Sin miedo a hacer clic

Índice

1. Navegación segura: ¿Misión imposible?

Nuestra sociedad está cada vez más digitalizada. Los dispositivos conectados a Internet han pasado a formar parte de la mayoría de las actividades diarias de las personas, no solo en el trabajo y los estudios, sino también en el tiempo libre, modificando la forma en la que nos relacionamos.

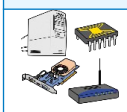
Este gran desarrollo digital ha dado lugar a numerosos avances y facilidades en la vida diaria, pero también está creando problemas como, por ejemplo, el aumento de los delitos cibernéticos. ¿Te atreves a intentar solucionarlos y contribuir a crear una sociedad digital mejor?

2. Exploración de control

Primera revisión

Los dispositivos digitales, como ordenadores o teléfonos móviles, están compuestos por ***hardware*** y ***software***. Para facilitar la comprensión de estos dos conceptos, es habitual compararlos con algo que todos conocemos muy bien: nuestro cuerpo y nuestra mente.

Por lo tanto, en un dispositivo electrónico se pueden diferenciar:

Hardware = Tu cuerpo	
 ¿Qué es?	El *hardware* es el conjunto de componentes físicos de los que está constituido el equipo. El *hardware* equivaldría a tu cuerpo: los huesos, los músculos y los órganos
¿Qué incluye?	En el caso de un ordenador, el *hardware* incluye componentes como la pantalla, el teclado, el ratón, el procesador, la memoria RAM y el disco duro, entre otros. Todos estos componentes son tangibles, es decir, los puedes tocar, al igual que puedes tocar tus brazos, tus piernas o tu cabeza. Por eso, en muchos libros, definen *hardware* como la "**parte física**" del sistema.
Software = Tu mente	
 ¿Qué es?	El *software* es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible su funcionamiento. El *software* sería equivalente a tu mente.
¿Qué incluye?	El *software* incluye todos los programas, aplicaciones y sistemas operativos que hacen que el ordenador funcione y realice las diferentes tareas. Así como tu mente te permite pensar, soñar y recordar, el *software* le permite al ordenador

	operar, ejecutar programas, procesar información y realizar todas sus funciones. Por eso, en muchos libros, definen software como la "**parte lógica**" del sistema.

Hardware

Lo veo y lo toco

La palabra *hardware* hace referencia al conjunto de componentes físicos de los dispositivos digitales. Se trata de la parte física, lo que podemos ver y tocar.

Se puede clasificar de la siguiente forma:

***Hardware* interno:**		
¿Qué es?	El *hardware* interno es aquel que se encuentra dentro del ordenador.	
Principales elementos	Placa base 	Circuito impreso al que se conectan el resto de los componentes de un ordenador para que estos funcionen de manera óptima. Podría decirse que es equivalente a la columna vertebral, ya que ejerce de soporte de los demás componentes.
	Procesador o CPU (*Central Processing Unit*) 	La CPU es la responsable de dirigir todas las tareas que lleva a cabo el equipo, equivalente al cerebro. También se denomina procesador. En estas tareas se encuentran implicados los periféricos de forma que: 1. El procesador o CPU recibe datos de los periféricos de entrada. 2. Realiza operaciones y cálculos matemáticos con los datos, es decir, los procesa, y ejecuta los programas. 3. Envía los resultados a los periféricos de salida.
	Memoria RAM 	Componente que permite almacenar temporalmente datos o instrucciones que se están utilizando en el momento. Es equivalente a tu memoria a corto plazo.
	Tarjeta gráfica	Componente que recibe y procesa la información gráfica, al igual que hace la parte de tu cerebro responsable de procesar las imágenes.
	Disco duro 	Componente del equipo en el que se guardan permanentemente grandes cantidades de datos. Pueden ser de varios tipos: • Discos de estado sólido (SSD) son las unidades de

		almacenamiento de datos más comunes en la actualidad, son equivalentes a nuestra memoria a largo plazo. Los SSD son más pequeños y rápidos que las clásicas unidades de disco duro. No generan ruido y permiten que los equipos sean más delgados y ligeros. • Unidades de disco duro (HDD).
***Hardware* periférico:**		
¿Qué es?	El *hardware* periférico se encuentra fuera del ordenador.	
Clasificación 	Periféricos de entrada	Elementos equivalentes a nuestros sentidos, ya que permiten captar información del entorno e introducirla al sistema. Ejemplos: el teclado, el ratón, el micrófono...
	Periféricos de salida	Elementos equivalentes a nuestros músculos, puesto que reciben información del disco duro (cerebro) y ejecutan una acción. Ejemplos: la impresora, los altavoces, la pantalla...

Software

El sistema operativo es el *software* más importante del ordenador porque coordina y dirige todos los servicios y aplicaciones que utilizas. Se trata de programas especializados que permiten y regulan los aspectos más básicos del sistema, como crear una estructura de carpetas adecuada para guardar o recuperar la información y gestionar los recursos del sistema (la impresora, el monitor, las unidades de disco, etc.). Los sistemas operativos más utilizados son **Windows**, **Linux** y **Mac OS**.

Los ordenadores del instituto tienen instalada la maqueta Abalar que, ni más ni menos, es un sistema operativo Linux con una serie de aplicaciones o programas preinstalados. **Linux** es un **sistema operativo libre**, el uso del *software* libre en educación permite que se puedan tener en casa todos los programas con los que trabajamos en el centro. Además, se puede disponer de ellos sin ningún desembolso económico.

Los sistemas operativos pueden usarse con **interfaces gráficas** que facilitan a la persona usuaria hacer los procesos del sistema (arrastrar, mover, copiar...). También se pueden usar con una línea de **comandos** que funciona basándose en órdenes introducidas en ella.

3. Aprende a conectarte

Ciberseguridad: escudo virtual

La **ciberseguridad** es el conjunto de prácticas que se llevan a cabo para proteger los datos digitales, los equipos informáticos y las redes de posibles ataques maliciosos e intentos de robo de información. Se encarga de prevenir y detectar cualquier tipo de actividad maliciosa con antelación.

Durante el manejo de dispositivos electrónicos pueden presentarse diferentes amenazas, peligros o riesgos. A continuación, aprenderás a identificarlos y cómo mantener tu equipo en forma y aplicando la ciberseguridad para proteger tanto tus dispositivos como tus datos.

3.1. ¡No te la juegues con los clics!

Aprende a conectarte

Para mantener protegido tu organismo debes llevar unos hábitos de vida saludables, como mantener una dieta equilibrada y hacer ejercicio de forma habitual. De la misma manera, debes establecer medidas para que tus dispositivos electrónicos se mantengan seguros y sean menos vulnerables frente ataques externos.

Aquí tienes algunas recomendaciones básicas para mantener tus dispositivos en forma:

Actualiza tus dispositivos:

Mantener el *software* actualizado ayuda a que el ordenador funcione mejor, esté más protegido y pueda aprovechar las últimas mejoras. Para mantener tu equipo actualizado puedes:

- Activar actualizaciones automáticas.
- Programar actualizaciones regulares para las aplicaciones.
- Eliminar aplicaciones que ya no usas o no necesitas.

Utiliza contraseñas fuertes y seguras:

Las contraseñas fuertes y seguras son esenciales para proteger tus cuentas y datos personales contra el acceso no autorizado. A continuación, tienes algunas pautas para crear contraseñas fuertes y mantener la seguridad de tus cuentas.

Navega por sitios seguros:

Si utilizas datos personales dentro de las páginas que visitas, asegúrate de que usan el protocolo: (**https://**). La "**s**" final te indica que es un lugar seguro.

Puedes habilitar y configurar opciones de seguridad en tu navegador, entre las cuales se encuentran:

- Activar la navegación segura.
- Bloquear las ventanas emergentes.

- Realizar configuraciones de privacidad.

Conéctate a redes seguras:

Conéctate sólo a redes Wi-Fi seguras y evita las redes públicas. Las redes públicas pueden ser menos seguras y estar expuestas a posibles amenazas.

Vigila tus descargas:

Ten precaución al realizar descargas desde Internet, pues podría tratarse de *software* malicioso. Para proteger tu equipo y tus datos de posibles amenazas es fundamental que sigas estas pautas:

- Utiliza páginas web oficiales y fuentes confiables.
- Evita abrir archivos adjuntos en correos electrónicos de remitentes desconocidos.
- Comprueba los archivos adjuntos antes de descargarlos, utilizando el antivirus.
- Al descargar aplicaciones en dispositivos móviles, utiliza las tiendas de aplicaciones oficiales, como la App Store para iOS o Google Play para Android.

Haz copias de seguridad:

Realizar copias de seguridad de tus datos es una práctica crucial para proteger tu información contra pérdidas, ya sea por errores humanos, fallos técnicos, ataques de *software* malicioso u otros problemas.

Guarda copias de seguridad en discos duros externos, unidades USB o almacénalas en la nube.

3.2 Intrusos en tus dispositivos

Vacunas contra invasores

¿Sabes cómo mantener tu ordenador, *tablet* o móvil a salvo de virus y otros invasores? Es parecido a vacunarnos para protegernos de enfermedades.

Cuando te vacunas, estás enseñando a tu sistema inmunológico a reconocer virus y bacterias para poder ser más eficiente en la lucha contra estas amenazas. Instalar un buen antivirus en tu ordenador o dispositivo móvil es equivalente a vacunarlo. El antivirus defiende a tu dispositivo de todo tipo de *software* malicioso.

Mantener actualizados tus dispositivos y usar programas antivirus te ayudará a proteger tus equipos de ataques y amenazas que podrían dañarlos o robar tu información personal.

Recuerda, así como cuidas de tu salud, es importante cuidar la salud de tus dispositivos. ¡Mantenlos actualizados, protegidos y listos para luchar contra esos molestos virus informáticos!

Amenazas

Malware:

Los **virus** y los **gusanos** son códigos maliciosos que se meten en nuestros ordenadores, *tablets* o móviles y cambian su funcionamiento.

El virus requiere que alguien, consciente o inconscientemente, propague la infección. En cambio, un gusano informático no requiere interacción humana para propagarse. Los virus y los gusanos son dos ejemplos de *malware*, una categoría amplia que incluye cualquier tipo de código malicioso.

Imagina que estos virus y gusanos son personas intrusas que se cuelan en una fiesta sin ser invitadas y empiezan a molestar. Algunos de estos "intrusos" tienen nombres especiales como:

- **Troyano**: *malware* escondido en un software aparentemente no malicioso.
- ***Adware***: *malware* que muestra publicidad, normalmente incrustada en las páginas web que visitas.
- ***Spyware***: programa espía.
- ***Ransomware***: programa malicioso que bloquea tus archivos y pide un rescate para desbloquearlos.
- ***Keylogger***: *malware* que registra lo que escribes en el teclado, como tus contraseñas o cualquier información privada.

Delitos cibernéticos:

Los delitos cibernéticos son otra amenaza informática que suele tener como objetivo obtener beneficios económicos, como es el caso de las estafas *online*, aunque también se realizan para dañar o interrumpir el funcionamiento de los sistemas informáticos.

Los y las **ciberdelincuentes** son personas que usan sus habilidades informáticas con fines maliciosos. No debes confundir *hackers* con ciberdelicuentes.

No le abras la puerta

El *malware* puede llegar a tu dispositivo de diferentes maneras. Las formas más habituales son las siguientes:

- Cuando abres un archivo adjunto de un correo electrónico o un SMS extraño.
- Si usas memorias USB o discos duros externos infectados.
- Al descargar juegos o programas de sitios web que no son seguros.
- Visitas páginas web que no son de confianza.
- Al hacer clic en enlaces engañosos en redes sociales o mensajes de texto.

Antivirus

Para evitar infecciones por *malware* y proteger la información almacenada en tus dispositivos debes usar programas **antivirus** y mantenerlos actualizados.

Los antivirus son programas que actúan activando un filtro que atrapa los virus informáticos y los elimina. Y lo mejor es que podemos tener antivirus no solo en los ordenadores, sino también en los móviles, las *tablets* e, incluso, en los televisores inteligentes.

Así que, igual que comes frutas y verduras para mantener fuerte tu cuerpo, debes mantener actualizados los antivirus para proteger tus dispositivos. ¡Es como darles una dieta sana y ejercicio a nuestros ordenadores y móviles!

3.3 Todo en orden

Mantenemos la higiene de nuestro ordenador

Igual que para mantenerte saludable tienes ciertos hábitos de higiene, cuando utilizas un dispositivo informático debes mantenerlo organizado y preparado para que su rendimiento sea máximo. Con las tres operaciones básicas propuestas a continuación tendrás siempre tu ordenador en plena forma:

- **Orden en los archivos**: lo primero que debes tener en cuenta es el orden que mantienes con los archivos y las aplicaciones, agrupándolos de forma ordenada en una estructura de carpetas y desinstalando las que ya no uses.
- **Mantenimiento de los discos duros**: debes tener claro el tipo de unidades de almacenamiento que tiene tu equipo. Si tienes disco duro (HDD) se recomienda desfragmentarlo periódicamente para que la información esté más ordenada, los tiempos de acceso a ella sean menores y la velocidad de tu ordenador mayor. Si, por el contrario, tu ordenador tiene una unidad de estado sólido SSD, la desfragmentación no se recomienda porque empeorará su funcionamiento, los SSD se ordenan de forma automática y su rendimiento no se ve afectado por ese "desorden" que sí ocurre en los HDD.
- **Limpieza del ventilador de forma periódica**: esto evita que la placa base se sobrecaliente. Piensa que el polvo es nuestro enemigo, lo mejor es que limpies el polvo de las ranuras de ventilación y del ventilador del procesador.

Evita rastreos

Cuando navegas en Internet, los sitios webs que visitas recopilan información sobre tus actividades en ellos y almacenan la información en tu dispositivo en forma de pequeños archivos. Esos archivos se llaman ***cookies***. Las *cookies* sirven para hacer que el sitio web sea más cómodo para las personas usuarias y seguir las actividades de las personas visitantes.

Por ejemplo, un sitio web de compras de videojuegos puede recordar en qué moneda elegiste pagar, o si marcas la opción “Recuérdame” en la página de inicio de sesión de

una red social, no tendrás que introducir tu nombre de usuario y contraseña cada vez que la visites. Sin embargo, además de facilitarte el acceso al sitio web, las *cookies* permiten recopilar tus datos para hacerte sugerencias y mostrarte anuncios dirigidos.

Existen dos formas de controlar las *cookies* en tu navegador:

- La primera es **configurar las *cookies*** en la página a la que accedes. Las páginas te van a preguntar al entrar si quieres aceptar todas las *cookies*, ninguna o solo las necesarias.
- La segunda es **bloquear las *cookies*** en la configuración de tu navegador, aunque si deshabilitas todas las *cookies*, algunos sitios web no funcionarán de forma amigable.

Muchas veces, bloquear las *cookies* en las webs no basta o es muy tedioso, en su lugar, muchos navegadores ofrecen un modo de incógnito. Habilitado, este modo permite que los sitios web instalen *cookies*, pero el navegador las elimina automáticamente cuando cierra la ventana de incógnito.

Respetamos las obras de los demás

Licencias de uso

Cuando se habla de **licencias de uso** hay que tener claro qué es la **propiedad intelectual**. Cuando una persona crea un producto, este producto va a estar protegido por la propiedad industrial (si es una creación relacionada con la industria como un juguete o un vehículo) o por la propiedad intelectual (si es una creación literaria o artística como un libro, una foto o una canción). Las obras quedan protegidas automáticamente por los **derechos de autoría**. Estos derechos están regulados por licencias de uso. Los tres tipos principales de licencias de uso son:

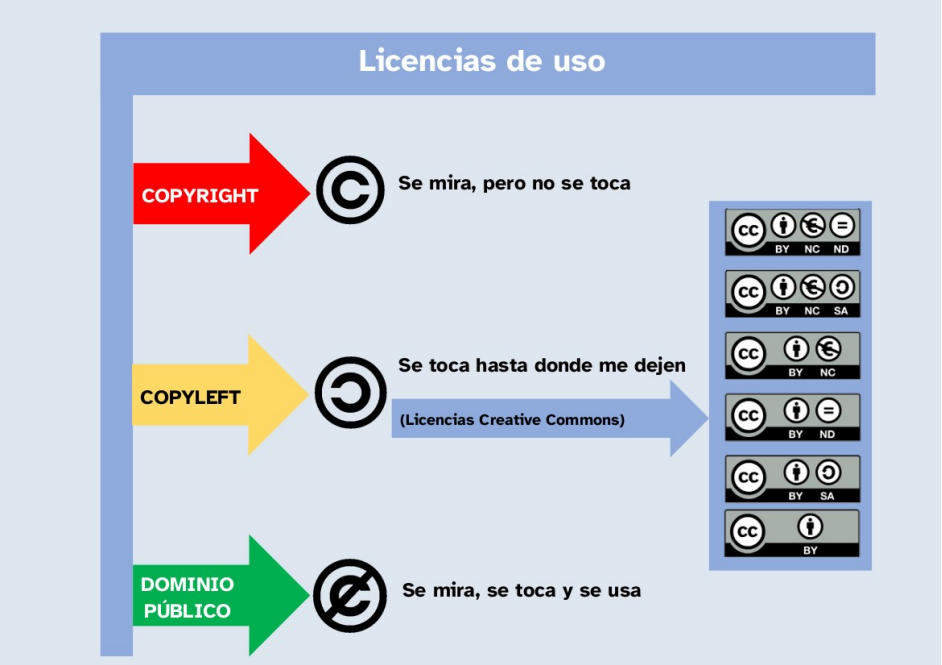
Copyright: Este tipo de licencia es la más utilizada, ya que le permite a la persona autora de la obra tener **todos los derechos**, de forma que cualquier otra persona solo podrá utilizar o modificar esta obra con el permiso justificado o pagando derechos de autoría.

Copyleft: Este tipo de licencia autoriza a que cualquiera la **reproduzca citando a la persona creadora** de la obra. Dentro de este tipo de licencia se encuentran las licencias Creative Commons.

Commons Creative Commons

Este tipo de licencia fue creada para que la persona creadora de la obra tenga poder para controlar cómo se puede compartir su obra. Las obras con licencia Creative Commons se pueden compartir respetando las condiciones de la licencia, siempre reconociendo su autoría, es decir, indicando la persona creadora.

Dominio público: Este tipo de licencia implica que las obras pueden ser **utilizadas sin restricciones** siempre que se respeten los **derechos morales**.



¿Cómo puedo referenciar las imágenes?

Al usar las imágenes debes **referenciarlas**, es decir, indicar de dónde las obtuviste y reconocer a las personas autoras. La forma de referenciar las imágenes correctamente en los trabajos es la siguiente:

Persona autora o nombre de la organización. Título del recurso. URL. Tipo de licencia

3.4 ¿Eres tú o tu avatar?

No solo es importante que mantengas tu equipo en forma, protegido y organizado, sino que también es fundamental que tú te cuides y te protejas durante el uso del mismo.

Ten en cuenta que debes proteger tanto tu identidad, como tu salud y tu bienestar digital, además de respetar las normas de ciberconvivencia.

¿Te reconoces en la pantalla?

Tu **identidad digital** es tu carta de presentación en Internet, ya que es el conjunto de datos acerca de tu persona publicados en la red. Al igual que en la vida real, esta

información proyecta una imagen tuya y crea una **reputación digital**. ¿Te habías preguntado alguna vez cómo te ven los demás a través de tu identidad digital?

Tu identidad digital se construye a partir de los siguientes datos:

Además, en el momento que accedes a la red, estás creando tu **huella digital**, constituida por el rastro que dejas al navegar por Internet, interactúas y publicas contenidos.

Ambas pueden coincidir con tu "yo real" o no.

Tú ya no eres tú

¿Sabías que otras personas pueden hacerse pasar por ti en la red y dañar tu identidad digital?

La **suplantación de identidad** es la apropiación de la identidad de otra persona (o también de una empresa) con motivos malintencionados. Estos motivos pueden ser muchos y muy diversos: robo de información, dañar la reputación digital de tu persona, cometer algún tipo de fraude o delito en tu nombre, acosar a otras personas...

¿Cómo puedes evitar que suplanten tu identidad?

- **Datos personales**: Evita la difusión de tus datos personales en Internet.
- **Contraseñas seguras**: Las contraseñas deben ser fuertes, robustas y privadas. Ya sabes que cuanto más débil es la contraseña, menos tarda un o una ciberdelincuente en descifrarla.
- **Acceso a webs y enlaces**: Acceder solo a las páginas webs seguras con protocolo https://

  Asegúrate de que un enlace es seguro antes de hacer clic.
- **Correo electrónico:** Desconfía de aquellos correos electrónicos procedentes de fuentes desconocidas y fíjate en la dirección remitente.
- **Ficheros adjuntos**: No abras los ficheros adjuntos a correos sospechosos o procedentes de fuentes desconocidas. Podrían tratarse de *malware* para robar tus datos.

Es importante fijarse en la extensión de los archivos adjuntos y que se corresponda con la esperada, para evitar la instalación de *software* malicioso en el equipo, por ejemplo, mediante la ejecución de archivos con extensión .exe.

- **Descargas**: Realiza descargas utilizando solamente fuentes seguras para evitar instalar *malware* en tu equipo.
- **Ordenador compartido**: Siempre que compartas ordenador o utilices un ordenador público, asegúrate de cerrar la sesión y evitar que otras personas accedan a tus cuentas.
- **Redes Wi-Fi**: Evita el acceso a datos personales desde redes Wi-Fi públicas y accede solo aquellas que sean seguras.

¡No te dejes pescar!

¿Te imaginas que recibes un correo electrónico de alguna amistad, invitándote a hacer clic en un enlace muy interesante? ¡Cuidado! Podría tratarse de un intento de ***phishing***. El *phishing* es un método de fraude mediante el envío de correos electrónicos que busca suplantar la identidad digital de alguien para engañarte y robar tu información, tu dinero o tu reputación. También se utiliza para instalar programas maliciosos, conocidos como *malware*, en tus dispositivos.

Para lograrlo, los y las ciberdelincuentes envían correos electrónicos fraudulentos que, suplantando la identidad de otras personas, empresas u organizaciones, solicitan a la persona destinataria que acceda al enlace facilitado en el correo o descarguen algún fichero adjunto malicioso.

¿Y si me engañan por otros medios?

La misma suplantación de identidad que ocurre en el *phishing*, puede llegarte a través de otros medios diferentes del correo. Los mecanismos y formas de actuación son los mismos, pero el nombre cambia. ¡Vamos a aprenderlos!

Vishing

En este caso, el fraude se realiza a través de una **llamada telefónica**. El o la ciberdelincuente se hace pasar por alguien de tu confianza, como un banco o una empresa, y te pide que confirmes o reveles tus datos personales o bancarios, aportando otros que, generalmente, han obtenido en la red. El nombre viene de la unión de voz y *phishing*.

Smishing

En este caso, el fraude llega a la persona destinataria a través de un **SMS o mensajería instantánea** (Whatsapp, Telegram...). Se solicita que se visite un enlace falso o se llame a un número falso a través del que se comete el delito. Su nombre deriva de la combinación de SMS y *phishing*.

QRishing

En este caso, los o las delincuentes **manipulan los códigos QR** originales para que las personas usuarias accedan a sitios falsos o descarguen aplicaciones maliciosas sin darse cuenta. Uno de los sitios más habituales es la consulta de la carta de los restaurantes,

donde suelen pegar encima el código falso. Su nombre deriva de la unión de QR y *phishing*.

¡No te dejes intimidar!

Se denomina **ciberacoso** al abuso e intimidación que se lleva a cabo mediante tecnologías digitales, de forma consciente y reiterada en el tiempo. Puede ejercerse de diferentes formas en el entorno virtual tanto por personas adultas como por menores de edad.

Generalmente, el término inglés para el acoso ejercido a través de medios digitales, el ***ciberbullying***, se ha reservado para aquel ciberacoso en el que tanto la víctima como la persona acosadora son menores de edad. Mientras que el término ciberacoso engloba también aquellos casos en los que puede haber implicadas personas adultas.

Además, existen otras prácticas peligrosas a través de la red que pueden derivar en ciberacoso, que se exponen a continuación.

El ***sexting*** se define como el envío de fotos o vídeos con connotación sexual a través de cualquier dispositivo conectado a la red. Se trata de una práctica de riesgo, ya que no sabes cómo puede ser utilizado este material por otras personas con la intención de hacerte daño.

Recuerda que en el momento que compartes una imagen en la red, pierdes el control sobre ella. Además, esta imagen puede circular durante un largo tiempo en la red, llegando a viralizarse y resultando complicado llegar a eliminarla completamente. Si estas imágenes o vídeos son utilizados para obtener algo a cambio, chantajeando y amenazando a la víctima con su publicación, estamos ante un caso de **sextorsión**.

Por otro lado, existen otros riesgos similares, pero incluso más peligrosos, como es el caso del **grooming**. Ya sabes que en la red no todo el mundo es quien dice ser. En ocasiones, hay personas adultas que fingen ser menores en la red, tratando así de ganarse tu confianza, pasando después al control emocional y, finalmente, al chantaje con fines sexuales.

¡No te calles y actúa!

Por muchas medidas preventivas que tomes, estás reduciendo riesgos, pero, aun así, es posible que el ciberacoso surja en algún momento. En ese caso, es primordial que adoptes una serie de medidas:

- No borres ninguno de los mensajes recibidos, ya que pueden ser una prueba de la situación vivida.
- Comunica lo sucedido a personas adultas de tu confianza que puedan ayudarte a gestionar la situación.

- Elimina o bloquea a aquellas personas que están acosándote en redes y no continúes en contacto virtual con ellas.
- Puedes solicitar información, asesoramiento o denunciar este tipo de situación en diferentes organismos: Policía, Guardia Civil, Incibe, servicios habilitados por diferentes redes sociales...

Además, el Incibe cuenta con la siguiente línea telefónica de referencia, gratuita y confidencial, donde te indicarán cómo actuar en tu caso concreto, llamando al 017.

Desconéctate para que no te desconecten

El bienestar digital consiste en mantener un equilibrio entre la salud, tanto física como mental, y el uso de las tecnologías, evitando el uso excesivo y poco saludable.

¡Usa las tecnologías de forma inteligente! La propia tecnología puede convertirse en tu aliada, ya que te ofrece aplicaciones que permiten gestionar el uso de los dispositivos electrónicos, limitar el número de notificaciones recibidas y hacer un uso más responsable. Además, es importante que cuides tu cuerpo durante el manejo de las tecnologías y tengas en cuenta la ergonomía.

Algunos consejos:

- Planea períodos de desconexión en los que la tecnología no esté presente.
- Desactiva las notificaciones, pues lo que hacen es distraerte e interrumpirte.
- Esconde las aplicaciones más adictivas, cuanto menos te tienten, mejor.
- Cambia los colores de tu pantalla a tonos grises. Te será más fácil desconectar si es menos atractiva.
- Desconéctate como mínimo una hora antes de dormir.
- Siéntate correctamente cuando estás ante el ordenador.

No es para ti

Fake News

No todo lo que aparece publicado en Internet es cierto. Muchos contenidos se crean para generar algún tipo de beneficio, económico o ideológico, o para crear alarma social. Por tanto, debes aprender a localizar fuentes seguras y fiables de información. Existen buscadores específicos que te ayudan a obtener información rigurosa. ¿Conoces Google Académico?

También es importante que no contribuyas a la distribución de este tipo de información.

Pornografía online

Hay contenido en Internet que no es apropiado para tu edad. Es normal que sientas curiosidad, pero las respuestas debes buscarlas siempre en fuentes fiables que te ayuden a resolver tus dudas.

Debes saber que existen diferentes tipos de pornografía, y que, en algunos casos, están relacionados con un delito, como el abuso sexual o la difusión de imágenes íntimas sin consentimiento. Además, debes ser consciente de que nadie puede forzarte a ver pornografía, ni debes sentirte presionado o presionada a hacerlo, aunque tus compañeros y compañeras lo hagan.

Apuestas y juegos de azar

Muchos anuncios en redes sociales presentan las apuestas como algo divertido y carente de riesgos pero, personas que han comenzado de forma inocente a jugar en Internet, finalmente se han visto envueltas en problemas sociales, legales, económicos y de salud a causa de la ludopatía.

Retos virales peligrosos

Muchos retos virales son beneficiosos, ya que cultivan aspectos positivos, como el trabajo en equipo, la creatividad, la expresión artística, la destreza física o la digital y, por supuesto, entretienen. Pero la lista de retos peligrosos es interminable y debes saber que es muy importante no participar en ellos y no compartirlos, evitando así su propagación.

4. El reto: Clics seguros

4.1 QR: Haz tu campaña viral

¿Qué es un código QR?

Los **códigos QR** (*quick response code*) son un tipo de código de barras bidimensional que permite el acceso a información guardada en ellos simplemente escaneándolos con la cámara de un teléfono móvil u otros dispositivos habilitados. Se trata de un recurso cada vez más popular y que se ha extendido a prácticamente todos los sectores.

¿Qué hay en un código QR?

Un código QR puede contener información de diversos tipos: texto, URL, imagen, tarjeta de contacto, audio, PDF, etc., que es interpretada por el dispositivo lector como si fuera un hipervínculo.

4.2 Arte con inteligencia artificial (IA)

Como seguramente sabes, en la actualidad, se pueden **generar imágenes con inteligencia artificial** (IA), sin embargo la edad mínima requerida para usar estas plataformas es de **13 años**. Si tienes entre 13 y 18necesitas el consentimiento explícito de tus tutores legales.

En el mundo de la creación de imágenes con IA hay herramientas y recursos totalmente gratuitos.

4.3 Netiqueta

Siempre con respeto

Desde el inicio de las civilizaciones, la sociedad ha establecido normas de comportamiento para asegurar una correcta convivencia. Algunas de estas normas de comportamiento las utilizas a diario, como saludar, despedirte o dar las gracias, entre otras muchas.

Con la irrupción de las tecnologías de la información y la comunicación, más concretamente con Internet, la convivencia se traslada a espacios virtuales en los que distintas personas interaccionan sin relacionarse físicamente.

Netiqueta es un acrónimo de net (*red*) y etiqueta, y hace referencia a las normas de conducta socialmente aceptadas en Internet. La definición de netiqueta comprende normas de presentación y de comportamiento y formas de expresión aceptadas. La netiqueta también se conoce como **etiqueta digital**.

La netiqueta no está definida, no existe una ley que la regule, pero existe un consenso entre las personas usuarias de Internet para relacionarse correctamente a través de la red. Cada comunidad puede establecer sus propias normas de netiqueta, aunque las básicas podrían resumirse en las siguientes:

Es importante recordar que las normas pueden variar según el contexto y la comunidad en la que te encuentres, así que siempre es útil prestar atención a las reglas específicas de cada plataforma o grupo.