Dispositivos

Muchas pueden ser las actuaciones que en materia de seguridad se pueden aplicar en nuestros dispositivos digitales, a continuación se enumeran los más imprescindibles.

1.-Proteger el acceso a los dispositivos con contraseñas robustas

Para crear una **CONTRASEÑA** robusta tendremos en cuenta:

- Que tenga como **mínimo 12 caracteres**. Por ejemplo: cuentasegura
- Alternar **mayúsculas** y **minúsculas**. Ej: CuentaSegura
- Sustituir **letras por números** (a=1, e=2). : Ej: Cu2nt1s2gur1
- Añadir **caracteres especiales**. Ej: Cu2nt1s2gur1!
- **Personalizar** la contraseña para **cada servicio,** una para el inicio de sesión de un dispositivo y otra para el el correo electrónico, poniendo las iniciales en mayúsculas al principio y al final. Ej del correo electrónico: CCu2nt1s2gur1!E

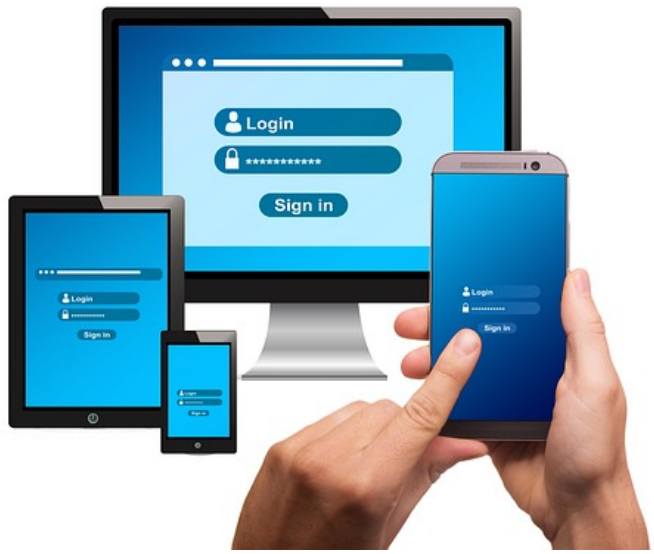


Imagen de Gerd Altmann en Pixabay

Y como medidas extra:

- **No las compartas** con nadie (ni amigos, ni familiares)
- Configurarlo de tal forma **que no se vean tus carácteres cuando los escribas**
- **Cámbialas cada cierto tiempo** (3 meses)
- **No repitas contraseñas en diferentes servicios** (@ corporativo, @ personal, RRSS,...)
- Si es posible configura la **verificación en dos pasos**
- Utiliza **gestores de contraseñas** para controlar todas tus claves. Si quieres conocer diferentes gestores de contraseñas gratuitos pulsa aquí.

> A continuación os proponemos dos propuestas para generar contraseñas de forma lúdica: "Mejora tus contraseñas". Construye contraseñas seguras jugando desarrollado por el Incibe y "Space Shelter": un juego para aprender a incrementar tu seguridad en Internet desarrollado por Google

2.- Importancia de las actualizaciones

Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad. Así, se corregirán las vulnerabilidades descubiertas y se contará con las últimas funciones implementadas por los desarrolladores.

Por tanto, si queremos mantener la seguridad de nuestros dispositivos, debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de **actualizaciones automáticas** siempre que esté disponible.
- Instalar las actualizaciones **tan pronto como se publiquen**, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser **cuidadosos con las aplicaciones que instalamos**, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar usar aplicaciones y sistemas antiguos que ya no dispongan de actualizaciones de seguridad.
- Es recomendable no congelar los dispositivos ya que no es posible que se efectuen las actualizaciones de seguridad tando de los sistemas operativos como de las aplicaciones.

Copyright 2026



Fuente Incibe

Es importante no confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Windows 10, a pesar de no tratarse de la última versión de este sistema operativo. Los fabricantes no solo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones.

> En los siguientes enlaces encontrarás una recopilación de los sistemas, navegadores y programas más conocidos, que nos facilitarán la **actualización** de nuestros dispositivos:
>
> Cómo actualizar el **sistema operativo**, cómo actualizar los **navegadores**, cómo actualizar los **programas y aplicaciones**

Debemos huir de sitios “pirata”, especialmente de aquellos que ofrecen aplicaciones o servicios gratuitos o extremadamente baratos, por lo tanto instalemos **aplicaciones solo de fuentes de confianza y revisemos siempre los privilegios**, por si fuesen excesivos o innecesarios para el propósito al que están destinados.

3.- Cifrado de datos vulnerables.

El cifrado implica convertir texto con formato legible por humanos en un texto incomprensible, conocido como texto cifrado. En esencia, esto significa tomar datos legibles y cambiarlos para que se vean como algo aleatorio.

El cifrado implica utilizar una clave criptográfica. Podemos distinguir entre datos en transito y en reposo.

- **Cifrado de datos en tránsito** es cuando se mueven entre dispositivos, como es el caso entre redes privadas o por Interne, durante la trasferencia, los datos (cuando enviamos un Whatsapp, compra on-line,...) se encuentran en mayor riesgo debido a la necesidad de descifrar antes de transferir y a las vulnerabilidades del propio método de transferencia. Cifrar los datos durante la transferencia, conocido como cifrado integral, garantiza la protección de la privacidad de los datos, incluso si los interceptan.
- **Cifrado de datos en reposo** es cuando permanecen en un dispositivo de almacenamiento y no se usan o transfieren activamente. A menudo, los datos en reposo son menos vulnerables que los en tránsito debido a que las funciones de seguridad del dispositivo restringen el acceso. Cifrar los datos en reposo reduce las oportunidades para el robo de datos que propician los dispositivos perdidos o robados, o bien por compartir contraseñas u otorgar permisos por accidente

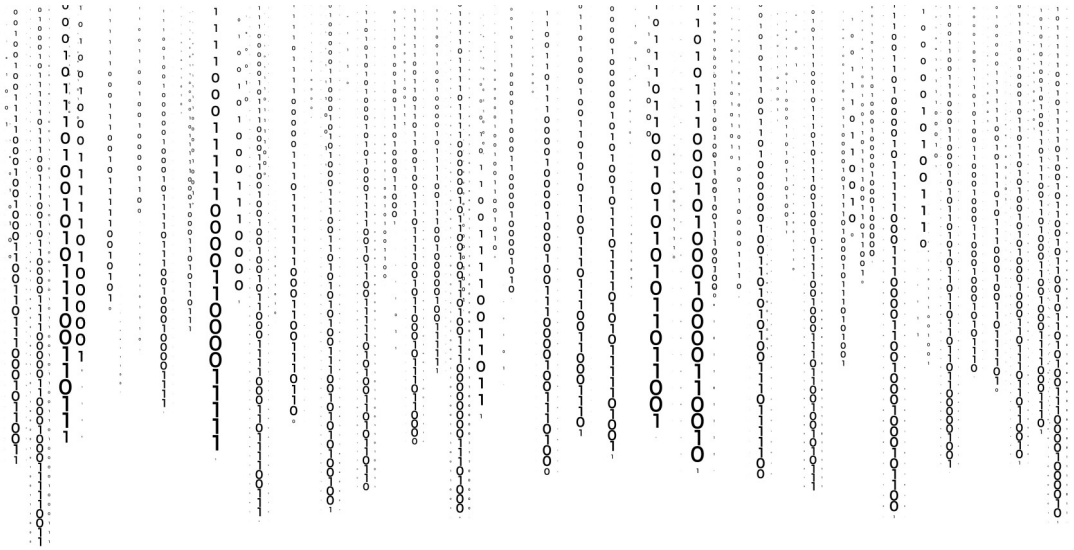


Image by vectorjuice on Freepik

> Si quieres herramientas para el cifrado de datos pulsa en el siguiente enlace

Copyright 2026

4.- Antivirus activado y actualizado

Es fundamental tener el antivirus activado y actualizado para proteger los dispositivos de las distintas amenazas que circulan por Internet. Recordemos que un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), pero para poder hacer su misión **debe estar activado**. Obviamente, no sirve [illegible] no está activo.



Image by vectorjuice on Freepik

Pero aún hay más, también es necesario que el **antivirus esté actualizado**. La explicación a esto es muy sencilla. Cuando instalamos un antivirus en el dispositivo, éste es capaz de detectar los virus existentes hasta ese momento. Es importante saber que los fabricantes de antivirus, a través del servicio de actualizaciones, lo que hacen es añadir a su base de datos, todos los nuevos virus que se descubren. Por tanto, si el usuario no actualiza la herramienta, los últimos virus podrán "colarse" en los dispositivos.

> Si quieres poder elegir entre diferentes antivirus y cleaners gratuitos puedes pulsar en el siguiente enlace

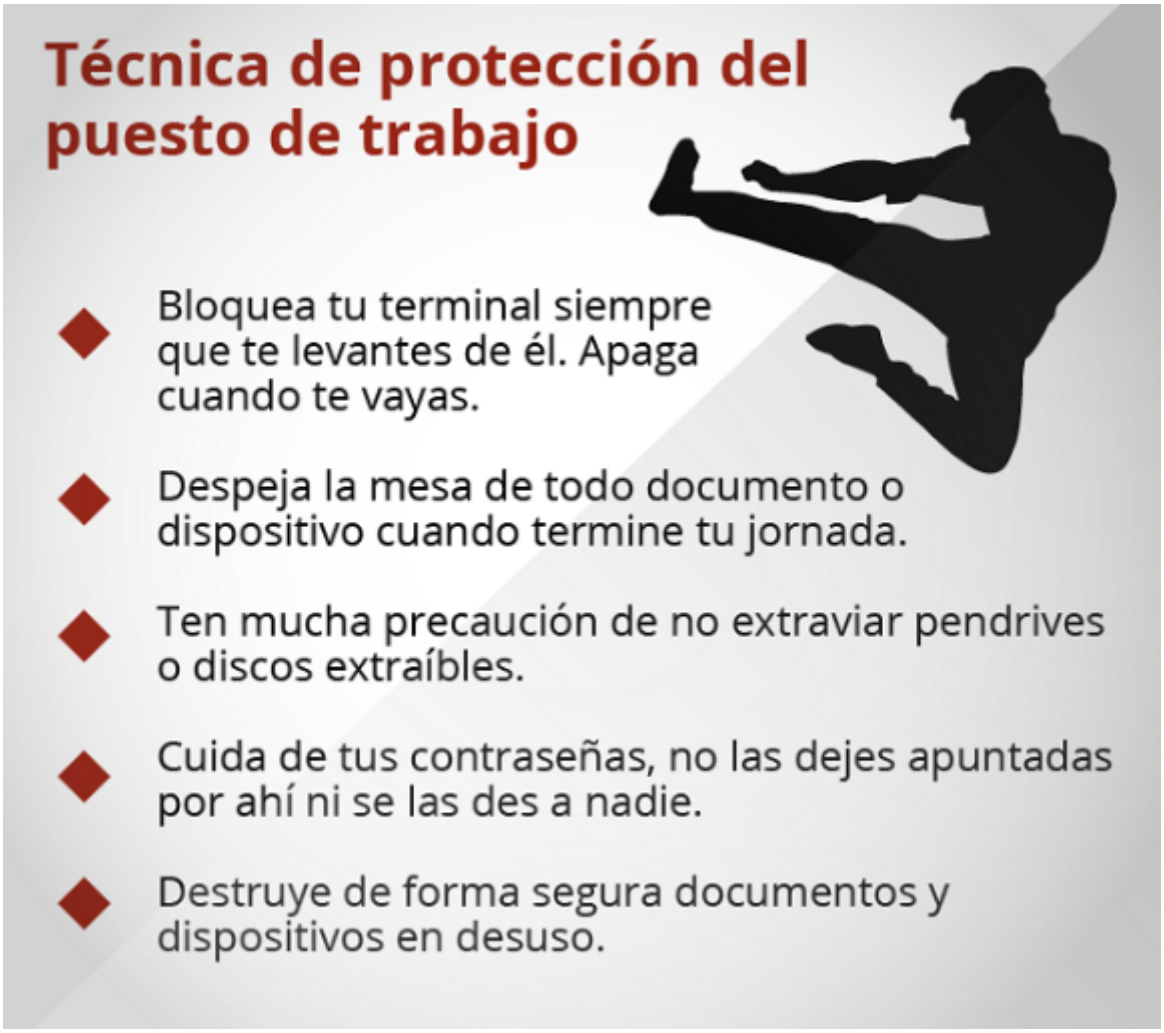
5. Configura el bloqueo automático del equipo cuando estás ausente o entra en reposo.

Cuando te levantes para descansar o no vayas a utilizar el ordenador en un rato, es importante bloquearlo, para que otras personas no tengan acceso a él. Los siguientes casos, son ejemplos de cuándo se bloquea el equipo:

- Dejar de teclear y usar el ratón por un tiempo definido según los ajustes.
- Tener un ordenador portátil y cerrar la tapa.
- Se bloquea manualmente.

Por ejemplo en los sistema Windows podemos hacerlo de diferentes formas:

- Desde el menú '**Inicio**', haz clic encima de tu nombre de usuario y luego en '**Bloquear**'.
- Usando el atajo de teclado **Windows + L** desde cualquier pantalla.
- Para portátiles, configura la suspensión cuando se cierra la tapa. Abre el menú '**Inicio**' y escribe '**Panel de control**'. Ábrelo y ve a '**Hardware y sonido**' > '**Opciones de energía**', y en esta ventana haz clic en '**Elegir el comportamiento del cierre de la tapa**' en la izquierda de la pantalla. Ahora configura las dos opciones marcadas en la imagen en '**Suspender**'.



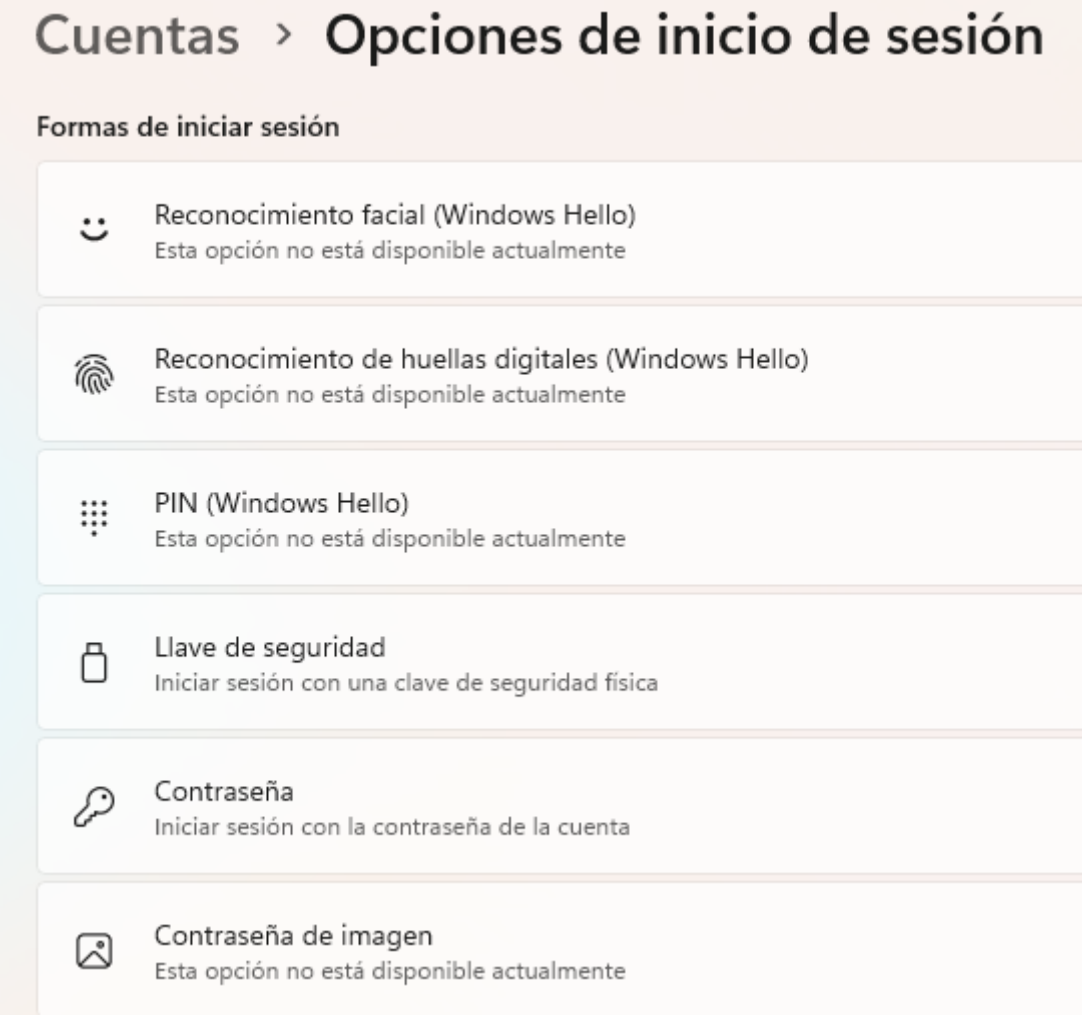
Fuente Incibe

6.- Incorpora mecanismos seguros de desbloqueo

Hoy en día, tanto los teléfonos móviles, tablets como los ordenadores disponen de algún mecanismo para evitar que cualquier usuario pueda hacer uso de nuestro dispositivo, una de las primeras configuraciones de seguridad que realizamos cuando encendemos nuestro equipo es el **bloqueo de acceso**, ya sea mediante un PIN, un patrón o una clave de seguridad.

En los **ordenadores** existen varias opciones, aunque su disponibilidad dependerá del tipo de ordenador y de si tenemos permisos de administrador, las más comunes (en Windows) son:

- **Rostro de Windows Hello**: podremos utilizar nuestro rostro para bloquear/desbloquear nuestro equipo.
- **Huella digital de Windows** Hello: en este caso, utilizaremos nuestra huella dactilar.
- **PIN de Windows Hello**: podremos escoger un código PIN (clave numérica de al menos 4 caracteres), aunque es la opción menos segura.
- **Clave de seguridad**: se trata de una clave física, que se instala dentro de un dispositivo, como una memoria USB, y que necesitamos conectar al equipo para iniciar sesión.
- **Contraseña**: podremos cambiar la contraseña que creamos junto con la cuenta de usuario, es decir, la que utilizamos para desbloquear el ordenador.



Fuente propia

Por otro lado los dispositivos móviles (***smartphones o tablets***) cuentan también con una herramienta muy importante que es el sistema de bloqueo, una gran variedad de dispositivos utilizan el sistema de Android y la configuración del bloqueo de pantalla es el siguiente:

- **Patrón**: consiste en un dibujo trazado uniendo una serie de nueve puntos en forma de un cuadrado de 3x3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla.
- **PIN**: se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.
- **Contraseña**: se trata de una clave de al menos 4 dígitos y letras. Debemos utilizar una contraseña difícil de averiguar y única para el dispositivo.
- Desbloqueo con **huella dactilar**: nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o tablet simplemente poniendo el dedo sobre el lector de la huella.
- Desbloqueo **facial**: nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.
- Desbloquear con dispositivo **Bluetooth**: podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o tablet, como una pulsera de actividad o reloj inteligente.

7. Instalar únicamente las aplicaciones necesarias, revisando privacidad y permisos

Tener muy claras las aplicaciones que vamos a utilizar y con que fines configurando convenientemente la privacidad y permisos que les damos a las mismas. Es conveniente actualizarlas desde los sitios oficiales y si ya no las utilizamos sería conveniente eliminarlas, pues pueden llegar a ser puertas de entrada de potenciales riesgos de nuestros dispositivos.

Copyright 2026



Imagen de edsys en Pixabay

Los **centros educativos tienen que analizar y consensuar las relación de aplicaciones** más adecuadas en el proceso de enseñanza y aprendizaje del alumnado en función del nivel educativo en el que se encuentren.

Un posible modelo de plantilla, donde ir rellenando las medidas en materia de seguridad adoptadas en los dispositivos podría comenzar así.

DISPOSITIVOS

- Las contraseñas de los diferentes dispositivos del centro deberían tener como mínimo 12 caracteres; alternar mayúsculas y minúsculas; letras y números; caracteres especiales; cambiarlas cada cierto tiempo (3 meses).
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Tener el antivirus activado y actualizado.
- ...

Revision #45
Created 2023-02-01 19:43:56 CET by Javier
Updated 2023-02-23 23:37:00 CET by Javier Gerico

Copyright 2026