Seguridad Digital

Documentación y datos digitales

En el **centro educativo** podemos tener múltiples aspectos que se pueden convertir en amenazas a la hora de tener **brechas de seguridad** que afectan de forma sensible al correcto funcionamiento del centro, nos pueden llegar desde los propios miembros que conformamos la comunidad educativa, programas maliciosos, errores en la programación y posibles accidentes que pueden acontecer.

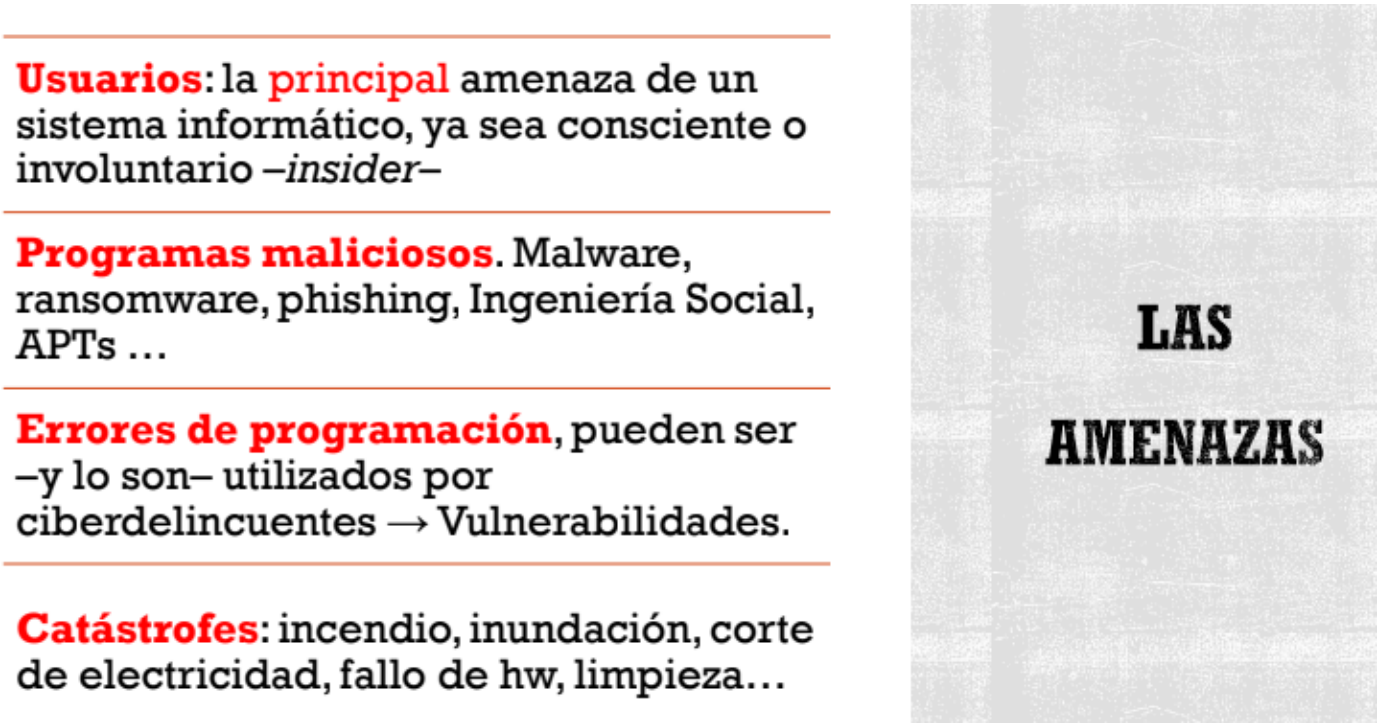


Imagen de Pedro González experto en Ciberseguridad

Si la amenaza se convierte en un ataque, la forma inmediata de detenerlo sería:

- **Desconexión del dispositivo de la red**
- **¿Apagarlo?**
- **Desconexión del router y switches del centro**
- **Llamar a soporte**

Por lo tanto en los centros educativos velaremos porque la información y los datos estén custodiados de forma segura y aplicaremos **medidas activas y pasivas** en lo concerniente a la **seguridad:**

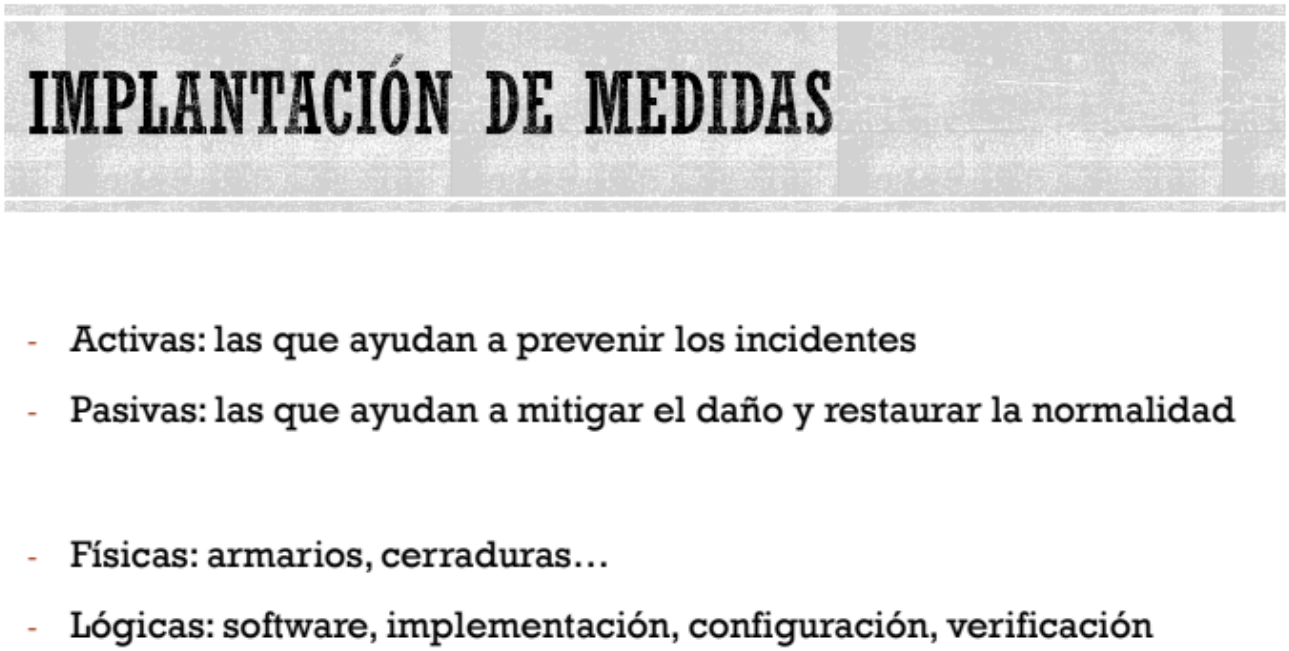


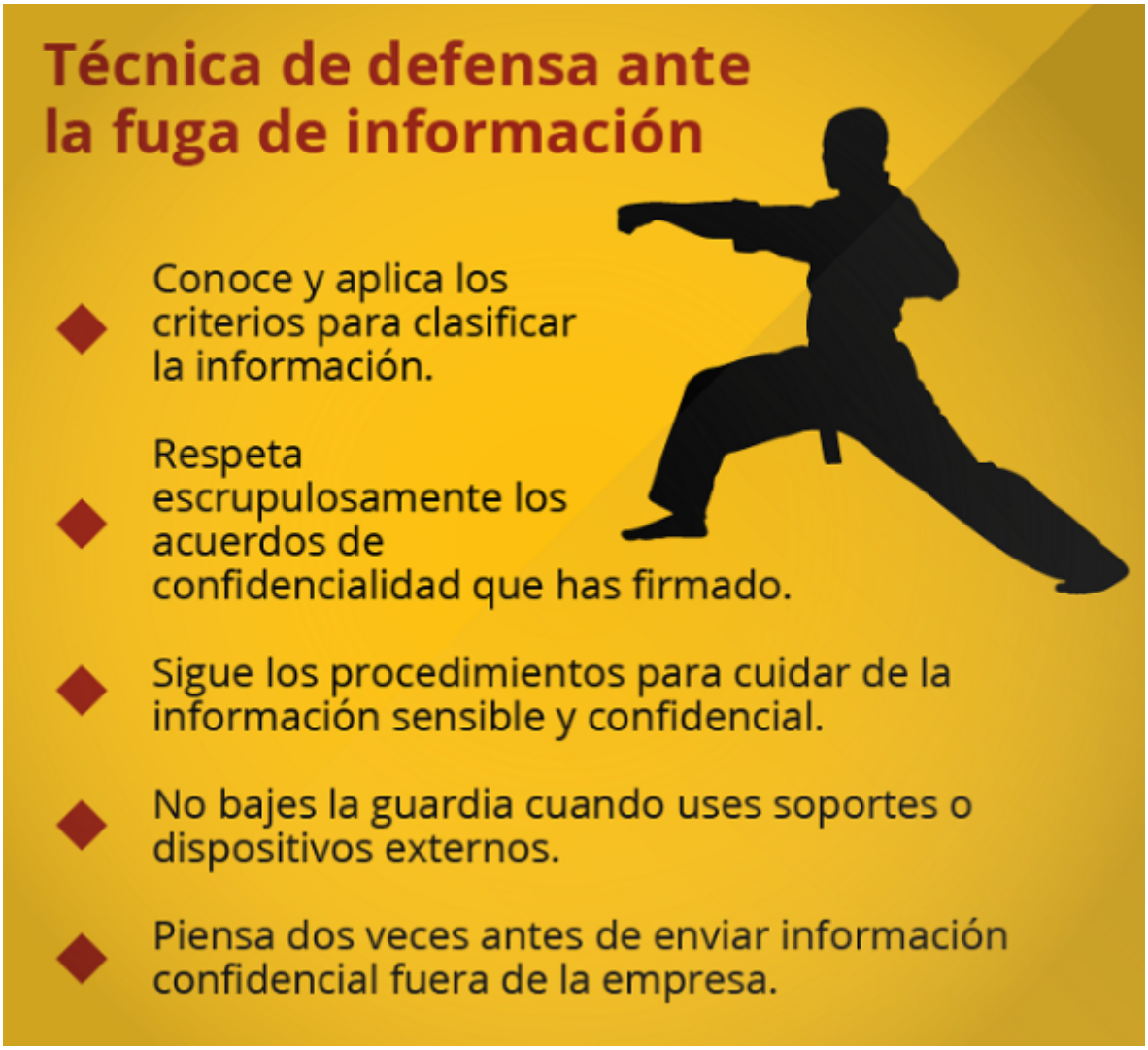
Imagen de Pedro González, experto en Ciberseguridad

Papeles y datos digitales

- La información digital ocupa menos espacio, pero depende de la vida útil del soporte donde esté almacenada. Los papeles suelen durar más tiempo y, en muchos casos, es necesario conservar los **originales**, sobre todo en documentación que legalmente debemos conservar durante un tiempo determinado, o **documentos firmados**. Para ambos tipos de soporte, lo fundamental es que los almacenemos de forma segura y ordenada, y que las condiciones sean las adecuadas para que no se deterioren.

Imagen de Freepik

- El **centro educativo fijará qué dispositivos pueden utilizarse y controlarlos**. Por ello antes de usar ningún dispositivo personal como pendrives o discos externos o nuestros servicios en la nube personales (Dropbox, Google Drive, etc.), tendremos que preguntar al responsable, siendo recomendable el uso de los **servicios en la nube del centro**. Su uso indiscriminado puede dar lugar a riesgos importantes y a fugas de información.



Fuente Incibe

- Debemos asegurarnos que los soportes dónde guardamos la información se encuentran en buen estado y así no arriesgarnos a perder dicha información. Cuando seleccionamos un dispositivo de almacenamiento tenemos que conocer su vida útil para sustituirlo a tiempo y no perder la información que contiene.
- Las **condiciones del entorno** de los soportes donde guardamos la información resultan tan importantes como la seguridad de la información misma. Debemos procurar que se den las condiciones físicas (humedad, temperatura, etc.) adecuadas para que el soporte no se deteriore. También es importante que no esté al alcance de cualquiera y si es extraíble de no perderlo.

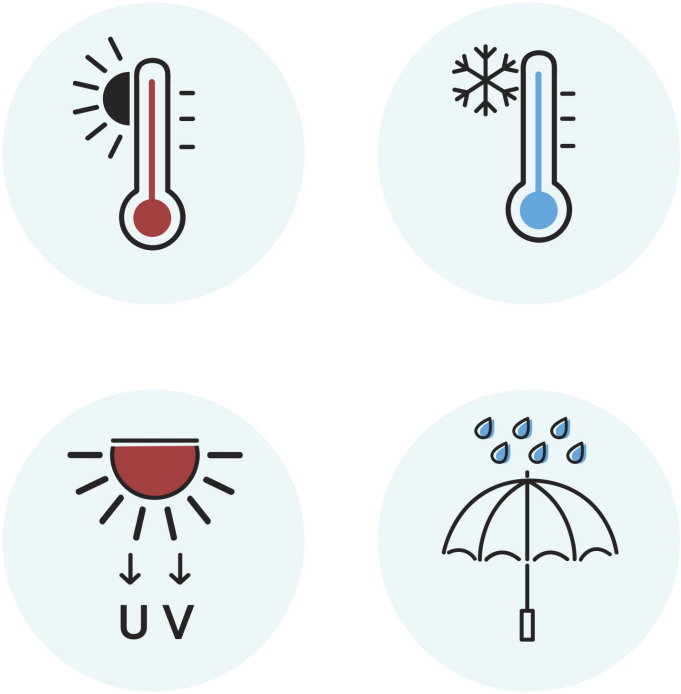
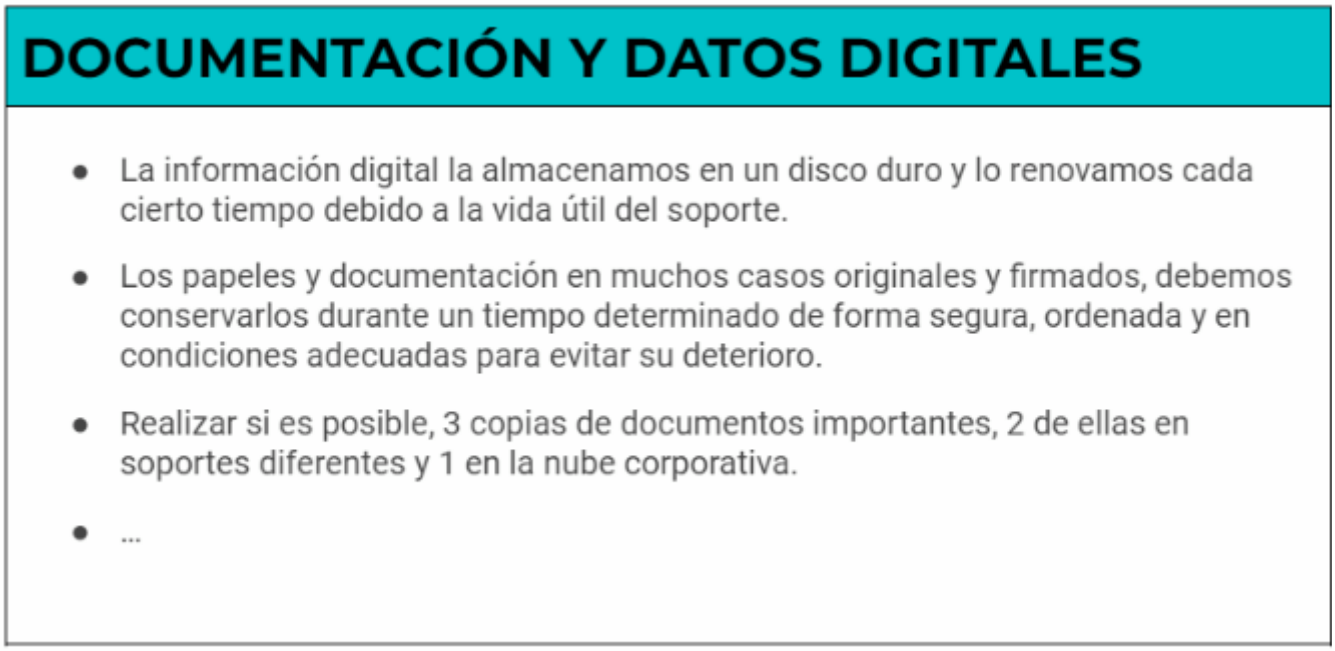


Imagen de rawpixel.com en Freepik

- Aunque reciclar está muy bien, no debemos tirar la información así sin más ya que alguien podría recuperarla. Debemos asegurarnos que la información se destruya antes de deshacernos de ella y que sea imposible su reconstrucción. En la siguiente guía mostramos las pautas para un borrado seguro. Guía sobre el borrado seguro de la información
- **Política de copias de seguridad (Backups)**. Tendremos presente la regla 3-2-1: Siempre se deben realizar y **mantener tres copias** de seguridad de los datos a respaldar. Se utilizarán al menos **dos soportes distintos** para realizar estas copias y **uno de ellos tiene que estar siempre fuera del centro educativo** (en el entorno actual de trabajo, en la **nube**).

Imagen de Apen

A continuación presentamos un modelo de plantilla, donde podremos ir rellenando las medidas en materia de seguridad adoptadas en el centro.



Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

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

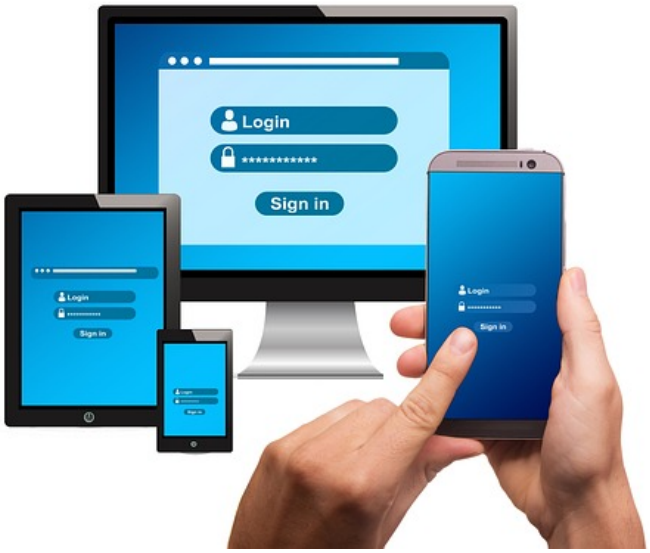


Imagen de Gerd Altmann en Pixabay

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.

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

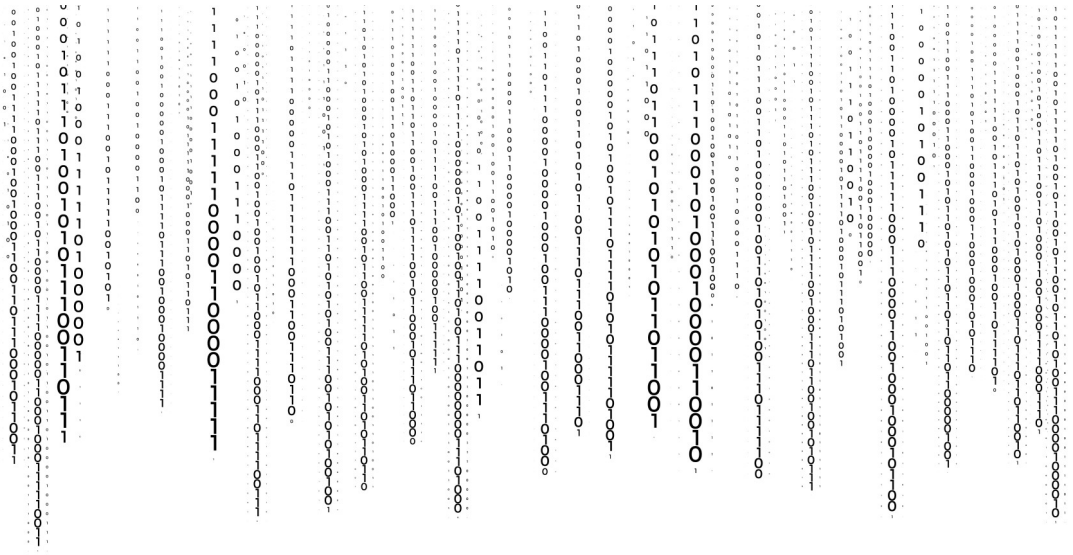


Image by vectorjuice on Freepik

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

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 de nada tener instalado en el equipo un antivirus si luego 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.

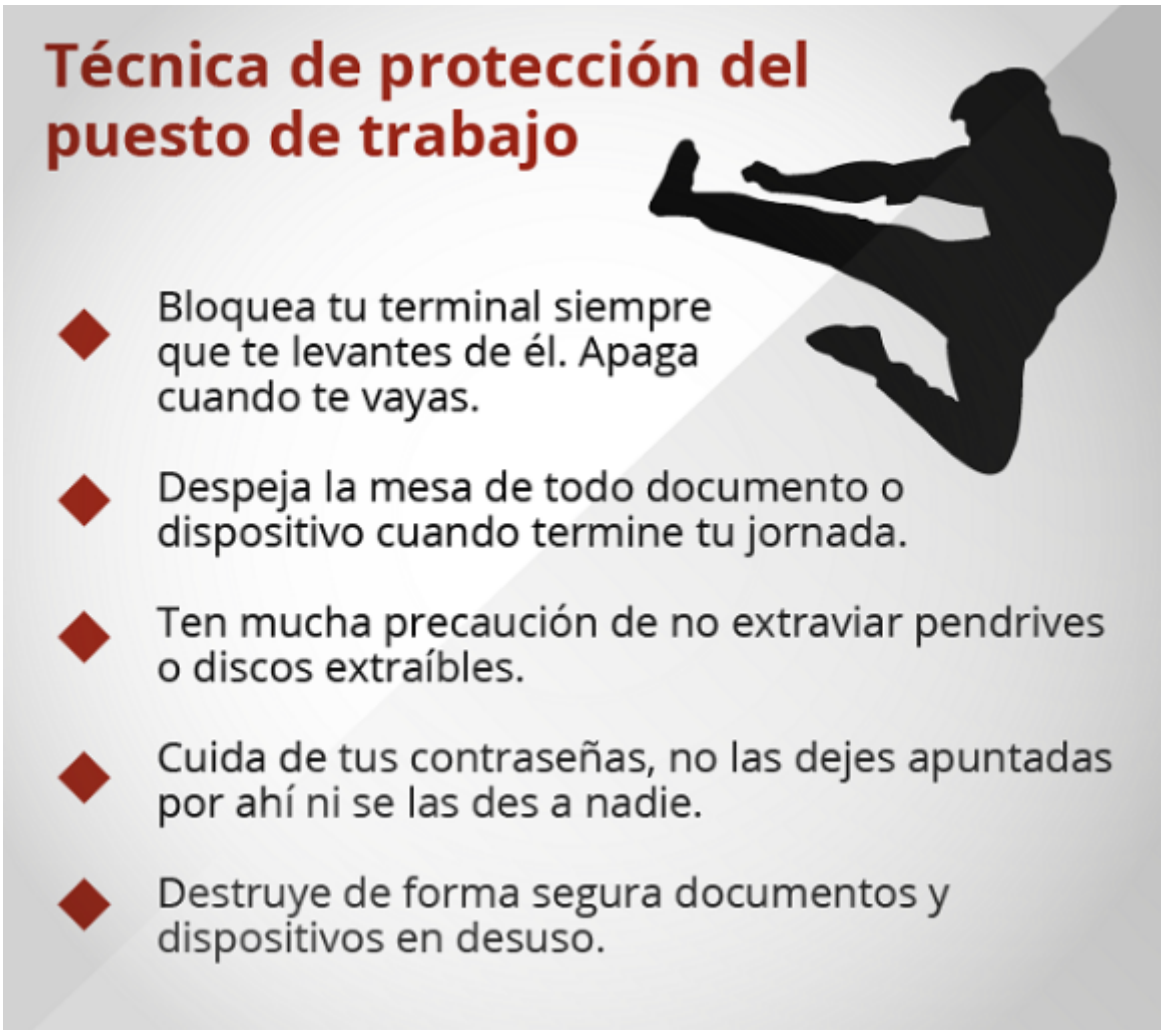
Cuando te levantes para descansar o no vayas a utilizar el ordenador en un rato, es importante bloquearlo, para que otras personas no tengan acceso a él. Los siguientes casos, son ejemplos de cuándo se bloquea el equipo:

- 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

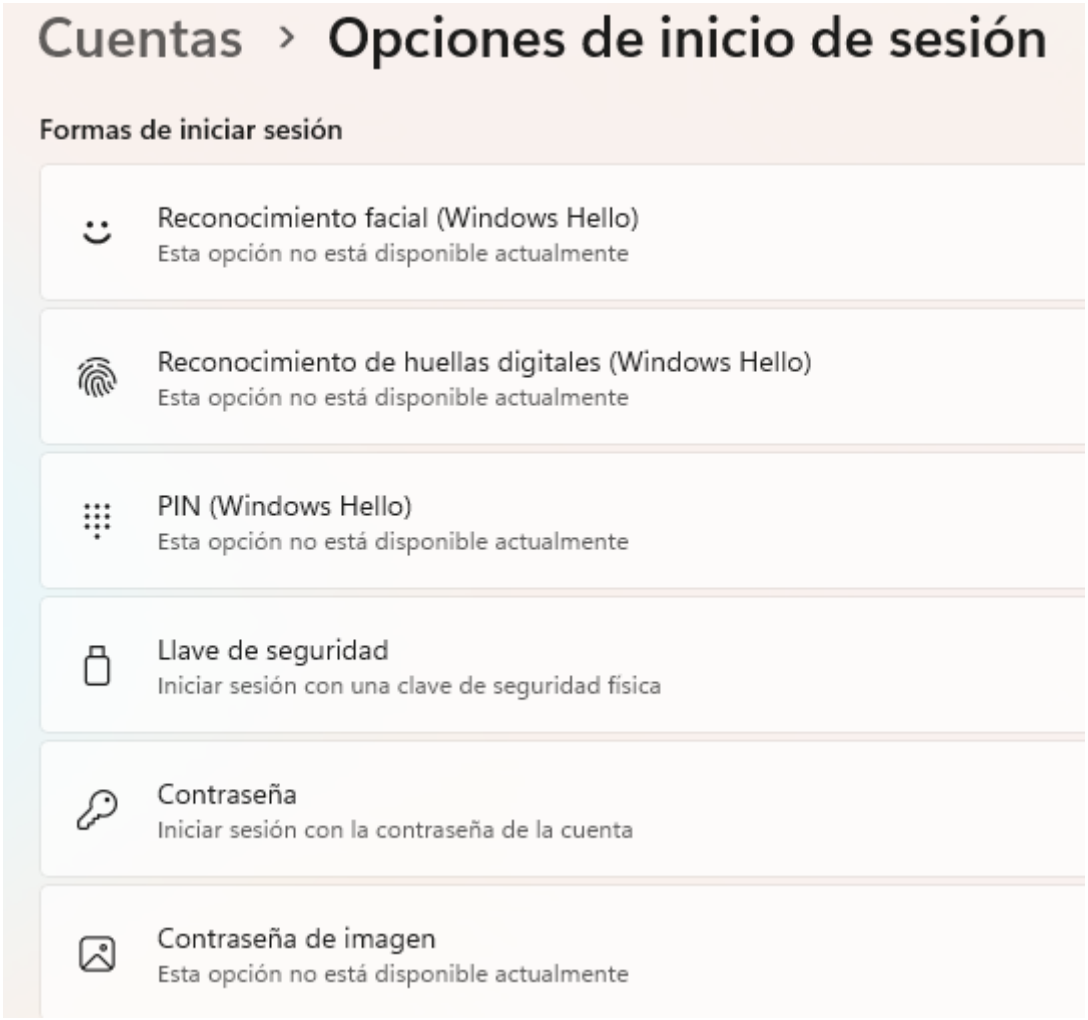
6.- Incorpora mecanismos seguros de desbloqueo

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.

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.
- ...

Infraestructura de red y conectividad

Recomendaciones de seguridad en torno a conectividades y redes:

- Definir **distintas redes en el centro** en función de la sensibilidad de los datos con los que se trabaje y proteger cada una de ellas de de accesos no autorizados, lo mismo si se dispone de conexión wifi**.** Para ello es recomendable crear una **subred** para dirección / administración, otra para profesorado, y otra para alumnado.
- Las tomas que dan **acceso a la red por medio de cable Ethernet también se deberán proteger**, evitando que estas se encuentren en lugares públicos o con poco control.

Imagen de storyset en Freepik

- Definir pautas de uso y política de usuario/contraseña de la **red WIFI** del centro, por parte de todos los miembros de la comunidad educativa.

Pixabay License

- **Controlar el DHCP.** El Protocolo de Configuración Dinámica de Host (DHCP) que es un protocolo de Internet que los equipos en red utilizan para obtener direcciones IP y otra información como la puerta de enlace predeterminada. Cuando el usuario se conecta a Internet, un equipo configurado como un servidor DHPC en el ISP le **asigna automáticamente una dirección IP**. Podría ser la misma dirección IP que tenía anteriormente o podría ser una nueva. Cuando se cierra una conexión a Internet que usa una dirección IP dinámica, el ISP puede asignar esa dirección IP a un usuario diferente. Por todos ello y con el fin de evitar vulnerabilidades, el centro educativo debe decidir sopesando la seguridad y las necesidades del centro, el tener habilitada / limitada la franja de IPs / deshabilitada, está configuración dinámica.

Imagen de storyset en Freepik

- Configuración del **Router** con criterios de seguridad (sino lo está, pueden espiar nuestras comunicaciones, utilizar la red para envío de spam, infectar los dispositivos conectados, reducir el ancho de banda,...), en los centros educativos sostenidos con fondos públicos, está **configuración viene por defecto definida por la administración educativa** y es la que realiza el soporte de los mismos, pero deberíamos de saber que aspectos de seguridad es conveniente conocer y si alguno podríamos personalizarlo para nuestro centro con la ayuda del servicio técnico que dispone la administración, por lo tanto tendremos en cuenta:
  - Asignar el mejor **protocolo de seguridad** posible en las conexiones Wifi, en estos momentos en los entornos educativos la mas segura y estable es el **WPA2**, pero ya se está hablando de la WPA3 aunque necesita ir adaptándose a la realidad educativa
  - **Cambiar u ocultar el nombre de la red o SSID**: Cuando modificamos las credenciales de acceso a nuestro router o a nuestra red wifi, estamos protegiéndolos de terceros evitando que puedan acceder a ellos. Para aumentar aún más la protección de nuestra red, es recomendable que cambiemos el nombre de nuestra red wifi (SSID)
  - **Filtrar las direcciones MAC**: Una práctica muy útil para mejorar la seguridad de nuestra conexión y protegerla de terceros es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC, que es un identificador único que posee cada dispositivo. De esta forma, habilitaremos el acceso solo a aquellos dispositivos que conocemos y evitaremos que se conecten dispositivos desconocidos

- **Desactivar el acceso remoto.** Si queremos evitar que se pueda entrar a nuestro router desde el exterior, es decir, desde otra red, tendremos que asegurarnos de que esta funcionalidad está desactivada

Imagen de vectorjuice en Freepik

- **Desactivar el WPS o conexión rápida**: Los router y sus configuraciones de seguridad han evolucionado mucho a lo largo de los años. La funcionalidad WPS, por ejemplo, es una funcionalidad que, si bien resultaba muy útil a la hora de conectar dispositivos a la red, a día de hoy puede suponer una gran amenaza contra nuestra seguridad y privacidad. El WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra red wifi. Aunque existen diversas formas mediante las cuales un dispositivo puede conectarse a una red inalámbrica utilizando, para ello, dicha funcionalidad, la más extendida de todas sigue siendo mediante una clave PIN.
- **Puertos del router**. Los puertos del router se utilizan como un canal para establecer conexiones de diferentes aplicaciones con los correspondientes servidores remotos para poder funcionar. Nuestro router es el encargado de transmitir la información que entra o sale de los dispositivos conectados a la red y la encamina, a través de router intermedios hasta su destino.
- **Crear una red para invitados**. Una red de invitados tiene como objetivo el permitir que varios dispositivos se conecten a nuestra conexión a Internet, pero permitiéndoles navegar en una red distinta a la de nuestros dispositivos habituales. De este modo, podrán acceder a nuestra conexión a Internet sin comprometer la seguridad de nuestra red principal y, sin que perdamos el control de los accesos.

A modo de resumen os dejamos un pequeño vídeo donde la OSI nos indican como proteger nuestra red

https://www.youtube.com/embed/POeuXk1UXHo

Una posible plantilla donde ir escribiendo lo relacionado con infraestructura de red y conectividad comenzaría así.

Videovigilancia en los centros educativos

En los centros educativos con la intención de mejorar el nivel de convivencia, vandalismo y seguridad es lícito el instalar cámaras de vigilancia con unas condiciones muy concretas y con una serie de condicionantes:

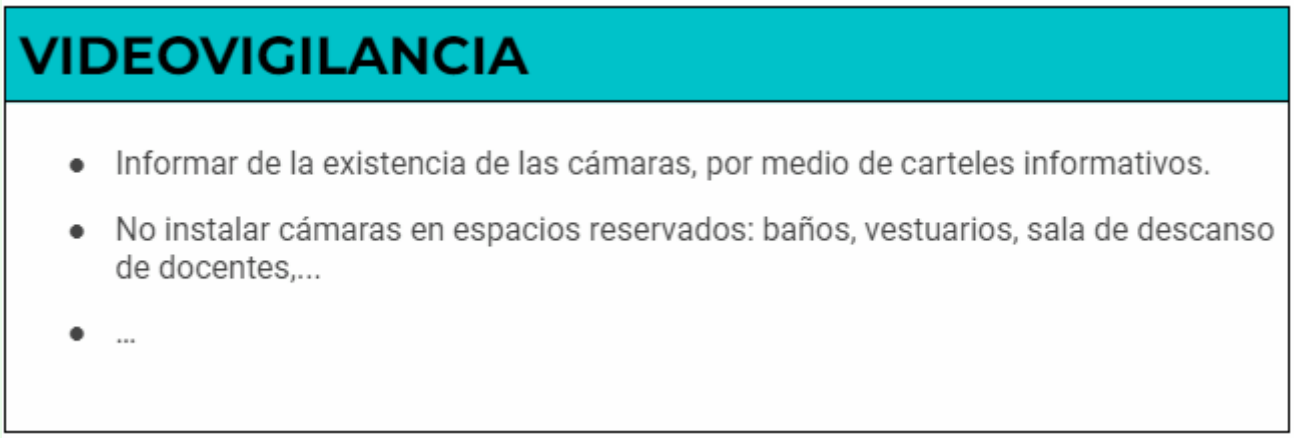
- Antes de proceder a su instalación, el centro debe planificarla respetando la **privacidad y el derecho a la imagen de quienes resulten grabados** según la normativa vigente
- En centro educativo puede instalar las cámaras y no es necesario el consentimiento del alumnado o de sus representantes legales
- Debe de **informarse de la existencia de las cámaras**, por medio de carteles informativos, en lugar bien visible, en los accesos de la zona donde serán captadas las imágenes. Los carteles mostrarán la dirección del responsable del tratamiento, los interesados (estudiantes, profesores, familias y terceras personas) pueden ejercer sus derechos de acceso, supresión y/o limitación de tales imágenes.

Imagen de rawpixel.com en Freepik

- Únicamente tendrán **acceso** a las imágenes captadas las personas que designen los **responsables del centro educativo**

- Las imágenes almacenadas no pueden guardarse indefinidamente y se conservarán durante **30 días**, a menos que capten hechos presuntamente delictivos, en cuyo caso el centro dispone de 72 horas (desde la existencia de la grabación) para comunicar tales imágenes a las autoridades competentes (Fuerzas y Cuerpos de Seguridad del Estado; de las CCAA; Fiscalía de menores / autoridad judicial)
- **En ningún caso** se instalarán cámaras en espacios reservados: **baños, vestuarios, sala de descanso de docentes, etc**.
- La instalación de **cámaras en las aulas no es justificable** con fines de videovigilancia, ya que el control del alumnado está garantizado por los docentes que imparten las sesiones.

Una posible plantilla donde reflejar lo acordado respecto a la videovigilancia sería esta.



Ciberseguridad para el alumnado

Muchas pueden ser las **actuaciones** que se pueden hacer para **concienciar al alumnado** para interiorizar la seguridad digital en las actuaciones de su día a día con los diferentes dispositivos. Nosotros como docentes podemos ayudar, formar y asesorar con una planificación de posibles actuaciones que vayan encaminadas a la prevención.

El adoptar hábitos en el día a día que estén en la dirección de un **buen uso y responsabilidad** con la tecnología ya hace que tengamos ese primera barrera de seguridad

> Más información en uso adecuado y responsabilidad del alumnado en el siguiente enlace

A continuación vamos a comentar algunas actuaciones para mejorar la ciberseguridad en el alumnado:

Jornadas formativas sobre ciberseguridad

Los centros educativos suelen concertar formaciones de prevención en muchas áreas, respecto a la seguridad, podemos contar con la participación de entidades que colaboran en la misión de divulgar y educar en las tecnologías digitales.

- Programa de Jornadas Escolares de IS4K

Las ‘Jornadas Escolares’ son de carácter **gratuito** y tienen por objetivo mejorar las competencias digitales en profesorado y alumnado de **Educación Primaria y Secundaria** para hacer un **uso seguro y responsable de Internet**.

> Más información en el siguiente enlace

- Plan director para la convivencia y mejora de la seguridad

El Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos donde los cuerpos y fuerzas de seguridad del estado (Guardia Civil y Policía Nacional viene)n a los centros y nos ayudan en temas vinculados a internet, ciberacoso, redes sociales... y las responsabilidades civiles e incluso penales que tienen las actuaciones delictivas.

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

Síguenos en

@interiorgob | @policia | @guardiacivil

www.policia.es

DESCÁRGATE ALERTCOPS PARA TU SEGURIDAD

www.guardiacivil.es

Además nos animan a descargarnos la aplicación Alertcops, con la que **cualquier persona**, con independencia de su idioma, origen o de sus discapacidades auditivas o vocales **pueda comunicar** a las Fuerzas y Cuerpos de Seguridad del Estado (**Policía y Guardia Civil) una alerta, información, dato o noticia sobre un acto delictivo** o incidencia de seguridad del que está siendo víctima o testigo.

ALERTCOPS

> Más información en el siguiente enlace

- Realización de Talleres online

Como el de "**Día de intenet seguro**" realizado por el INCIBE, con actividades para fomentar, entre niños, jóvenes y sus entornos más cercanos, un uso seguro y positivo de las tecnologías digitales, promocionando sus competencias en esta materia y ayudándoles a ser respetuosos, críticos y creativos, en línea con los principios digitales europeos

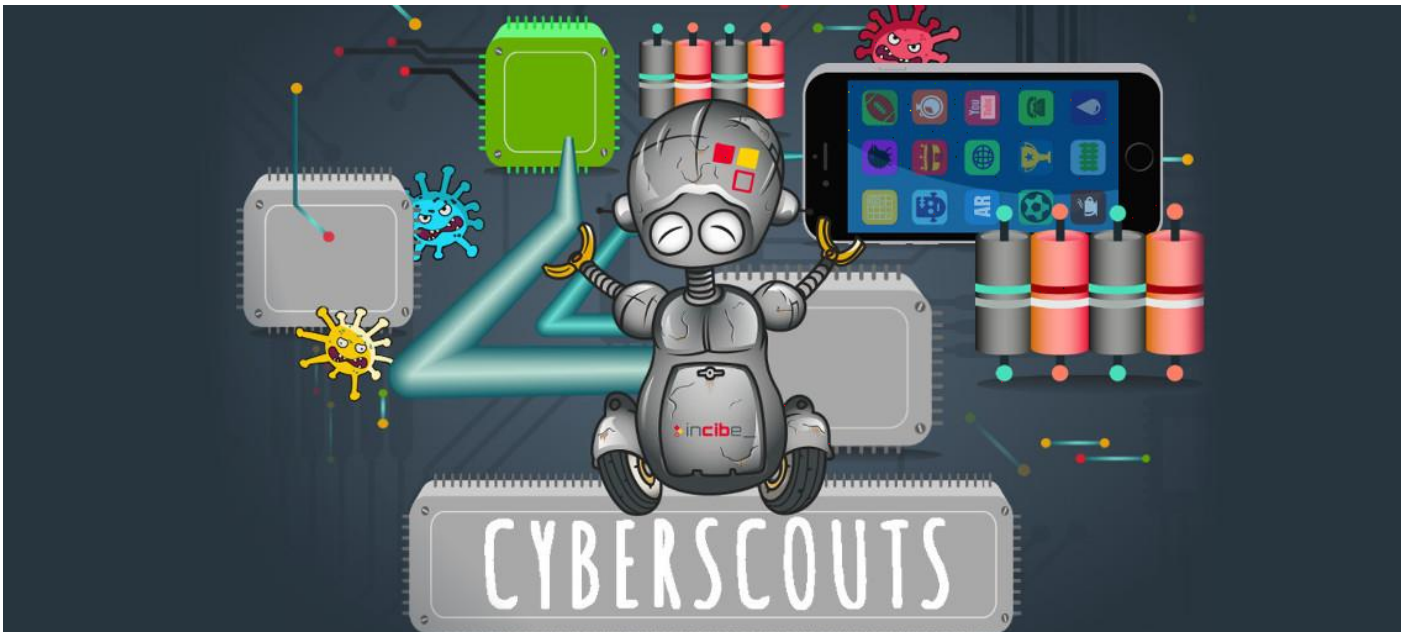
> Más información de estos talleres en el siguiente enlace

Juegos que nos conciencian en seguridad digital

Muchos son los juegos que tenemos en internet que buscan aprender más sobre seguridad a modo de ejemplo hemos seleccionado

- Juego de Cyberscouts

Es un juego desarrollado por el INCIBE donde el alumnado aprende a proteger su identidad digital, a reconocer una buena contraseña, a identificar riesgos en internet, además de trabajarlo en clase puede hacerse posteriormente en familia consiguiendo adquirir conocimientos para hacer un uso más seguro de los servicios de Internet.



Más información en el enlace

- Juego de Hackers vs Cybercrook

Juego desarrollado por INCIBE donde a través de las diferentes misiones, tendremos la oportunidad de aprender sobre la importancia de generar contraseñas seguras, la necesidad de realizar copias de seguridad, las precauciones al conectarte a redes wifi públicas y ¡muchas cosas más! Todo ello aderezado con la diversión de aprender jugando.

Más información en el siguiente enlace

Instalación de la APP CONAN mobile

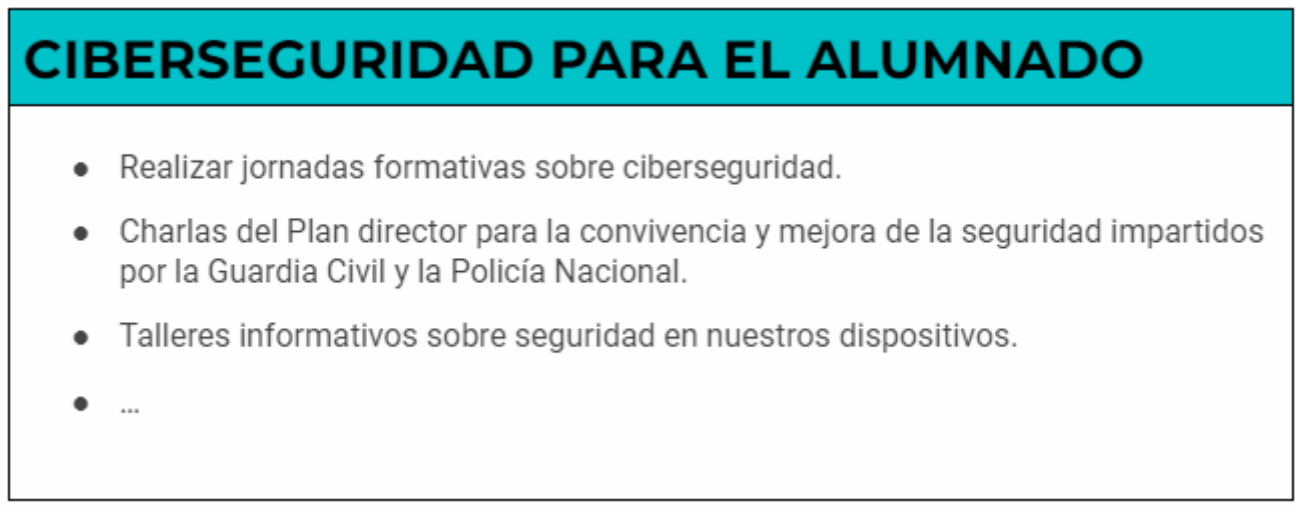
Finalmente vamos a presentar una **herramienta gratuita** avalada por el instituto nacional de ciberseguridad, de comprobación integral de la seguridad de nuestros **smartphones y tabletas**, que muestra soluciones a posibles riesgos a los que estamos expuestos y proporcionándonos algunos consejos que nos ayudarán a mejorar la seguridad de nuestros dispositivos.

Analizando vulnerabilidades a nivel de **configuración**: propiedades de configuración, redes Wifi inseguras, dispositivos bluetooth inseguros; a nivel de **aplicaciones**: maliciosas o sospechosas; a nivel de **permisos**: alto, medio, bajo, otros.

Además tiene un **servicio proactivo** de eventos relevantes que se están registrando en nuestro dispositivo (si estoy con mensajes de tarificación especial -servicios premium-, si mis aplicaciones tienen conexiones potencialmente peligrosas, información de la IP/dominio/localización geográfica)

https://www.youtube.com/embed/BOhfRa91HRg

Plantilla de posibles actuaciones con el alumnado en materia de ciberseguridad.



La seguridad digital en el entorno familiar

Las familias tenemos la responsabilidad de conocer las situaciones de riesgo a la que están sometidas nuestros hijos cuando navegan por la red, para **ayudarles a disfrutar con seguridad**, como parte de nuestra labor de mediación parental. Por eso, es necesario saber el origen de estos riesgos y las medidas de protección a nuestro alcance.

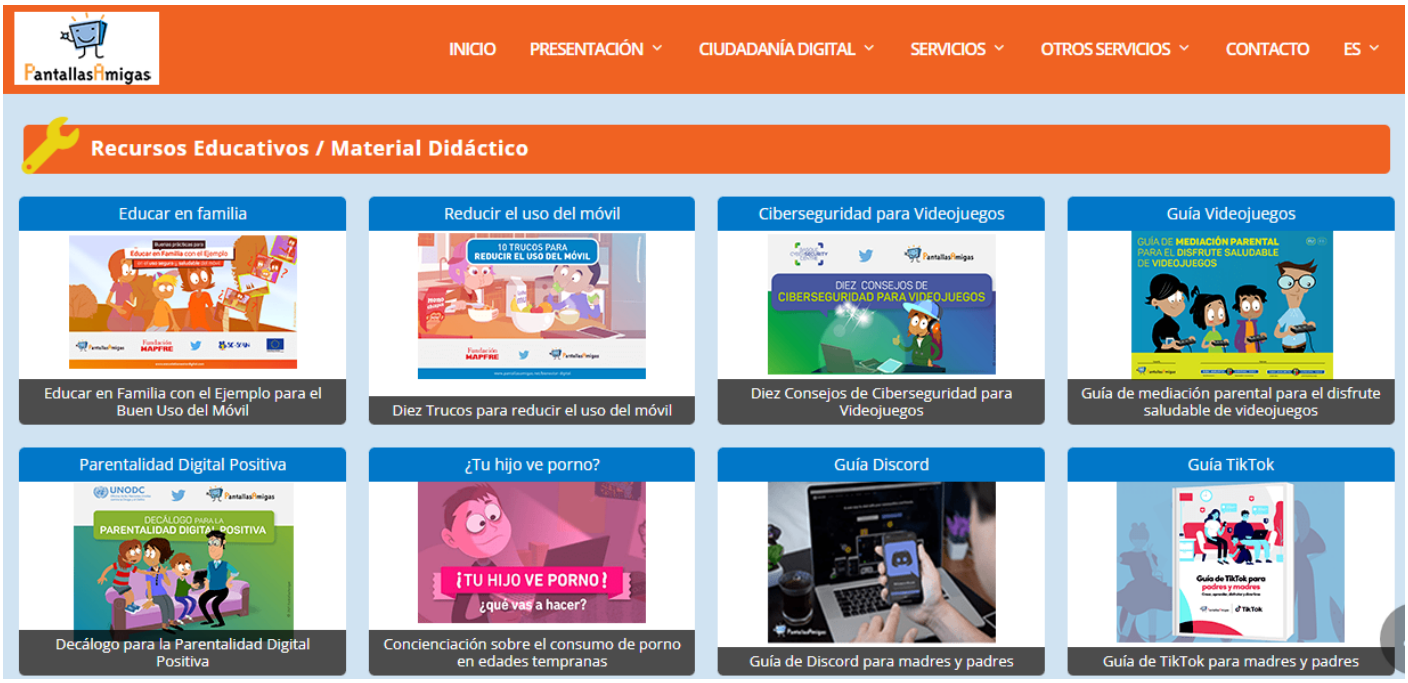
¿Cómo reaccionaremos las familias desde casa ante los problemas de la Red?

1. ***Mantener la calma.*** Es normal sentir temor ante las posibles consecuencias de los problemas online, pero debemos ser conscientes de que en esos momentos los y las menores necesitan de nuestro apoyo, seguridad y confianza, evitando empeorar la situación, culpabilizándoles o sobrerreaccionando.
2. ***Guardar evidencias.*** Es recomendable no eliminar impulsivamente las pruebas del conflicto o problema, como imágenes, mensajes, perfiles de redes sociales o páginas web, sin consultar con un servicio especializado. De hecho, puede ser de utilidad tomar capturas de pantalla para ayudar a resolver el caso o esclarecer lo ocurrido, si posteriormente fueran borradas.

3. ***Buscar información y contactar con un profesional.*** Existen muchos servicios de ayuda en los que nos podemos apoyar para saber cómo actuar, ya que cada situación es distinta. Todas las redes sociales, juegos y la mayoría de las páginas web poseen centros de ayuda y seguridad y soporte técnico, que nos permiten contactar con los administradores, reportar un problema o solventar un conflicto.

Conocer recursos online donde informarse las familias

En caso de necesitar conocer las últimas novedades sobre seguridad, las familias deben de conocer páginas fiables a las que poder recurrir. Por ejemplo la web https://www.pantallasamigas.net/ desarrolla proyectos y recursos educativos para la capacitación del alumnado de forma que puedan desenvolverse de manera autónoma en Internet, siendo el objetivo final que desarrollen las habilidades y competencias digitales que les permitan participar de forma activa, positiva y saludable en la Red.



Web de pantallas amigas

Además el **Instituto Nacional de Ciberseguridad (INCIBE)** pone a disposición de la comunidad educativa una serie de recursos, algunos de ellos a través de **Internet Segura for Kids (IS4K)** y de la **Oficina de Seguridad del Internauta (OSI) que son de gran ayuda, recordamos Línea de Ayuda 017**que es la línea de ayuda gratuita de ciberseguridad de INCIBE, operativa todos los días del año. Se atienden, entre otros, consultas de menores, madres y padres, profesores y otros profesionales de la educación.

- **Redes Sociales**

Estar al día en todo lo relativo a internet y tecnologías, para poder ayudar y acompañar a sus hijos o hijas en el buen uso de ellas. Por ejemplo en las manejo de las redes sociales

> Más información en el siguiente enlace

- **Charlas formativas a las familias del Plan director para la convivencia y mejora de la**

seguridad

Las **familias suelen ser citadas** a charlas informativas para conocer de primera mano lo que van a escuchar sus hijos en los centros educativos y poder trabajar de forma colaborativa familias-centro-alumnado.

El Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos donde los cuerpos y fuerzas de seguridad del estado (Guardia Civil y Policía Nacional viene)n a los centros y nos ayudan en temas vinculados a internet, ciberacoso, redes sociales... y las responsabilidades civiles e incluso penales que tienen las actuaciones delictivas.

- **Controles parentales como herramientas de seguridad**

El **control parental** es una herramienta que permite a las familias controlar y limitar el contenido al que acceden los niños en internet, independientemente del dispositivo que usen (móviles, ordenadores, tablet, etc).

Entre las **funciones habituales** que suelen ofrecer este tipo de herramientas destacan: control web, control de aplicaciones, bloqueo de llamadas, tiempo de uso, alarmas, geolocalización o botón de emergencia.

Estas herramientas son un **complemento en nuestra labor de mediación parental**, siempre deben ir acompañadas de actividades digitales en familia que faciliten un clima de comunicación y confianza.

> Más información sobre controladores en los diferentes aparatos electrónicos en el siguiente enlace

- ## Utilizar los grupos de mensajería instantánea o Whatsapp entre familias como herramienta de ayuda en la convivencia y seguridad

Los grupos de mensajería instantánea son herramientas que pueden ser muy útiles a las familias para ayudarse a organizarse, y mantenerse en contacto en todo lo relacionado con el centro educativo, además puede servirnos con criterios de **seguridad**.

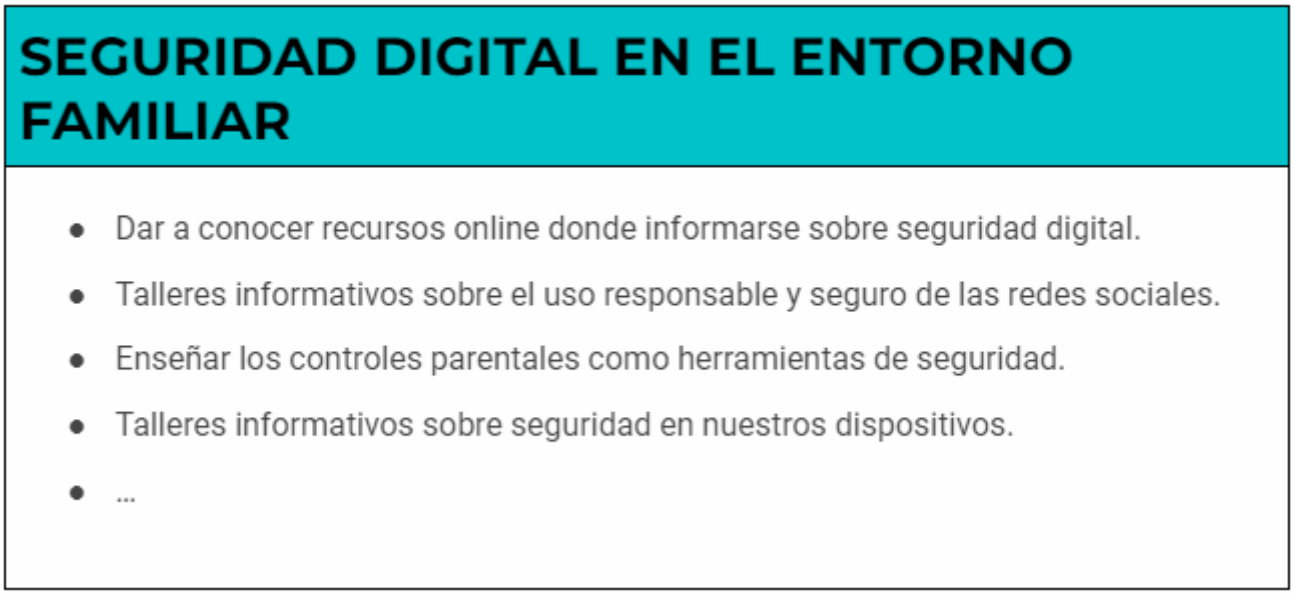
Es muy importante respetar una serie de normas para que el grupo aproveche el gran potencial, de lo que es tener información de primera mano, en lo que concierne a nuestros hijos.

En la siguiente imagen se indican 8 normas para el grupo del colegio.

Finalmente recordamos una recomendación de la Agencia Española de Protección de Datos (AEPD) exponiendo que, las **comunicaciones** entre profesores y padres de alumnos deben llevarse a cabo, preferentemente, a través de los medios puestos a disposición de ambos por el centro educativo **(plataformas educativas, correo electrónico** del centro,...).

Foto de Anton en Pexels

El uso de aplicaciones de mensajería instantánea (como WhatsApp) entre profesores y padres o entre profesores y alumnos no se recomienda. No obstante, **en aquellos casos en los que el interés superior del menor estuviera comprometido**, como en caso de accidente o indisposición en una excursión escolar, y con la finalidad de **informar y tranquilizar a las familias**, titulares de la patria potestad, **se podrían captar imágenes y enviárselas.**

> Plantilla de posibles orientaciones a las familias en materia de ciberseguridad.
>
> 
>