IESÁLVARO DE MENDAÑA - PONFERRADA

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

ÍNDICE

1. Introducción.

Este plan está destinado a toda la comunidad educativa del Centro, alumnado, familias y docentes, con el propósito de aportar indicaciones y consejos en el uso seguro de las Tecnologías de la Información y las Comunicaciones (TIC).

La referencia a las TIC es visible en prácticamente todos los documentos institucionales del Centro, desde la Programación General Anual (PGA), las propuestas curriculares, el Reglamento de Régimen Interior (RRI) o el Plan de Contingencia, por ello se ha considerado la importancia de priorizar la seguridad para fomentar una confianza digital.

En el apartado 7.10 del Reglamento de Régimen Interior, así como el Plan Digital o Plan TIC se explica como el IES Álvaro de Mendaña promueve acciones que fomenten el uso seguro, creativo, crítico y responsable de las TIC entre los distintos sectores de la comunidad educativa. Así mismo, somos conscientes del enorme potencial que las herramientas TIC tienen en el proceso de enseñanza y aprendizaje contribuyendo a la adquisición y desarrollo de competencias.

Para concienciar a nuestro alumnado, disponemos del Anexo I del anteriormente citado RRI con una **guía de buenas prácticas TIC para las familias** y en el Anexo II de un **decálogo de buenas prácticas contra la violencia de género en el uso de las redes sociales**.

2. Contraseñas seguras

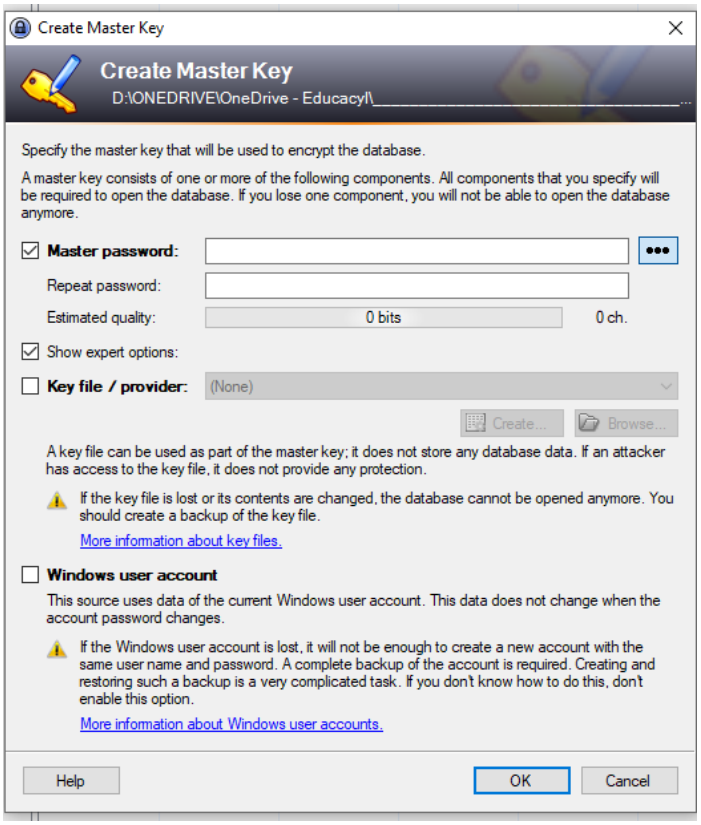
2.1. Almacén o gestores de contraseñas.

Somos conscientes de la importancia que tienen los aspectos de seguridad y privacidad en relación con las TIC. Por este motivo, insistimos en la necesidad de concienciar a toda la comunidad educativa del uso responsable y seguro de los recursos tecnológicos.

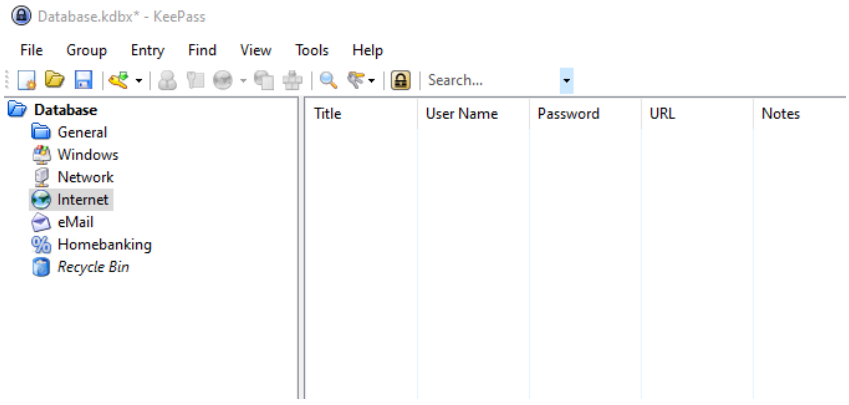
Sugerimos las siguientes recomendaciones:

- No facilitar nunca usuarios ni contraseñas de ningún tipo.
- No dejar nunca el ordenador encendido y sin bloquear si no estamos presentes. Antes de salir del aula debemos apagar el equipo. Podemos cerrar sesión con la combinación de teclas **CTRL+ALT+SUPR** y seleccionando "**Cerrar sesión**" en el menú que aparece.
- Como consejo para almacenar contraseñas, puedes usar aplicaciones de gestión de contraseñas en tu dispositivo móvil, ya sean de pago o gratuitas como KeePass.

KeePass: Es un programa gratuito para ordenadores personales que nos permite guardar en un archivo encriptado todas nuestras contraseñas. Una vez instalado el programa tendremos que decirle dónde queremos guardar ese archivo de contraseñas: **Database.kdbx**

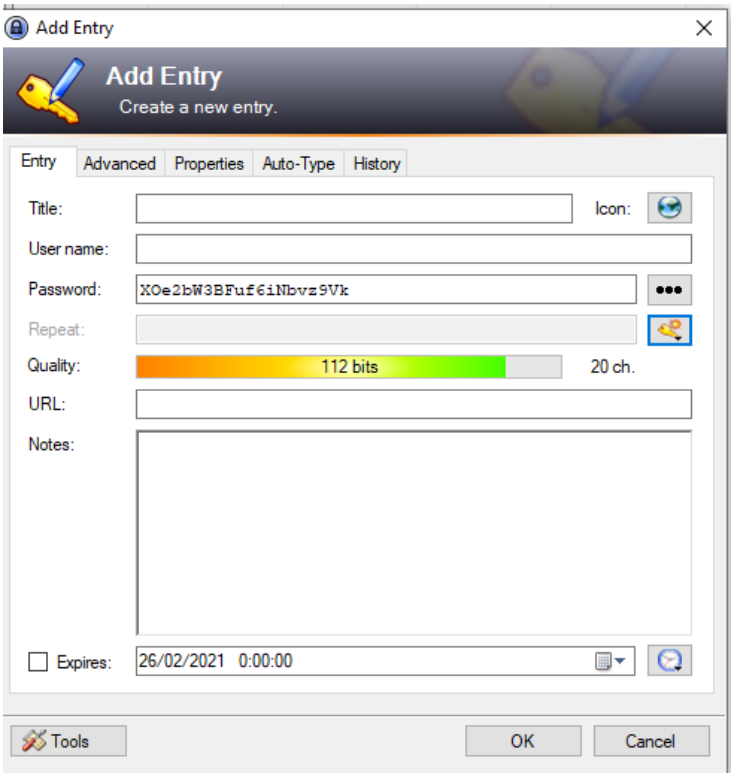


Puesto que es un archivo encriptado, podemos guardarlo en nuestra nube de OneDrive para poder importarlo después desde las aplicaciones móviles y sincronizar los contenidos.



Completaremos los datos referentes al nombre de la base de datos y finalizaremos su configuración. Una vez en la pantalla principal, seleccionaremos la categoría donde queremos añadir la contraseña y pulsaremos en 

Nos aparecerá la siguiente ventana donde introduciremos todos los datos de la clave en cuestión.



Pulsando en el botón que hay a la derecha de “Repeat” podremos generar contraseñas aleatorias para ese sitio web o aplicación.

También hay disponibles gestores para dispositivos móviles tanto Android como iOS. Se recomienda su uso para evitar pérdidas de contraseñas o repeticiones de las mismas hasta el punto de hacer muy inseguras sus cuentas.

2.2. Contraseñas seguras.

Las contraseñas personales son las que gestionamos nosotros mismos, las que podemos elegir y modificar cuando queramos. Esto conlleva que somos responsables de su custodia y nos obliga a elegir contraseñas difíciles de adivinar pero que, a la vez, sean fáciles de recordar para nosotros.

Una contraseña, para que sea realmente segura, debe estar formada, al menos, por una letra **mayúscula**, una **minúscula**, un **número** y un **símbolo** que no sea alfanumérico **(#, $, %, &, -,** _**, @,** etc.). Además, su longitud debe ser de, al menos, 8 caracteres. Por desgracia, no todos los servicios admiten contraseñas que cumplan con todas estas premisas.

Hay que evitar contraseñas sencillas como “12345678”, “11111111” o “qwerty” y fáciles de adivinar como la fecha de nuestro cumpleaños o nuestro número de teléfono. También sería conveniente evitar palabras que aparezcan en el diccionario, pues algunos virus y programas maliciosos prueban todas las palabras posibles.

No por ser tremendamente larga, una contraseña va a ser más segura y corremos el riesgo de que nos resulte difícil recordarla. Por ese mismo motivo, también debemos evitar palabras con faltas de ortografía.

Las contraseñas "*perfectas*", según expertos como Edward Snowden, son aquellas compuestas por frases absurdas que carecen de sentido pero que por hablar de cosas que conocemos o ser graciosas, nos resultan fáciles de recordar, pero difíciles de adivinar. Por ejemplo, "MigatoEnrique17_gobierna_Angola" o "margaretthatcheres110%SEXY".

3. Seguridad en ordenadores personales.

Por ordenadores personales, también conocidos como PC, entendemos cualquier ordenador, ya sea de sobremesa o portátil, destinado al uso particular de una persona.

Dicho de otra manera, son los ordenadores que se venden comercialmente, al público en general, en las tiendas. No nos referimos a los grandes ordenadores servidores que se usan en el entorno empresarial y que requieren configuraciones específicas de seguridad por parte de especialistas en informática.

Mantener seguro nuestro ordenador personal no es tan difícil como parece, solamente tenemos que seguir unas sencillas pautas.

3.1. Usuarios y contraseñas

En el centro educativo el alumnado accede a los equipos informáticos a través de su cuenta personal de educa.jcyl.es. Como se explica en el Manual TIC para alumnado y familias, la contraseña no se debe facilitar a nadie y en el caso que exista una posibilidad de vulneración, se debe reiniciar desde este enlace: https://edaplica.educa.jcyl.es/AUPO/indexRecordatorio.jsp o desde la secretaría del centro.

Para el ordenador personal que dispongan en sus domicilios, lo recomendable es crear un usuario para cada personal que acceda al mismo. De esta forma cada usuario sólo podrá acceder a sus datos y no a todos los datos del resto de usuarios. De la misma forma, cada usuario deberá tener una contraseña segura.

Los sistemas informáticos tienen dos tipos de usuarios:

Usuario administrador: este tipo permite al usuario acceder a todas las herramientas del sistema y a todos los datos del ordenador, incluidos los datos de otros usuarios, instalar y configurar programas, etc.

Usuario estándar: este tipo solamente permite al usuario acceder a sus datos, no a los de los demás y no le da acceso a herramientas avanzadas del sistema ni a poder instalar y configurar programas.

Así pues, si nuestro ordenador tiene solamente un usuario, éste deberá ser administrador para poder acceder a todas las funciones del sistema, pero si va a tener varios, es conveniente que solamente tengan cuenta de administrador aquellos usuarios que realmente lo necesiten, siendo preferible que el resto se queden como usuarios estándar.

3.2. Actualizaciones.

Todos los equipos del centro disponen de un sistema operativo en red con función cliente-servidor. Eso significa que todos los equipos están gestionados de manera remota por los servidores de la Junta de Castilla y León y por ende actualizados de manera automática e instantánea.

Como recomendación para los equipos personales domésticos, se recomienda actualizar siempre los sistemas operativos (Windows, macOS o Linux) ya que las actualizaciones suelen corregir errores del sistema y solucionar fallos de seguridad.

Para realizar las actualizaciones, es conveniente revisarlo de forma manual y estar atentos a las notificaciones que nos dé el sistema.

Además del sistema operativo, también es conveniente tener completamente actualizados todos los programas que tenemos instalados en el ordenador o, al menos, aquellos que tienen acceso a Internet o que utilizan ficheros descargados de Internet, ya que, de tener algún fallo de seguridad, pueden ser una puerta de entrada para virus y ciberataques.

En general, los programas que deberíamos tener siempre actualizados son los siguientes:

- Aplicaciones de seguridad: como antivirus, cortafuegos, antiespías, etc.
- Navegadores de Internet: como *Microsoft Edge, Google Chrome, Mozilla Firefox*, etc.
- Clientes de correo electrónico: como *Microsoft Outlook, Mozilla Thunderbird*, etc.
- Aplicaciones de descargas: como *BitTorrent, eMule*, etc.
- Aplicaciones de comunicación: como *Microsoft Teams, Discord, Slack, Whatsapp, Telegram*, etc.
- Aplicaciones ofimáticas: como *Microsoft Office, LibreOffice*, etc.

3.3. Aplicaciones de seguridad

Dada la cantidad de amenazas que pueden afectar a nuestro ordenador, es recomendable disponer de ciertos programas de seguridad que nos ayuden a protegerlo.

En sistemas operativos como macOS o Linux, este tipo de programas no son necesarios porque el propio sistema incorpora los mecanismos de seguridad necesarios y, al ser sistemas minoritarios en número de usuarios, la cantidad de amenazas para ellos es más bien escasa.

Sin embargo, en sistemas Windows, se hace imprescindible la presencia de estas aplicaciones para reforzar la seguridad, aunque desde la aparición de Windows 10, el sistema viene acompañado de las herramientas de seguridad básicas que necesitamos (en versiones anteriores de Windows, tendremos que instalarlas).

Las aplicaciones de seguridad principales que podemos necesitar son las siguientes:

- **Antivirus:** este tipo de aplicaciones nos protegen de programas maliciosos (conocidos con el nombre genérico de *malware*), como pueden ser virus, troyanos, programas espía (también llamados *spyware*), etc. Windows 11 y Windows 10 incorporan una herramienta llamada Seguridad de Windows, también conocida como *Windows Defender* que se encarga de hacer estas labores de protección. Si usamos Windows 7, esta herramienta no viene instalada por defecto, pero Microsoft permite descargarla, de forma gratuita, con el nombre de *Microsoft Security Essentials*. Con esto ya dispondremos de seguridad suficiente, pero si no nos gustan estas herramientas o preferimos otras aplicaciones más avanzadas, siempre podremos instalar algún antivirus comercial de los que existen en el mercado, sea gratuito o de pago.

- **Cortafuegos o firewall:** es un tipo de aplicación que controla el tráfico de datos que salen o entran en nuestro ordenador, procedentes de la red local y de Internet. Los cortafuegos bloquean toda comunicación no autorizada para evitar que un ciberdelincuente o un *malware* puedan acceder a nuestro ordenador desde la red. Cuando una aplicación necesita acceder a Internet, el cortafuegos nos mostrará un mensaje pidiendo permiso para dejar que la aplicación pueda hacerlo. Si aceptamos, a partir de ese momento, la aplicación tendrá siempre acceso a Internet, salvo que modifiquemos la configuración del cortafuegos. Por este motivo, es recomendable prestar atención a los avisos del cortafuegos y no dar permiso a ninguna aplicación que no conozcamos, que nos ofrezca dudas o que no necesite realmente Internet para funcionar. Todas las versiones actuales de Windows incluyen una herramienta de *firewal*l pero, si no nos gusta o preferimos tener más opciones de configuración, siempre podremos instalar alguna aplicación comercial de cortafuegos, ya sea gratuita o de pago.

- **Antiespías o antispyware:** es un tipo de aplicación que sirve para eliminar programas publicitarios (también llamados *adware*) y *spyware* que los antivirus no eliminan porque han sido instalados con nuestro consentimiento cuando instalamos otros programas y aceptamos ciertas condiciones sin fijarnos en que están marcadas o porque el programa que estamos instalando nos lo ofrecen gratuitamente a cambio de aceptarlas. Generalmente, no son programas necesarios, pero sí pueden resultar convenientes en el caso de que instalemos en nuestro ordenador muchos programas y juegos descargados de Internet. A diferencia de los antivirus y los cortafuegos, los antiespías no están funcionando todo el tiempo, en segundo plano, sino que los ejecutaremos manualmente cada cierto tiempo (una vez a la semana o una vez al mes) para hacer un chequeo del sistema y borrar aquellos elementos no deseados que vaya encontrando. Algunas de estas aplicaciones son *Malwarebytes Anti-Malware* y *Spybot Search & Destroy*, ambas de pago, pero con versiones gratuitas.

3.4. Copias de seguridad.

Para evitar una pérdida de información o datos importante en nuestro sistema debido a un fallo de *hardware* o un virus, se recomienda realizar copias de seguridad (también llamada *backup*) cada cierto tiempo.

La frecuencia con la que hagamos las copias de seguridad dependerá del uso que hagamos de los datos. Si éstos cambian con mucha frecuencia, haremos las copias cada poco tiempo (diaria o semanalmente). Si cambian poco, podemos hacerlas más de vez en cuando (mensual o trimestralmente).

Para hacer las copias de seguridad, nos bastará con tener un soporte externo donde guardar la copia, como puede ser un disco duro externo. Es conveniente que este disco duro externo se use solamente para hacer las copias y luego lo guardemos hasta la siguiente copia, ya que, si el disco permanece conectado a un equipo, es más probable que pueda sufrir también una avería y se encontrará además expuesto a que algún virus o ciberataque pueda borrar o robar las copias.

Realizar una copia de seguridad puede ser tan sencillo como copiar y pegar las carpetas de las que queramos tener copia al disco duro externo, pero también podremos hacerlo con las herramientas de *backup* que suelen tener los sistemas operativos, como el Copia de seguridad de Windows o el *Time Machine* de macOS.

Si queremos disponer de más opciones de configuración de las copias de seguridad, podemos instalar aplicaciones específicas como *Cobian Backup* o *FreeFileSync*, ambas gratuitas.

También se dispone de la opción de copia de seguridad en la nube utilizando el espacio que educa.jcyl nos proporciona con *Onedrive*.

3.5. Instalación de aplicaciones.

A la hora de instalar aplicaciones descargadas de Internet en nuestro ordenador, debemos tener en cuenta una serie de recomendaciones:

- Es preferible hacerlo desde la herramienta de “tienda de aplicaciones” que trae el sistema operativo (*Microsoft Store* en Windows, *App Store* en macOS o la tienda específica que provea nuestra distribución de Linux concreta). Se supone que las aplicaciones que se encuentran en estas tiendas han pasado por un proceso de selección que ha descartado aquellas maliciosas o fraudulentas.
- Si la aplicación que queremos instalar no se encuentra en la tienda de nuestro sistema, podemos descargarla de Internet directamente pero siempre desde la página oficial del desarrollador de esta, para evitar bajarnos versiones que puedan estar manipuladas por terceros.
- De la misma forma, debemos evitar descargar aplicaciones de sitios de descargas como *Softonic* y similares que no son los desarrolladores originales, ya que este tipo de páginas tienen fama de añadir publicidad molesta y *spyware* a los programas originales.

4. Seguridad en dispositivos móviles.

Como ya se ha comentado el uso de los dispositivos móviles dentro del centro está restringido y controlado como se detalla en el RRI. Pero hay que tener en cuenta que la responsabilidad del buen funcionamiento de este, ya que le corresponde al individuo al que pertenece.

El acceso inmediato a Internet las 24 horas del día y las posibilidades de comunicaciones a nivel mundial, provoca que se maximicen los riesgos de seguridad. Se ha convertido en un elemento imprescindible en nuestros días, por ello se explican unas pautas para reforzar la seguridad y hacer un buen uso de este.

4.1. Acceso protegido.

Para limitar el acceso a nuestros dispositivos móviles es conveniente activar el acceso protegido de los mismos, ya sea mediante contraseña, código numérico, patrón de movimiento o reconocimiento biométrico (facial, de voz o de huellas dactilares), siendo este último el más seguro.

Este acceso protegido se debe activar cada vez que bloqueamos el dispositivo e impide que alguien que intente usar el dispositivo sin permiso pueda acceder al sistema si no es el dueño de este o conoce la contraseña o código de desbloqueo. Nunca se debe revelar esta contraseña o patrón a nadie.

4.2. Actualizaciones.

Como en el caso de los ordenadores personales, el mantener actualizados nuestros dispositivos móviles es vital para reducir los riesgos de seguridad de los mismos.

Aunque nuestro dispositivo no soporte la última versión del sistema Android o iOS, cada versión de estos tiene un tiempo de soporte que va más allá de la aparición del siguiente, por lo que seguirán saliendo, durante un tiempo, mejoras de seguridad para nuestro móvil.

También como en los ordenadores personales, es recomendable configurar las actualizaciones para que se instalen de forma automática o, al menos, cuando el dispositivo esté conectado a una red wifi. De esta forma, podremos estar actualizados sin esfuerzo.

Dado que en los sistemas para dispositivos móviles, las actualizaciones de todas las aplicaciones son gestionadas por el sistema, podemos configurarlo para que se actualicen también de forma automática y así no tener que hacerlo de una en una como en los ordenadores personales.

4.3. Copias de seguridad.

Esta dependencia de los dispositivos móviles hace que sean más susceptibles a sufrir averías, golpes, pérdidas o robos, de ahí que se recomiende la realización de copias de seguridad de la información que contienen (imágenes, vídeos, números de teléfonos, notas, documentos…)

Los sistemas móviles, como Android e iOS, ofrecen la posibilidad de hacer copias de seguridad en la nube a través de Google Drive e iCloud respectivamente. Es recomendable usar estas herramientas para poder recuperar posteriormente esa copia si es necesario.

También podemos realizar la copia de seguridad en *Onedrive*, directamente en la nube desde la aplicación móvil, para poder disponer de toda la información desde cualquier dispositivo, fijo o móvil.

4.4. Instalación de apps.

Una recomendación fundamental en la instalación de aplicaciones (también llamadas *apps*), es realizarlo a través de la tienda oficial del sistema operativo (*Google Play* en Android y *App Store* en iOS). Estas *apps* pasan un cierto control de calidad y no podrán ser ofrecidas en la tienda si se trata de programas maliciosos o fraudulentos. Esto nos da una cierta garantía a la hora de instalar aplicaciones en nuestro dispositivo.

En cualquier caso, este control no es infalible, por lo que, aunque sea ofrecida por la tienda oficial, si una *app* nos ofrece dudas o consideramos que pide más permisos de los que necesitaría para funcionar, es conveniente desecharla y buscar otra más fiable para instalar.

Es recomendable realizar esporádicamente una revisión de los permisos que las aplicaciones tienen de acceso al dispositivo móvil, ya que se han dado casos como que una aplicación que sólo es una linterna solicite acceso a la agenda o incluso a la cámara de fotos.

4.5. Robo.

Cuando tratamos con dispositivos móviles, no solamente tenemos que prestar atención a la seguridad del sistema y de las *apps*, sino también a la del propio dispositivo físico, que puede sufrir golpes, lo podemos perder o nos lo pueden robar.

Para evitar esto último, podemos seguir una serie de consejos:

- Nunca perder de vista el dispositivo móvil.
- Acostumbrarse a llevarlo siempre encima y no a dejarlo en cualquier sitio.
- Nunca posar el dispositivo encima de la mesa en sitios públicos donde podamos dejarlo olvidado o alguien pueda cogerlo y salir corriendo con él.
- Activar el acceso protegido para evitar que alguien pueda desbloquear el dispositivo.
- Utilizar las opciones para encontrar el dispositivo en caso de robo o pérdida que incluyen los sistemas móviles (“Encontrar mi dispositivo de Google” en Android y “Buscar mi dispositivo” en iOS).

5. Seguridad en redes wifi

La forma de conexión habitual cuando estamos en casa, la oficina, biblioteca, comercios… sobre todo con dispositivos móviles, es a través de redes inalámbricas, más conocidas como wifi. Nos ofrecen una conexión de alta velocidad estable, disponible gracias a una conexión física de fibra óptica, ADSL, cable, conexión 4G/5G o satélite.

El objeto de este tipo de redes es ofrecer conexión a red local y a Internet de banda ancha para dispositivos móviles, ordenadores personales, televisores inteligentes y todo tipo de dispositivos y electrodomésticos capaces de conectarse a través de ellas, usando ondas similares a las de la radio, por el aire y sin necesidad de cables de comunicaciones.

La ausencia de cables facilita la movilidad y nos permite acceder a Internet desde cualquier lugar que esté dentro del alcance de la red wifi. Esto es especialmente cómodo en el hogar, ya que podremos hacerlo desde el sofá, la cama, etc.

Pero no todo son ventajas, las redes wifi tienen un inconveniente importante. Al realizar la transmisión de datos por el aire, la información puede ser interceptada de forma muy fácil por ciberatacantes, solo necesitan estar en el alcance de la red wifi (zona de cobertura) e ir recogiendo todo lo que se transmite alrededor. Por este motivo, es necesario prestar mucha atención a los mecanismos de seguridad de los que disponen las redes wifi para evitar que personas no autorizadas puedan conectarse a ellas y usarlas sin nuestro permiso o descifrar la información que se transmite a través de ellas (que la capture no lo evitaremos porque no controlamos el aire, pero sí al menos podemos lograr que no pueda leerla).

5.1. Redes wifi públicas.

Muchas instituciones públicas y comercios ofrecen acceso wifi gratuito a sus visitantes o clientes. Dado que no podemos estar seguros de que estas redes estén correctamente configuradas y bien aseguradas, la recomendación general es ser precavidos a la hora de conectarse a ellas.

Si la red wifi no está protegida con contraseña, **no debemos conectarnos a ella** en ningún caso, ya que la contraseña no solamente sirve para controlar el acceso a la red sino también para cifrar o encriptar los datos que circulan por ella. Sin la contraseña, todo lo que transmitamos estará sin cifrar y, por lo tanto, podrá ser leído por cualquiera que esté espiando la red wifi.

Si la red wifi está protegida con contraseña, al menos sabemos que los datos se van a cifrar pero aún así, resulta conveniente no usarla para transmitir datos personales o confidenciales y menos todavía bancarios, de manera que lo recomendable será limitarse a usarla para cuestiones de ocio como navegar por sitios de noticias y cosas similares y no para cuestiones de trabajo ni para hacer compras por Internet.

5.2. Redes wifi privadas.

Las redes wifi privadas son aquellas que podemos encontrar en las oficinas y centros de trabajo o en nuestra casa. La red deberá estar protegida por una contraseña que

solamente deben conocer las personas autorizadas para usarlas y que nunca se debe decir o poner al alcance de terceros.

En el caso de redes wifi empresarial como por ejemplo la que tenemos en el centro, será el personal informático de la empresa el que se encargue de configurar y asegurar esa red, así que nosotros, como alumnado, podemos conectarnos a ella con total confianza.

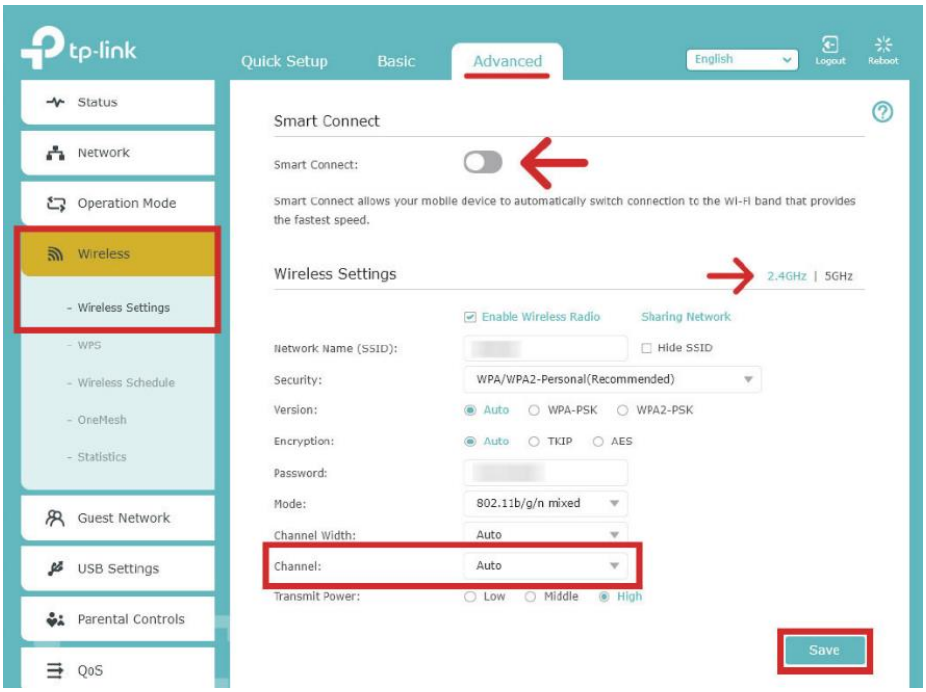
En el caso de redes wifi domésticas como la que podemos tener en nuestra casa, seremos **nosotros los responsables de configurar y asegurar la red**. Por ello, deberíamos tomarnos un poco de tiempo para leer el manual de usuario de nuestro router o punto de acceso wifi y conocer cómo podemos acceder a la configuración del mismo y cómo modificarla.

Dependiendo del tipo de router o de punto de acceso wifi de que se trate, éste puede tener más o menos opciones de configuración o estar éstas organizadas de forma diferente pero las opciones más básicas serán las mismas en todos ellos. Si se trata de un modelo popular, puede que en Internet encontremos tutoriales o incluso vídeos que nos ayuden a realizar la configuración de forma más sencilla, sobre todo si no tenemos unos grandes conocimientos de informática.

En cualquier caso, las configuraciones básicas en las que debemos fijarnos serán las siguientes:

- **Contraseña de acceso a la configuración del router o punto de acceso wifi**: suelen venir de fábrica con una contraseña genérica que será igual para todos los del mismo modelo. Por ello, es altamente recomendable que lo **primero que hagamos al entrar en la configuración sea cambiarla** por una contraseña segura.
- **SSID o nombre de la red wifi:** es el nombre que aparece cuando buscamos redes wifi desde un ordenador o dispositivo móvil. Los fabricantes suelen asignar un nombre por defecto que, en muchos casos, da pistas sobre el operador de telecomunicaciones o sobre la marca y modelo del router o punto de acceso. Esta información puede ser relevante para un posible ciberatacante, por lo que será **recomendable cambiarlo por un nombre que no dé ninguna pista sobre nosotros ni sobre nuestros dispositivos.**
- **Contraseña de la red wifi:** por defecto, los fabricantes asignan a cada router o punto de acceso una contraseña diferente que suele venir en una pegatina, debajo del dispositivo. Es altamente recomendable cambiarla de forma que sea una contraseña segura como ya se ha comentado en el apartado 2 te este Plan.
- **Tipo de seguridad o de cifrado:** establece cómo se van a cifrar los datos que se van a transmitir. Los routers o puntos de acceso más antiguos usaban el tipo WEP, pero éste ya está desfasado y los ciberatacantes saben cómo descifrarlo. Para mayor seguridad, elegiremos el tipo WPA2 (más seguro). Existe un WPA3, pero es más moderno y no todos los dispositivos móviles lo soportan.

- **Desconectar la red que no usemos:** los routers y puntos de acceso modernos ofrecen dos redes wifi a la vez en lugar de una sola. Una emite en la banda de frecuencia de 2,4 GHz y la otra en la de 5 GHz. Ésta última es más moderna y más rápida, aunque tiene menos alcance, pero no está soportada por ordenadores y dispositivos móviles antiguos, por lo que éstos deberán conectarse a la de 2,4 GHz. En el caso de que no vayamos a usar alguna de las dos redes, lo ideal es desconectarla para que no pueda usarla nadie más. También es recomendable, aunque es una opción avanzada, modificar el canal en el que se está emitiendo la señal wifi, ya que por defecto suele ser un canal en la mitad de la banda de transmisión (Canal 6 o 7).



- **Filtrado MAC:** esta opción es un poco avanzada y consiste en permitir el acceso a la red wifi solamente a una lista con aquellos dispositivos que nosotros queramos, impidiendo el acceso a cualquier otro que no esté en la lista. Para crear la lista, debemos conocer la dirección MAC de la tarjeta de red wifi de cada ordenador o dispositivo móvil que queramos incluir (el dato lo podemos encontrar en la configuración de red del sistema operativo) y copiarla en la lista de direcciones MAC de la configuración del router o punto de acceso. La dirección MAC es un número de serie que cada tarjeta de red recibe de fábrica y no existen dos iguales. Aun así, el filtrado MAC no es perfecto, ya que empiezan a aparecer técnicas capaces de falsear la dirección. También tiene el inconveniente de que, si cambiamos de dispositivo cada cierto tiempo o recibimos invitados en casa regularmente, tenemos que estar modificando la lista continuamente.

6. Seguridad en Internet.

Internet es un conjunto de redes interconectadas entre sí de forma global por todo el mundo. Se la conoce también con el nombre de Web. Internet nos facilita el acceso a un mundo amplio de conocimiento, posibilidad de comunicación y de intercambio de ideas, pero es un entorno que esconde algunas amenazas con las que debemos tener cuidado.

La mejor manera de moverse por Internet es hacerlo de forma responsable, respetando siempre a los demás internautas y prestando atención a un conjunto de medidas de seguridad básicas.

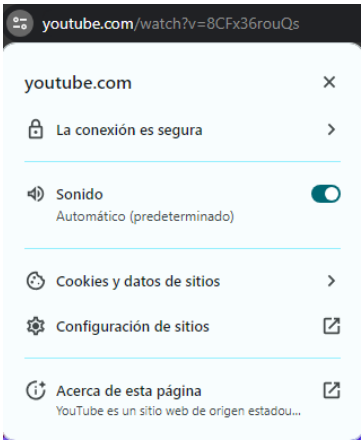
6.1. Seguridad en la navegación.

Para navegar por Internet, bien sea desde un ordenador, portátil o un dispositivo móvil o tableta, lo hacemos a través de una aplicación creada para tal efecto llamada navegador.

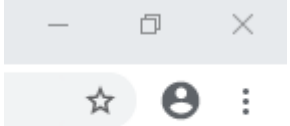
Los navegadores son capaces de entender el código de programación (HTML) y muestra su contenido y permite al usuario moverse por el mismo. Los navegadores más usados son: Google Chrome, Mozilla Firefox y Microsoft Edge, aunque en el mercado podemos encontrarnos con otros como Safari u Opera. Todos ellos son gratuitos, algunos necesitan ser instalados por el usuario y otros vienen instalados en el sistema operativo.

Las recomendaciones de seguridad en navegación por Internet:

- Mantener siempre actualizados el navegador de Internet y el antivirus.
- Revisar la configuración de seguridad y privacidad del navegador.
- Evitar visitar páginas poco éticas o delictivas.
- Descargar ficheros de los sitios originales y observar que el tipo de fichero sea el esperado.
- Fijarse siempre en las URL (direcciones de las páginas web) que visitamos para asegurarnos de que son realmente las que queremos visitar y no falsificaciones.
- Comprobar que una web es realmente segura antes de intercambiar datos personales o bancarios con ella. Buscar el candado identificativo.



- Cerrar siempre las sesiones de usuario cuando hayamos terminado de trabajar con ellas y antes de cerrar el navegador.
- Usar la navegación privada o de incógnito si no queremos dejar rastro de nuestra navegación en el equipo o dispositivo.
- Estar alerta y tratar de contrastar siempre posibles bulos, informaciones falsas o *fake news*.
- Si accedes a Internet a través de un ordenador que no es el tuyo, utiliza la opción más segura abriendo una ventana de incógnito. Para acceder desde el navegador Google Chrome



debemos pulsar en el botón que tiene tres puntos en la esquina superior derecha o pulsar a la vez Ctrl+Mayús+N. El modo incógnito nos permite navegar libremente por internet sin que el navegador guarde el historial, contraseñas o cualquier otro dato personal.

Se recomienda la visualización de los siguientes videos y juegos:

- La seguridad en Internet por Chema Alonso (4min 17s) https://www.youtube.com/watch?v=LeMGhqX3_yQ
- Conexiones Wifi gratuitas (12min 38s) https://www.youtube.com/watch?v=WY6g-KzeMNw
- Tu vida entera está online: (2min 28s) https://www.youtube.com/watch?v=k046eLzdU1o
- Juego - ¿Puedes detectar el Phishing (suplantación de identidad? https://phishingquiz.withgoogle.com/?hl=es
- Juego - Detectar URLs maliciosas https://ai.sophos.com/demos/ai-challenge-human-vs-machine/

6.2. Seguridad en el correo electrónico.

Tanto alumnado, familias como profesorado, utilizamos el correo electrónico como una de las vías de comunicación, por lo que es recomendable entender los peligros para utilizarlo de la manera lo más segura posible.

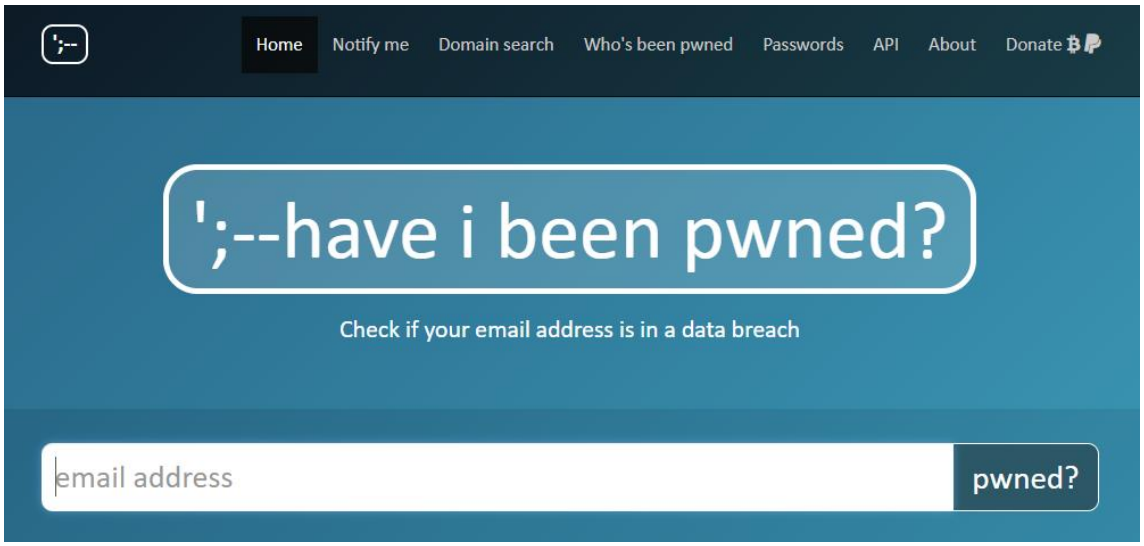
Hace ya unos años que todo el correo electrónico no deseado va directamente a una papelera llamada *Spam*. Esto es gracias a que los proveedores de correo electrónico disponen de potentes filtros antispam.

Las recomendaciones son:

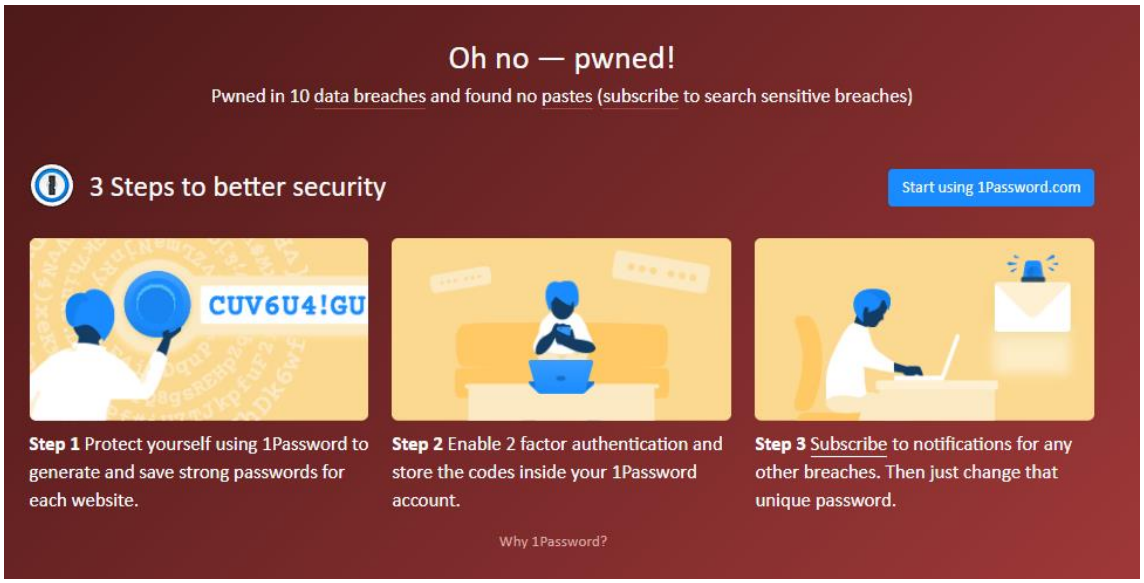
- Nunca incluir datos personales, confidenciales o bancarios: el correo electrónico es inseguro por diseño y los mensajes no van cifrados por defecto, lo que hace que cualquiera pueda leer su contenido si son interceptados.
- No responder a mensajes procedentes de remitentes ocultos o desconocidos: y, ni mucho menos, abrir los adjuntos que los acompañen. Si, además en esos correos nos intentan vender algo que no nos interesa, lo adecuado es marcar el mensaje como spam, para que los filtros antispam añadan al remitente a su "lista negra".
- No abrir adjuntos de remitentes conocidos si se trata de ficheros sospechosos o han hecho saltar al antivirus: en estos casos, lo que procede es ponerse en contacto con el remitente para informarle del hecho. Se han visto casos de facturas de compañías eléctricas o de telefonía.
- Cuidado con los mensajes fraudulentos: algunos mensajes de correo electrónico parecen legítimos porque piden ayuda para los necesitados después de una desgracia o nos prometen un empleo o un negocio redondo a cambio de dinero o de nuestros datos, pero en realidad, son fraudes. Como en el caso anterior, marcarlos como spam.

- Los bancos nunca piden información confidencial por e-mail: si recibimos un e-mail de nuestro banco solicitando nuestros datos de la cuenta corriente o de la tarjeta de crédito, podemos estar seguros de que no es nuestro banco y se trata de otro fraude. El banco nunca pediría un dato que ya debería tener y menos todavía por un medio tan inseguro como el correo electrónico.

También hay que estar muy pendiente de las noticias en cuanto a robo de datos en servidores, ya que pueden avisarte mediante un correo electrónico y pensar que es *spam*. Para ello una actividad a realizar tanto en el aula con alumnado, como en el ámbito familiar, es saber si *"Have I been pwned?"*.



Esto significa en la jerga informática, si han vulnerado los datos de alguna de nuestras cuentas. Para ello accedemos a: https://haveibeenpwned.com/ Simplemente poniendo nuestro correo electrónico nos advertirá si en algunos de los sitios donde nos hayamos registrado con ese correo, existe una brecha de seguridad.



Si en tu caso aparece que has sido vulnerado en 10 sitios (como en la imagen), automáticamente te recuerdan que debes modificar las claves de acceso de esos

sitios Web. Piensa que, aunque ciberdelincuentes roben los datos de miles de cuentas, pueden no haber hecho nada con ellos.

6.3. Identidad digital.

La identidad digital se define como el conjunto de informaciones publicadas en Internet sobre nosotros y que componen una imagen, real o imaginaria sobre nosotros mismos.

Para entender correctamente este nuevo término realizaremos un ejercicio que pretende concienciarnos de los datos que colgamos en Internet o incluso de los datos que publican sobre nosotros determinadas empresas.

Antes de realizar el ejercicio, hay que entender la siguiente frase:

"Cuando el producto es gratis, el producto eres tú"

Y es que esta frase tiene mucho que ver si somos una de esas personas que alguna vez han completado algún cuestionario, panfleto, han aceptado alguna tarjeta descuento o descuentos en factura sin haber pagado nada a cambio. Si, no estás solo en esto, nos ha pasado a todos alguna vez.

Como ya sabéis con el cambio de normativa, podemos acceder a nuestros datos personales y prohibir que las empresas los vendan a otras, pero hace unos años esto no era así. Muchas compañías de telecomunicaciones juegan vendiendo nuestros datos, que no solo son molestos con publicidad telefónica a horas intempestivas o *spam* en nuestros correos electrónicos, sino que dejan al descubierto datos personales significativos como dirección o nombre y apellidos completos.

Se recomienda realizar un ejercicio básico, en www.google.es escribe tu nombre y apellidos o sólo tu nombre y el primer apellido. De esta forma puedes comprobar cual es tu identidad digital.

Recomendaciones:

- No utilizar tu nombre y apellidos reales en redes sociales en la medida de lo posible.
- Tener los perfiles de las redes sociales privados para un mejor control de quién accede a tu información.
- Cuidado con subir fotos a redes sociales en tiempo real, ya que pueden geolocalizarnos sacando información de la misma foto y otras personas podrían aprovecharse. Por ejemplo, podrían robarnos en casa si geolocalizan una de nuestras fotografías en las que estamos de vacaciones.
- Desmarcar las casillas de consentimiento de autorización al acceso de tus datos personales, de esta forma no podrán vender tus datos y podrás darte de baja de notificaciones o publicidad.
- En las páginas Web donde aparezcan nuestros datos podemos escribir un email solicitando la eliminación de los datos personales. Gracias a la nueva normativa deberían eliminarnos.

6.4. Netiqueta y redes sociales.

Hay que ser conscientes de que Internet es un medio de comunicación público más, como la prensa, la radio o la televisión, no se trata de un medio anónimo del todo y lo que hagamos en ella puede trascender más allá de nuestros contactos conocidos, con el agravante de que, a diferencia de los medios tradicionales, puede permanecer ahí durante años y perjudicarnos en un futuro. No deberíamos comportarnos en Internet de una forma que no haríamos a través de un medio tradicional. En definitiva, comportarse con los demás como nos gustaría que los demás se portaran con nosotros y bloquear y denunciar a aquellos que tengan comportamientos incívicos con nosotros o con otros usuarios. Las redes sociales suelen establecer mecanismos de denuncia para señalar a aquellos usuarios que no se comportan con educación e infringen las normas de la propia red social.

Como guía de comportamiento, existen unas normas de buenos modales en Internet y redes sociales, conocidas como **netiqueta**. Sus reglas básicas son las siguientes:

- No olvidar nunca que las personas que leen nuestros contenidos son seres humanos con sentimientos que pueden ser lastimados. Así, no debemos faltar al respeto ni publicar material ofensivo que no mostraríamos públicamente estando esas personas presentes.
- Comportarse con educación, como lo haríamos en la vida real.
- Cuidar la ortografía en los textos y evitar escribir con todas las letras en mayúsculas, ya que eso se entiende como gritar o estar enfadado. Usar emoticonos puede ayudar a que se interprete mejor el tono en el que nos expresamos, pero no conviene tampoco abusar de ellos. En todo caso, en cada entorno en el que nos movamos nos podemos encontrar distintas formas de expresión, por lo que conviene tomarnos un tiempo para observar cómo lo hacen los demás, antes de ponernos a participar.
- Respetar siempre el tiempo y el ancho de banda de otras personas. No somos el centro del ciberespacio.
- Mostrar siempre nuestro lado bueno. Eso nos ayudará a crear una identidad digital respetable y bien considerada.
- Compartir nuestros conocimientos con la comunidad. Difundir información útil y veraz nos proporcionará una buena fama en la Red.
- Ayudar a mantener los debates en un ambiente sano y educativo. Evitar discutir de temas que no dominamos o entrar en confrontaciones inútiles. Se pueden defender nuestras opiniones en un tono cordial y sin faltar al respeto a los demás.
- Respetar la privacidad de los demás. No debemos publicar datos personales, fotos y otros contenidos que afecten a terceras personas, sin permiso de estos.
- No abusar de nuestro poder o de las ventajas que podamos tener sobre otros. Que seamos los administradores de un sitio web, no nos da derecho a tratar de imponer nuestras opiniones a los demás ni a censurar, eliminar o ridiculizar las opiniones de otros usuarios, si éstas están expresadas con educación y respeto. Como administradores, tampoco debemos hacer mal uso de los datos personales de los demás ni aprovechar nuestros privilegios para acceder a correos electrónicos u otros contenidos privados de terceros.

- Excusar los errores de otros. Todos hemos sido novatos en algún momento y cometido fallos sin querer, por lo que debemos ser tan comprensivos con los demás como nos gustaría que ellos lo fueran con nosotros.

6.5. Licencias de contenidos.

Cuando creamos nuestros propios contenidos, ya sea en forma de textos, fotos, audios, vídeos, animaciones, etc., a veces "tomamos prestados" contenidos de otras personas y copiamos y pegamos partes de sus textos, adaptamos o hacemos uso de sus materiales para hacer composiciones y montajes propios, etc. pero no siempre nos paramos a pensar si lo que estamos haciendo es legal o no.

Las licencias de contenidos en Internet son acuerdos legales que definen los términos y condiciones bajo los cuales se pueden utilizar, distribuir, modificar y compartir obras creativas en línea. Estas licencias son esenciales para proteger los derechos de autor y permitir a los creadores compartir su trabajo con el público de manera controlada. Aquí hay algunas de las licencias de contenido más comunes:

- ***Copyright*** (Derechos de autor): El copyright es automático en la mayoría de los países y otorga al creador el derecho exclusivo de reproducir, distribuir y mostrar su obra. Los demás deben obtener permiso para usar la obra, a menos que su uso esté permitido por las excepciones legales, como el uso justo.
- **Licencia *Creative Commons*:** Estas licencias ofrecen una forma flexible de gestionar los derechos de autor. Hay varias combinaciones de condiciones que los creadores pueden elegir al aplicar una licencia *Creative Commons* a su obra. Algunas permiten el uso comercial, otras no; algunas permiten la modificación, otras no. Estas licencias permiten a los creadores retener ciertos derechos mientras otorgan a otros permisos específicos.
- **Dominio público:** Si un creador renuncia a sus derechos de autor o si estos expiran, la obra pasa al dominio público. Esto significa que cualquiera puede usar, modificar y distribuir la obra sin restricciones.
- **Licencias de código abierto:** En el caso de software, las licencias de código abierto permiten a los usuarios acceder, modificar y redistribuir el código fuente. Ejemplos de licencias de código abierto incluyen la Licencia MIT, la Licencia Apache y la Licencia GPL (Licencia Pública General de GNU).
- **Licencias de software propietario:** Al contrario de las licencias de código abierto, las licencias de software propietario restringen el acceso al código fuente y establecen condiciones específicas sobre el uso y la distribución del software. Los usuarios suelen tener que pagar por el uso del software y están limitados por los términos de la licencia.

Es importante que los creadores comprendan y elijan cuidadosamente la licencia que mejor se adapte a sus necesidades y objetivos. Además, los usuarios deben respetar las condiciones establecidas por estas licencias para evitar violaciones de derechos de autor y problemas legales.

6.6. Peligros en Internet.

Por desgracia, no todos los usuarios de Internet y las redes sociales se comportan de manera cívica y siempre hay alguien que actúa de mala fe con intención de aprovecharse de los medios digitales para su propio beneficio o para perjudicar a los demás.

Los peligros más habituales que nos podemos encontrar en la red son los siguientes:

- **Tecnoadicciones:** el uso excesivo de Internet y los dispositivos móviles puede hacer que lleguemos a depender tanto de ellos que nos volvamos adictos. Esto puede ser peligroso si alcanzamos un punto en el que empecemos a descuidar nuestro trabajo, nuestros estudios o nuestras responsabilidades familiares. Para evitar este riesgo, es conveniente que organicemos nuestra jornada de tal manera que dispongamos de tiempo para cumplir con todas nuestras obligaciones, estableciendo y limitando el tiempo que dedicamos al uso de Internet. También puede derivar en adicciones en cuanto al gasto de dinero real por dinero ficticio en videojuegos o casinos online.
- **Suplantación de identidad:** para evitar que alguien pueda hacerse pasar por nosotros, es conveniente que revisemos las opciones de seguridad y privacidad de todos los servicios de Internet y redes sociales que utilicemos, limitando la visibilidad de nuestros datos personales. También debemos usar contraseñas seguras y cambiarlas cada cierto tiempo para que nadie pueda acceder a dichos sitios con nuestro usuario.
- **Ciberacoso o ciberbullying:** nunca debemos ampararnos en el cierto anonimato (que realmente no es tal) que parece que nos ofrece Internet para acosar o molestar a otras personas conocidas o desconocidas. Si somos denunciados, las fuerzas del orden pueden solicitar información a los proveedores de servicios de Internet, a los administradores de las redes sociales e incluso a nuestro operador de telecomunicaciones, con lo que tarde o temprano terminarán por dar con nosotros. Si tenemos constancia de que a alguien le están acosando, debemos intentar ayudar a la víctima o, de lo contrario, nos convertiremos en cómplices de los acosadores.
- **Sexting:** consiste en enviar fotos y vídeos de carácter sexual a través de Internet. Antes de enviar este tipo de contenidos, deberíamos pensar atentamente en el uso que podría hacer la persona que los recibe de ellos. Nunca debemos enviárselos a personas desconocidas, ya que no podemos estar seguros de cuál es su identidad real y podrían utilizarlos para subirlos a sitios de pornografía y hacernos chantaje. Si conocemos a la persona a la que se lo vamos a enviar, también deberíamos ser conscientes de que la relación que tenemos con ella puede terminarse algún día, pero los contenidos seguirán estando en su poder y podría usarlos para enseñárselos a otros con objeto de burlarse o directamente con la intención de vengarse de nosotros. Además, hay que tener en cuenta que, si las fotos o vídeos están guardados en un dispositivo móvil, éste puede ser objeto de pérdida o de robo y hacer que terminen en manos desconocidas de forma indirecta.
- **Grooming:** son técnicas que llevan a cabo personas adultas, a través de Internet, para ganarse la confianza de menores y conseguir de estos favores

de tipo sexual que pueden ir desde el envío de fotos y vídeos, hasta el tener encuentros reales. Para evitar este riesgo hay que concienciar a los menores de que es peligroso fiarse de gente a la que no se conoce en persona y que puede estar haciéndose pasar por otro de su edad para ganarse su confianza y nunca enviarles información personal, ni mucho menos fotos o vídeos personales de ningún tipo.

7. Difusión y evaluación.

La difusión de este plan se realiza a través de la página web del Centro, en el apartado recursos TIC. Además, se dará a conocer a principio de cada curso y se realizarán sesiones de difusión en el Día Internacional de Internet Segura (*Safer Internet Day*) en Febrero.

Se trabajará desde todas las asignaturas relacionadas con las TIC en las aulas de informática, reforzando y potenciando una confianza y seguridad en el uso de las TIC.

Este plan se evaluará mediante encuestas tanto a profesorado, alumnado como familias, donde se tendrán en cuenta todas las sugerencias o mejoras del mismo para los siguientes años.

https://forms.office.com/e/SgLEXxJVTq

8. Webgrafía.

- Netiqueta en Wikipedia
- Plan de Seguridad y Confianza Digital de la Junta de Castilla y León
- Internet Segura For Kids (is4k)
- Oficina de Seguridad del Internauta (OSI)
- Pantalla amigas
- Licencias Creative Commons