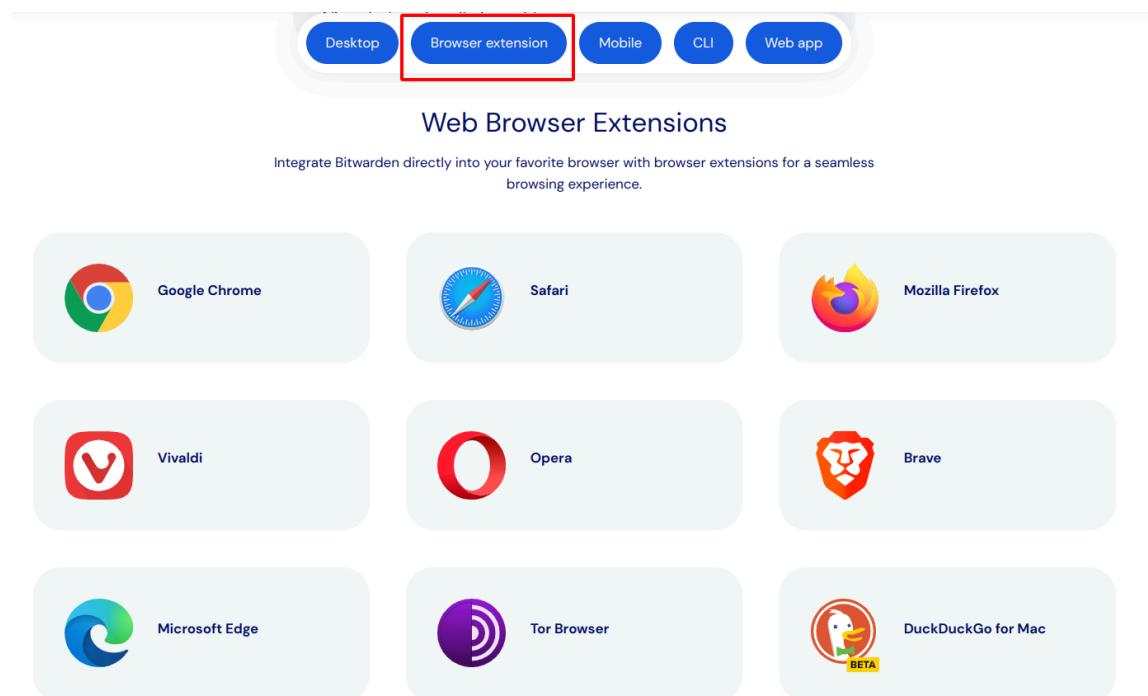
## Configurando Bitwarden: Un tutorial paso a paso

Aunque hay diversos gestores de contraseñas disponibles para distintos dispositivos y plataformas, todos comparten funciones básicas con algunas diferencias menores. En esta guía, nos centraremos en cómo configurar y

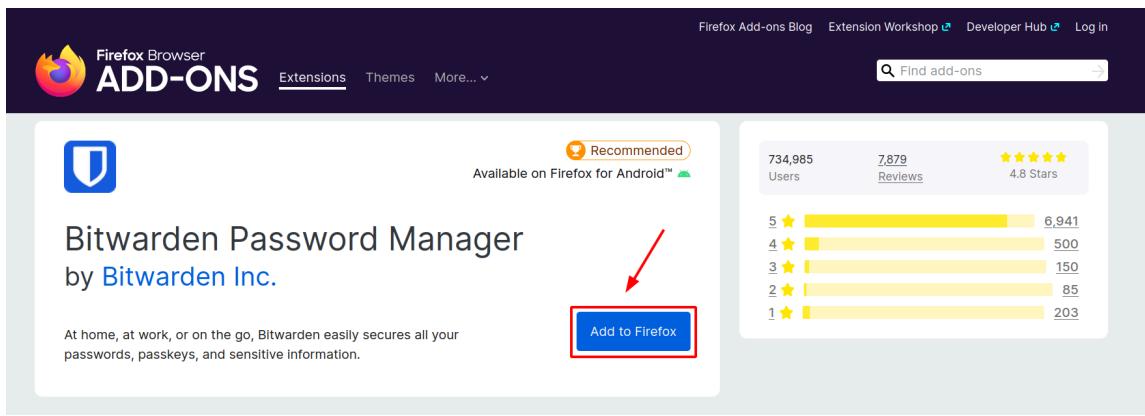
usar **Bitwarden** <<https://bitwarden.com/>> , uno de los gestores gratuitos más populares, para manejar de manera eficiente y segura nuestras credenciales.

- **Selección del gestor:** En nuestro caso, como hemos dicho, se ha elegido Bitwarden.
- **Instalación de la aplicación:** **Descarga Bitwarden** <<https://bitwarden.com/download/#downloads-web-browser>> desde su sitio web oficial o tiendas oficiales de aplicaciones y procede con la instalación. En este caso vamos a proceder a la instalación de la extensión del navegador.

Accede al apartado de descargas de la web oficial, busca tu navegador habitual, y haz clic en descargar:



- **Añade la extensión a tu navegador:** Al hacer clic en descargar, se nos abrirá una pantalla que nos da la opción de añadir la extensión a nuestro navegador.



- **Permisos:** En la esquina superior derecha se nos despliega una ventana donde la aplicación pide los permisos que necesita para realizar sus funciones.

#### 💡 ¿Añadir Bitwarden? Esta extensión tendrá permiso para:

- Acceder a sus datos de todos los sitios web
- Obtener datos del portapapeles
- Introducir datos en el portapapeles
- Acceder a las pestañas del navegador

[Saber más](#)

[Cancelar](#)

[Añadir](#)



Le damos a añadir y a continuación aceptamos. Si queremos que se ejecute también cuando usemos el navegador en modo incógnito, tenemos que marcar la casilla correspondiente.

#### 💡 Se ha añadido Bitwarden

Administre sus complementos y temas desde el menú de la aplicación.

Permitir que esta extensión se ejecute en ventanas privadas



[Aceptar](#)

- **Crear tu cuenta:** Ya tenemos la extensión instalada, ahora abre Bitwarden y regístrate. Lo más importante es definir una **contraseña maestra segura**; ésta será tu llave maestra.

Hacemos clic en la opción de crear cuenta:

The screenshot shows two side-by-side browser windows. On the left, the Bitwarden extension interface is displayed, showing a sign-up form with fields for email and password, and options to remember the email and continue. A red arrow points from the 'Crear cuenta' button in the extension's sign-up form to the 'Sign up for free now' button on the Bitwarden Browser Extension landing page. On the right, the Bitwarden Browser Extension landing page is shown, featuring the Bitwarden logo, navigation links for Personal, Business, Developers, and Download, and a large title 'Bitwarden Browser Extension'. Below the title, there is a brief description and two buttons: 'Sign up for free now' and 'Download options'.

Y cumplimentamos los datos que nos solicita:

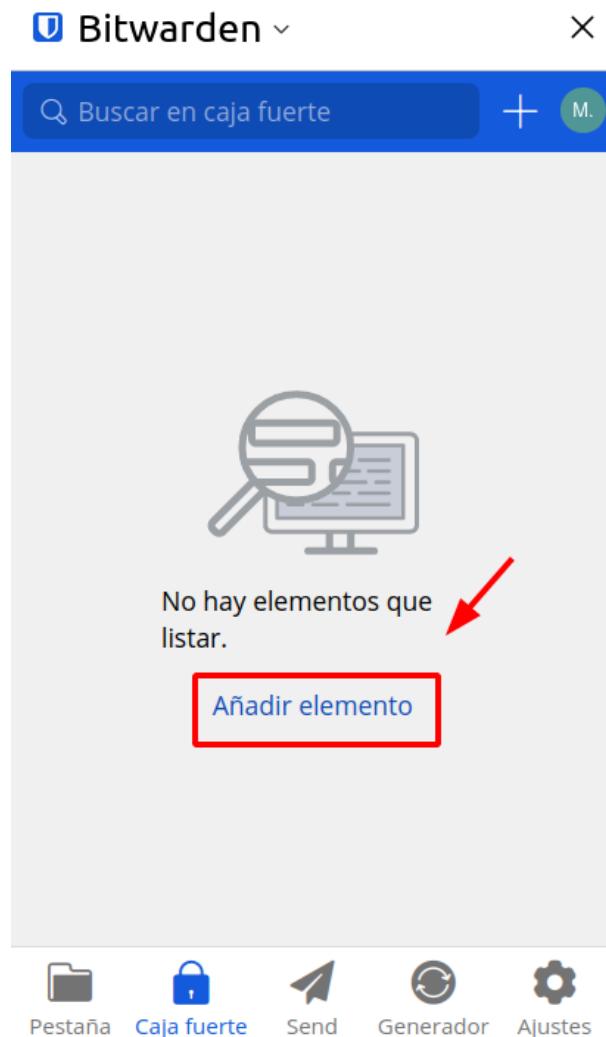
The screenshot shows two side-by-side browser windows. On the left, the 'Crear cuenta' (Create account) form is displayed. It includes fields for email and password, a note about the master password, and checkboxes for accepting terms and conditions and privacy policy. A red arrow points from the 'Enviar' (Send) button in the form to the 'Sign up for free now' button on the Bitwarden Browser Extension landing page. On the right, the Bitwarden Browser Extension landing page is shown, featuring the Bitwarden logo, navigation links for Personal, Business, Developers, and Download, and a large title 'Bitwarden Browser Extension'. Below the title, there is a brief description and two buttons: 'Sign up for free now' and 'Download options'.

Una vez registrados, ya podemos iniciar sesión en la aplicación y comenzar a trabajar con ella.

- **Agregar credenciales:** Puedes comenzar a introducir tus contraseñas en Bitwarden manualmente o dejar que capture las credenciales al iniciar

sesión en tus sitios web. Veamos como introducirlas manualmente.

En primer lugar, seleccionamos añadir elemento.



Cuando agregamos una nueva cuenta nos pide rellenar una serie de campos. Habitualmente, todos los gestores pedirán la URL o servicio para el que será utilizado, el nombre de usuario, la contraseña y algún comentario o nota que queramos añadir.

Bitwarden

Cancelar Añadir elemento Guardar

INFORMACIÓN DEL ELEMENTO

Tipo Entrada

Nombre Seneca

Usuario [REDACTED]

Contraseña   
[REDACTED]

Clave de autenticación (TOTP)

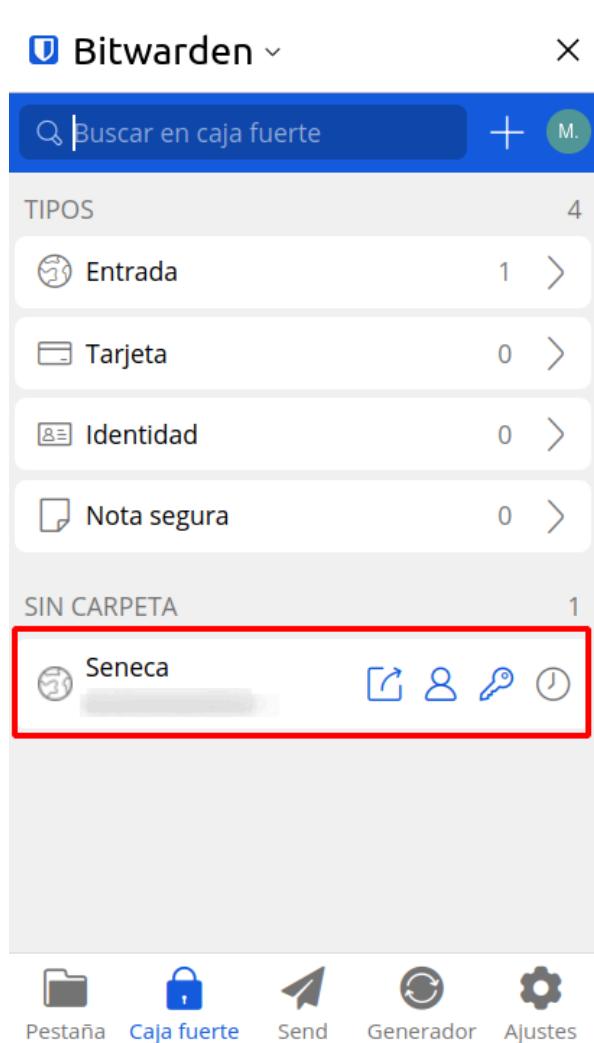
URI 1   
https://seneca.juntadeanda

+ Nueva URI

Completamos el formulario con los datos que nos solicita:



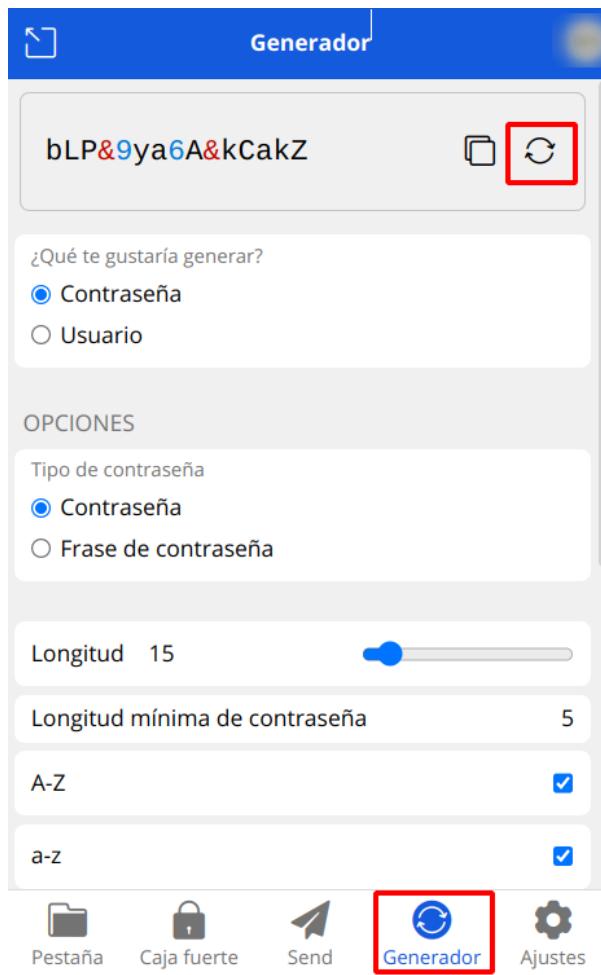
Ya tenemos las credenciales añadidas a nuestro gestor.



- **Probamos el gestor:** Si ahora accedemos al portal Séneca, veremos que Bitwarden nos está indicando que tiene guardadas las credenciales de esa aplicación.



- **Generar contraseñas seguras:** Podemos usar el generador de bitwarden para crear contraseñas fuertes para tus cuentas nuevas o existentes. Para ello, abrimos la extensión del navegador y en la parte inferior, hacemos clic en "Generador":



A partir de este momento, cuando nos registremos en una aplicación web o servicio, el gestor lo detectará y nos preguntará si queremos que guarde los datos.

*Nota: Se ha elegido Bitwarden para este ejemplo debido a que su versión gratuita permite la instalación en múltiples dispositivos, facilitando la gestión de contraseñas en ordenadores, teléfonos, tablets, etc. Sin embargo, existen otros gestores de contraseñas que también ofrecen funcionalidades similares y pueden ser igualmente efectivos. Te invitamos a explorar diferentes opciones disponibles en el mercado para encontrar la que mejor se adapte a tus necesidades.*

**Actividad (opcional):** Exploración y configuración de un gestor de contraseñas

**Descripción:** Investiga los diferentes gestores de contraseñas gratuitos disponibles, elige uno que se ajuste a tus necesidades y comienza a

organizar tus credenciales digitales.

#### Pasos:

1. Visita el enlace proporcionado por INCIBE para explorar las opciones de gestores de contraseñas gratuitos.
2. Elige un gestor de contraseñas que consideres adecuado para tus necesidades y que sea compatible con tus dispositivos.
3. Descarga e instala el gestor seleccionado.
4. Crea tu cuenta y establece una contraseña maestra segura y única.
5. Añade al menos tres contraseñas de sitios que frecuentes al gestor.
6. Reflexiona sobre cómo la elección de este gestor y la organización de tus contraseñas puede mejorar tu seguridad en línea.

#### Recursos necesarios:

- Acceso a la lista de gestores de contraseñas **recomendados por INCIBE** <[https://www.incibe.es/ciudadania/filtro/herramientas?tid=303607&tid\\_1>All&tid\\_2>All&tid\\_3>All](https://www.incibe.es/ciudadania/filtro/herramientas?tid=303607&tid_1>All&tid_2>All&tid_3>All)> .
- Conexión a internet.
- Dispositivo para instalar el gestor de contraseñas.



## Más allá de la contraseña

Aunque un gestor de contraseñas refuerza enormemente nuestra primera línea de defensa, la seguridad más robusta se logra mediante la adición de capas. Aquí es donde entra en juego la **autenticación de dos factores (2FA)**, añadiendo una capa adicional de seguridad que va más allá de la simple contraseña.

La 2FA exige no solo algo que sabes (tu contraseña), sino también algo que tienes (como un móvil o un token de seguridad). Este enfoque de seguridad por capas significa que, incluso si una contraseña es comprometida, el acceso no autorizado a tus cuentas puede ser significativamente más difícil.



En este apartado, desentrañaremos el funcionamiento de la 2FA y cómo implementarla efectivamente para proteger nuestras cuentas.

Imagen generada con IA (DALL-E) ([CC BY-NC-SA](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

## Objetivos:

- Comprender la importancia de la Autenticación de Dos Factores (2FA) como un método efectivo para añadir una capa adicional de seguridad a tus cuentas online.
- Aprender a activar y utilizar 2FA en distintas plataformas y servicios para fortalecer la protección contra accesos no autorizados.

## Lecturas recomendadas:

- **¿Qué es la Autenticación de Dos Factores y Dónde Debo Utilizarla?** <https://latam.kaspersky.com/blog/que-es-la-autenticacion-de-dos-factores-y-donde-debo-utilizarla/3270/> - Un artículo de Kaspersky que explora en profundidad qué es la 2FA, su necesidad y dónde implementarla para una seguridad optimizada.
- **¿Cómo funciona la autenticación en dos pasos (2FA)?** [https://www.avast.com/es-es/c-how-does-two-factor-authentication-work#:~:text=La%20autenticaci%C3%B3n%20de%20dos%20factores%20\(tambi%C3%A9n%20conocida%20como%202FA%20o,se%20a%C3%B1ade%20a%20la%20contrase%C3%B1a.](https://www.avast.com/es-es/c-how-does-two-factor-authentication-work#:~:text=La%20autenticaci%C3%B3n%20de%20dos%20factores%20(tambi%C3%A9n%20conocida%20como%202FA%20o,se%20a%C3%B1ade%20a%20la%20contrase%C3%B1a.) - Avast detalla el

funcionamiento de la 2FA, por qué es crucial para la seguridad online y cómo puede implementarse para proteger tus datos personales.

La **autenticación de dos factores (2FA)**, también conocida como verificación en dos pasos, es una capa de seguridad que se suma a la tradicional contraseña para proteger el acceso a tus cuentas online. Esta metodología se basa en dos etapas o factores de verificación:

1. **Primer factor:** Algo que conoces, por ejemplo tu contraseña habitual o un código PIN.
2. **Segundo factor:** Algo que posees, por ejemplo, un teléfono móvil, una llave física USB, o incluso una aplicación que genere códigos únicos temporales, conocidos como OTP (One-Time Password).

Implementar 2FA complica significativamente cualquier intento de acceso no autorizado. Incluso si un atacante consigue tu contraseña, necesitaría también el segundo factor, algo físicamente en tu posesión, para acceder a tu cuenta.

Es muy recomendable activar el 2FA en todas tus cuentas online que lo soporten, como el correo electrónico, redes sociales, servicios de mensajería, banca online, y cualquier otro servicio que almacene datos sensibles.

Podríamos establecer los siguientes como unos pasos genéricos:

1. **Inicia sesión** en tu cuenta con tus credenciales habituales.
2. **Busca la opción de seguridad** dentro de los ajustes o configuración de la cuenta, usualmente en un apartado relacionado con la seguridad.
3. **Activa la verificación en dos pasos**, seleccionando la opción correspondiente para habilitar 2FA.
4. **Elige tu segundo factor** de autenticación, que puede variar desde un mensaje de texto, un correo electrónico, hasta una aplicación generadora de códigos.
5. **Sigue los pasos** para completar la activación, que pueden incluir la verificación de tu dispositivo o correo electrónico.
6. **Guarda códigos de respaldo** en un lugar seguro, si el servicio los proporciona, para casos de emergencia.

El procedimiento exacto puede variar ligeramente según el servicio, por lo que es recomendable consultar las instrucciones específicas de cada plataforma para la activación de la 2FA.

- **Android:** Activar la verificación en dos pasos.  
[https://support.google.com/accounts/answer/185839?  
hl=es&co=GENIE.Platform%3DAndroid](https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DAndroid)
- **iOS:** Autenticación de doble factor para el ID de Apple.  
<https://support.apple.com/es-es/HT204915#:~:text=En%20el%20iPhone%2C%20iPad%20o,sigue%20las%20instrucciones%20en%20pantalla.>

- **Instagram:** Proteger tu cuenta de Instagram con la autenticación en dos pasos. [<https://es-es.facebook.com/help/instagram/566810106808145>](https://es-es.facebook.com/help/instagram/566810106808145)
- **Facebook:** Cómo funciona la autenticación en dos pasos en Facebook. [<https://es-la.facebook.com/help/148233965247823>](https://es-la.facebook.com/help/148233965247823)
- **TikTok:** Activa la verificación en dos pasos. [<https://support.tiktok.com/es/safety-hc/account-and-user-safety/account-safety>](https://support.tiktok.com/es/safety-hc/account-and-user-safety/account-safety)
- **Twitter (X):** Cómo usar la autenticación de dos factores. [<https://help.twitter.com/es/managing-your-account/two-factor-authentication>](https://help.twitter.com/es/managing-your-account/two-factor-authentication)
- **LinkedIn:** Activar y desactivar la verificación en dos pasos. [<https://www.linkedin.com/help/linkedin/answer/a1380089/activar-y-desactivar-la-verificacion-en-dos-pasos?lang=en-us&intendedLocale=es#:~:text=Toca%20tu%20foto%20de%20perfil,y%20haz%20clic%20en%20Continuar.>](https://www.linkedin.com/help/linkedin/answer/a1380089/activar-y-desactivar-la-verificacion-en-dos-pasos?lang=en-us&intendedLocale=es#:~:text=Toca%20tu%20foto%20de%20perfil,y%20haz%20clic%20en%20Continuar.>)
- **YouTube:** Activar la verificación en dos pasos. [<https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DDesktop>](https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DDesktop)

- **Gmail:** Activar la verificación en dos pasos. <https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DDesktop>
- **Outlook:** Cómo utilizar la verificación en dos pasos con su cuenta de Microsoft. <https://support.microsoft.com/es-es/account-billing/c%C3%B3mo-utilizar-la-verificaci%C3%B3n-en-dos-pasos-con-su-cuenta-de-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4>
- **Yahoo!:** Verificación en dos pasos con una llave de seguridad. <https://es-us/ayuda.yahoo.com/kb/account/Verificaci%C3%B3n-en--pasos-con-una-Clave-de-seguridad-sln35380.html?guccounter=2>

- **WhatsApp:** Cómo administrar los ajustes de la verificación en dos pasos. <https://faq.whatsapp.com/1920866721452534/>
- **Telegram:** ¿Cómo funciona la verificación en dos pasos? <https://telegram.org/faq/es#:~:text=Puedes%20hacerlo%20en%20Ajustes%20%3E%20Privacidad,seguridad%20%3E%20Verificaci%C3%B3n%20en%20dos%20pasos.>

- **Google Drive:** Activar la verificación en dos pasos.  
<https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DDesktop>
- **Dropbox:** Cómo activar y desactivar la verificación en dos pasos.  
<https://help.dropbox.com/es-es/account-access/enable-two-step-verification>
- **iCloud:** Activar la autenticación de doble factor para el ID de Apple.  
<https://support.apple.com/es-es/HT204915#:~:text=Activar%20la%20autenticaci%C3%B3n%20de%20doble%20factor%20para%20el%20ID%20de%20Apple&text=En%20el%20iPhone%2C%20iPad%20o,sigue%20las%20instrucciones%20en%20pantalla.>

- **Amazon:** ¿Qué es la verificación en dos pasos?  
<https://www.amazon.es/gp/help/customer/display.html?nodeId=G3PWZPU52FKN7PW4>
- **eBay:** Nueva verificación en dos pasos de eBay.  
<https://comunidad.ebay.es/t5/%C3%9Altimas-noticias/Nueva-verificaci%C3%B3n-en-dos-pasos-de-eBay/ba-p/392613#:~:text=Inicia%20sesi%C3%B3n%20en%20tu%20cuenta,Activa%20%22Verificaci%C3%B3n%20de%20eBay%22.>

**Actividad (opcional):** Fortaleciendo mi seguridad en redes

**Descripción:** Evalúa la fortaleza y seguridad de tus contraseñas actuales y activa 2FA en al menos tres de tus cuentas importantes.

1. Selecciona tres servicios online que utilices frecuentemente.
2. Para cada servicio, verifica si utilizas 2FA. Si no es así, activa la opción siguiendo las instrucciones del servicio.

### Recursos necesarios:

- Acceso a internet.
- Dispositivo con acceso a un navegador web.



## Recursos educativos



Imagen generada con IA (DALL-E) ([CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es))

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para promover el **uso de contraseñas seguras** entre nuestros

estudiantes.

- **Mejora tus contraseñas:** Juego de mesa para aprender a crear contraseñas fuertes y seguras. Descargar el juego <[https://www.incibe.es/sites/default/files/docs/c3\\_pdf\\_rp\\_mejora\\_tus\\_contraseñas.pdf](https://www.incibe.es/sites/default/files/docs/c3_pdf_rp_mejora_tus_contraseñas.pdf)> .
  - **Infografía sobre como crear una contraseña robusta:** Una guía enfocada en cómo construir contraseñas seguras y difíciles de descifrar. Ver guía <[https://www.incibe.es/sites/default/files/docs/osi-crear\\_contrasena-robusta.pdf](https://www.incibe.es/sites/default/files/docs/osi-crear_contrasena-robusta.pdf)> .
- 

Obra publicada con Licencia Creative Commons Reconocimiento No comercial Compartir igual 4.0 <<http://creativecommons.org/licenses/by-nc-sa/4.0/>>

# Módulo 1. Protege tu espacio digital

## 1.4 Actividades obligatorias

### Manual de supervivencia de ciberseguridad



Imagen generada con IA (DALL-E) (CC BY-NC-SA  
<http://creativecommons.org/licenses/?lang=es> )





El **objetivo** final del curso es que, al concluirlo, no solo hayas absorbido información valiosa, sino que también hayas comenzado a **construir hábitos sólidos de ciberseguridad** que perdurarán mucho más allá de este curso. Tu **guía de supervivencia de ciberseguridad** será un recurso esencial que podrás consultar y actualizar continuamente, reflejando tu evolución y comprensión del complejo mundo de la seguridad en internet.

Para comenzar y establecer un fundamento sólido para tu aprendizaje, en estas actividades te animamos a enfocarte en la **creación del documento**. Esta guía será tu compañera a lo largo de todo el curso, un documento vivo donde irás anotando y reflexionando sobre las medidas de seguridad más relevantes para tu entorno digital.



## Actividad 1.1: Manual de supervivencia de ciberseguridad I

**Descripción:** Esta actividad está diseñada para ayudarte a comenzar tu manual personal de ciberseguridad, incorporando las medidas de seguridad más relevantes para ti.

### Pasos:

- **Selección de medidas de seguridad:**

- Revisa los contenidos del Módulo 1 y elige las medidas de seguridad, estrategias y herramientas que consideres más relevantes para tu entorno digital.
- Justifica por qué has seleccionado cada medida y cómo se aplican a tus necesidades específicas.
- Añade a tu manual una sección que contenga una lista de las medidas seleccionadas con una breve descripción de cada una y los recursos necesarios para su implementación. Esta sección servirá como referencia rápida de las estrategias de seguridad que has considerado importantes.

- **Implementación de medidas de seguridad:**

- De las medidas seleccionadas, implementa al menos una en tu entorno digital actual.
- Describe el proceso de implementación y cómo has aplicado la medida, incluyendo cualquier dificultad que hayas encontrado y cómo la superaste.

- **Estado de madurez de mi seguridad digital:**

- Añade a tu manual una nueva sección que liste las medidas de seguridad que ya has aplicado y las que están pendientes de implementación.
- Reflexiona sobre tu estado actual de seguridad digital y justifica tus decisiones y planes futuros para mejorar tu seguridad.

### Recursos necesarios:

- Procesador de texto (Word, Google Docs, etc.).
- Acceso a los contenidos del Módulo 1.
- Herramientas y recursos de ciberseguridad mencionados en el módulo.
- Plantilla proporcionada en el aula virtual del curso.

**Formato y entrega de la actividad:** La actividad debe ser entregada en formato PDF a través del enlace habilitado en el aula virtual del curso.

*Nota: Asegúrate de que cada sección de tu manual esté claramente identificada y desarrollada según las instrucciones dadas.*

#### *Rúbrica de la actividad 1.1 **Aplicar***

	<b>Nivel Alto</b>	<b>Nivel Medio</b>	<b>Nivel Básico</b>
<b>Selección de medidas de seguridad (2,5 pts)</b>	Se han identificado y seleccionado las estrategias y herramientas de manera completa y detallada, justificando claramente su relevancia y aplicación. (2.5)	Se han identificado y seleccionado estrategias y herramientas de manera adecuada, aunque las justificaciones son poco detalladas. (1.25)	No se ha incluido la sección. (0)
<b>Implementación de una medida de seguridad</b>	Se describe detalladamente la implementación de una medida, incluyendo las dificultades encontradas y cómo se superaron, reflejando un entendimiento profundo del proceso. (2.5)	La descripción de la implementación es adecuada, pero carece de detalles sobre las dificultades encontradas o posibles soluciones. (1.25)	No se ha incluido la sección o no se ha descrito la implementación de una medida. (0)
<b>Estado de madurez de mi seguridad digital (2,5 pts)</b>	Se ha incluido una sección detallada que refleja un análisis completo y una comprensión de la seguridad personal, mostrando claramente las medidas aplicadas y pendientes. (2.5)	La sección incluida muestra una comprensión adecuada de la seguridad personal, pero el análisis es superficial y necesita mayor profundidad. (1.25)	No se ha incluido la sección. (0)
<b>Elaboración del manual (2,5 pts)</b>	El manual incluye descripciones claras y	El manual incluye descripciones y	No se ha elaborado el documento. (0)

	Nivel Alto	Nivel Medio	Nivel Básico
	recursos necesarios bien definidos. (2.5)	recursos, pero no están completamente claros o son incompletos. (1.25)	



## Actividad 1.2: Reflexión colaborativa sobre medidas de seguridad

**Descripción:** El propósito de esta tarea es fomentar la **reflexión colaborativa** sobre las medidas de seguridad propuestas en el módulo. Para ello, debes compartir tus experiencias en la **implementación** de alguna de las **medidas de seguridad** presentadas en el módulo 1 y reflexionar sobre su efectividad en tu entorno digital. Además, se espera que comentes las contribuciones de tus compañeras y compañeros, ofreciendo tu perspectiva y posibles alternativas de uso. Asegúrate de responder al menos a una entrada del foro para promover la interacción y el intercambio de ideas en el foro.

Considera enriquecer tus comentarios con preguntas estimulantes para promover una discusión más profunda y significativa.

### Recursos necesarios:

- Acceso al foro del curso para la participación.

### Formato y entrega de la actividad:

- Foro del módulo.

### Rúbrica de la actividad 1.2 *Aplicar*

	Nivel Alto	Nivel Medio	Nivel Bajo
<b>Participación activa en el foro (2,5 pts)</b>	Se han compartido experiencias de manera detallada y constructiva, promoviendo la discusión. (2.5)	Se han compartido experiencias, pero de manera general o sin profundizar. (1.25)	No se han compartido experiencias en el foro. (0)
<b>Reflexión sobre medidas</b>	Se ha demostrado una reflexión	Se ha mostrado una reflexión básica sobre	No se han compartido reflexiones sobre las

	Nivel Alto	Nivel Medio	Nivel Bajo
implementadas (2,5 pts)	profunda sobre las medidas implementadas, destacando su importancia. (2.5)	las medidas implementadas, sin detalles específicos. (1.25)	medidas implementadas. (0)
Colaboración y apoyo a compañeras y compañeros (2,5 pts)	Se ha ofrecido apoyo constructivo y colaborativo a las reflexiones de las compañeras y compañeros. (2.5)	Se ha ofrecido apoyo a las compañeras y compañeros, pero de manera limitada o superficial. (1.25)	No se ha ofrecido apoyo ni colaboración a las compañeras y compañeros. (0)
Propuestas alternativas de medidas de seguridad de compañeras y compañeros (2,5 pts)	Se han presentado alternativas aplicables y bien fundamentadas a las medidas de seguridad, demostrando una comprensión profunda. (2.5)	Se han planteado alternativas a las medidas de seguridad; no obstante, estas requieren de un desarrollo más amplio o ejemplos que demuestren su aplicabilidad. (1.25)	No se han propuesto alternativas aplicables, sin aportar significativamente a la discusión sobre seguridad. (0)

Obra publicada con Licencia Creative Commons Reconocimiento No comercial Compartir igual 4.0  
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

# Módulo 1. Protege tu espacio digital

## Otros formatos y autoría

---



### Autoría

---

Título	Módulo 1 del curso "La Ciberseguridad en el ámbito educativo"
Descripción	<p>Este módulo "<b>Protege tu espacio digital</b>", está diseñado para dotarte de las herramientas y el conocimiento clave para fortalecer la seguridad de tu espacio digital. A lo largo de este módulo, aprenderás sobre la importancia de proteger tu privacidad, cómo crear y manejar contraseñas robustas y las estrategias para proteger tu información personal tanto en dispositivos móviles como en ordenadores.</p>
Autor	Manuel Jesús Rivas Sánchez <a href="https://twitter.com/0xmrvias">https://twitter.com/0xmrvias</a>
Licencia	Creative Commons BY-NC-SA 4.0 <a href="https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es">https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es</a>





## Versión imprimible PDF

---

Este material está diseñado para ser leido y trabajado de manera interactiva en un ordenador, pero si quieres puedes descargártelo en [este enlace](https://raw.githubusercontent.com/0xmrvias/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo1.pdf) en formato pdf.



---

Obra publicada con Licencia Creative Commons Reconocimiento No comercial Compartir igual 4.0 <<http://creativecommons.org/licenses/by-nc-sa/4.0/>>