MERCURIO

CENTRO DE FORMACIÓN PROFESIONAL ESPECÍFICA

Centro Concertado con la Consejería de Educación de la Junta de Castilla y León

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

Curso 2020-2021

ÍNDICE

1. Introducción. 3
2. Contraseñas seguras. 3
3. Seguridad en ordenadores personales. 4
   3.1. Usuarios y contraseñas. 5
   3.2. Actualizaciones. 5
   3.3. Aplicaciones de seguridad. 6
   3.4. Copias de seguridad. 7
   3.5. Instalación de aplicaciones. 8
4. Seguridad en dispositivos móviles. 8
   4.1. Acceso protegido. 9
   4.2. Actualizaciones. 9
   4.3. Aplicaciones de seguridad. 9
   4.4. Copias de seguridad. 9
   4.5. Instalación de *apps*. 10
   4.6. Robo. 10
5. Seguridad en redes *wifi*. 11
   5.1. Redes *wifi* públicas. 11
   5.2. Redes *wifi* privadas. 12
6. Seguridad en Internet. 14
   6.1. Seguridad en la navegación. 14
   6.2. Seguridad en el correo electrónico. 16
   6.3. Seguridad en las redes sociales. 17
   6.4. Peligros en Internet. 19
7. Salud. 21

1. Introducción.

En un mundo globalizado, en el que las comunicaciones se han convertido en un eje fundamental de la civilización, los dispositivos tecnológicos están presentes en todos los aspectos de nuestra existencia.

La omnipresencia de la tecnología en nuestro modo de vida nos brinda unas oportunidades nunca vistas antes en la historia. Ahora tenemos un universo de conocimiento en el bolsillo y podemos acceder a contenidos de cualquier tipo desde cualquier lugar del mundo.

Estas herramientas, como cualquier otra, si son bien utilizadas, pueden proporcionarnos soluciones útiles para nuestro trabajo o nuestros estudios, actividades de ocio, oportunidades de negocio, etc. Pero también, mal utilizadas, pueden ser una fuente de problemas tanto laborales como personales.

Este plan está dirigido a toda la comunidad educativa del entorno del Centro Mercurio y tiene como propósito el aportar indicaciones y consejos para el uso seguro de las Tecnologías de la Información y la Comunicación (TIC). El objetivo es poder disfrutar de las ventajas que nos ofrecen las nuevas tecnologías, minimizando los inconvenientes que nos pueda acarrear el uso de las mismas.

2. Contraseñas seguras.

El principal elemento de seguridad que manejamos actualmente es el uso de contraseñas, tanto para el acceso a equipos informáticos como a servicios en Internet.

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 por un mínimo de 8 caracteres, entre los cuales debe haber, por lo menos:

- Una letra mayúscula.
- Una letra minúscula.
- Un número.
- Un carácter no alfanumérico (#, $, %, &, -, _, @, etc.)

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".

También es conveniente no usar siempre la misma contraseña en todos los sitios. Lo mejor es tener una diferente para cada servicio o, al menos, variaciones de la misma que sigan las recomendaciones de seguridad y que sean difíciles de adivinar.

El tener varias contraseñas puede hacer que sea complicado recordarlas todas o que las recordemos pero no tengamos claro a qué sitio correspondía cada una.

Para ello, se hace necesario anotarlas en algún lugar, pero ese lugar nunca debe ser un objeto físico que alguien pueda ver como libretas o post-it y, menos todavía, dejarlos pegados a la pantalla del ordenador o en sus alrededores. Tampoco es conveniente anotarlas en ficheros de texto en el propio ordenador, ya que éstos no están cifrados y, por lo tanto, si un ciberdelincuente se hace con el control del equipo, podría tener acceso a ellas.

Lo mejor para guardar las contraseñas es utilizar un programa gestor de contraseñas. Este tipo de programas nos permite almacenar nuestras contraseñas en un fichero encriptado, protegido por una contraseña maestra que pondremos nosotros y que nunca debemos olvidar. De esta forma, solamente tenemos que recordar siempre la contraseña maestra, ya que las demás las podemos ver abriendo el fichero.

Algunos de estos programas son:

- **Keepass** (https://keepass.info): y otros derivados de él (ver *Downloads* en la propia página de Keepass). Se trata de un programa de software libre, gratuito y multiplataforma que permite almacenar contraseñas en nuestro ordenador o teléfono móvil.
- **Bitwarden** (https://bitwarden.com) y **LastPass** (https://www.lastpass.com): son programas para almacenar contraseñas en la nube. Aunque son programas de pago, tienen versiones gratuitas con ciertas limitaciones.

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.

Si el ordenador va a ser utilizado por distintas personas, lo mejor es crear una cuenta de usuario para cada una de ellas. De esta forma, cada usuario podrá acceder solamente a sus datos y no a los del resto y personalizar el escritorio a su gusto.

Es conveniente que cada usuario proteja su cuenta con una contraseña segura, aunque el equipo tenga solamente un usuario, para que si alguien intenta usar el equipo sin permiso, no pueda acceder al sistema.

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.

Sea cual sea el sistema operativo que use nuestro ordenador (Windows, macOS o Linux), tenerlo siempre actualizado es algo vital para la seguridad del equipo, ya que las actualizaciones suelen corregir errores del sistema y solucionar fallos de seguridad.

Por ello, es conveniente comprobar que el sistema está configurado para recibir las actualizaciones de forma automática y, de esta forma, conseguiremos que esté siempre al día sin ningún esfuerzo por nuestra parte. Aun así, es conveniente revisar de vez en cuando las actualizaciones de forma manual y estar atentos a los avisos que nos dé el sistema, sobre el estado de las actualizaciones.

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 10 incorpora 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 firewall 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.

Por mucho cuidado que tengamos con nuestro ordenador, siempre pueden ocurrir cosas ajenas a nuestra voluntad, algunas de las cuales no podemos prevenir como, por ejemplo, una avería del equipo.

Para evitar que alguna desgracia en nuestro ordenador pueda hacer que perdamos datos que sean importantes para nosotros, es conveniente hacer copia de seguridad (también llamada *backup*) de estos datos 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 (diariamente o semanalmente). Si cambian poco, podemos hacerlas más de vez en cuando (mensualmente 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.

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 la misma, 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.

Los dispositivos móviles se han convertido en un elemento imprescindible en nuestra vida diaria. *Smartphones* y *tablets* son ya un complemento de nuestra persona como puede ser la ropa o el calzado y no vamos a ningún sitio sin nuestro dispositivo.

El acceso inmediato a Internet y las posibilidades de comunicación que ofrecen, nos mantienen conectados las 24 horas del día pero también introducen una serie de riesgos de seguridad que debemos tener muy en cuenta y que podemos minimizar si seguimos una serie de sencillas indicaciones.

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 éste 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 del mismo o conoce la contraseña o código de desbloqueo.

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 los mismos 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. Aplicaciones de seguridad.

También existen aplicaciones de seguridad como antivirus y antiespías para sistemas móviles pero, dado que son sistemas muy cerrados, limitan mucho lo que el usuario puede hacer con el dispositivo y las aplicaciones se descargan desde la tienda oficial del sistema, donde habrán pasado un control de calidad para evitar aplicaciones maliciosas o fraudulentas, el uso de este tipo de programas no se estima necesario.

Es más, tener aplicaciones de seguridad en el móvil ralentizará y hará bajar el rendimiento del sistema y de la batería, a cambio de mejorar poco o nada la seguridad, por lo que no se recomienda usarlas salvo motivos muy concretos.

4.4. Copias de seguridad.

Al igual que con los ordenadores personales, las copias de seguridad de nuestros datos móviles nos evitará disgustos si el dispositivo sufre algún percance.

En el caso de dispositivos móviles, la copia de seguridad es de suprema importancia ya que son más susceptibles de sufrir averías, golpes, pérdidas y robos.

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

Apple ofrece también la posibilidad de hacer una copia de seguridad local en nuestro ordenador a través de la aplicación **iTunes** en Windows y de **Finder** en macOS.

4.5. Instalación de *apps*.

En los sistemas móviles, la instalación de aplicaciones (también llamadas ***apps***) se realiza a través de la tienda de aplicaciones oficial del sistema (**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.

Algunos usuarios de dispositivos móviles aplican lo que en el argot informático se denomina técnicas de ***rooting*** o ***rooteo*** en los sistemas Android y ***jailbreak*** en los sistemas iOS. Estas técnicas consisten en saltarse las limitaciones de los sistemas móviles impuestas por los fabricantes de dispositivos o por los operadores de comunicaciones, con el fin de obtener el control total del sistema para cambiar configuraciones ocultas o instalar *apps* de fuera de la tienda oficial.

No es recomendable hacer *rooteo* o *jailbreak* de un dispositivo móvil si no se tienen los conocimientos informáticos necesarios, ya que un dispositivo así manipulado resulta más vulnerable a los fallos de sistema, al *malware* y a los ciberataques.

4.6. 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*.

Desde hace algunos años, con el auge de los dispositivos móviles, podemos encontrar redes inalámbricas, también llamadas redes *wifi*, en las casas, oficinas, comercios, bibliotecas… prácticamente nos rodean por todas partes.

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.

Además, la velocidad de las redes *wifi* ha evolucionado tanto que ya no tiene nada que envidiar a las redes móviles de los operadores de telecomunicaciones e incluso a muchas redes cableadas. Esto hace que sea una forma de conexión muy usada por los dispositivos móviles, ya que nos permite ahorrar "megas" de nuestra tarifa de telefonía móvil.

Pero no todo son ventajas, las redes *wifi* tienen el inconveniente de que al transmitir los datos por el aire, la información puede ser interceptada de forma muy fácil, ya que no hay que "pinchar" ningún cable. A un ciberatacante le basta con estar en el alcance de la red *wifi* 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.

Estas redes son de uso exclusivo de los trabajadores de la empresa, en caso de que se trate de una red *wifi* empresarial o de uso personal si es una red *wifi* doméstica. En ambos casos, 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 tener una red *wifi* empresarial en el trabajo, será el personal informático de la empresa el que se encargue de configurar y asegurar esa red, así que nosotros, como empleados, podemos conectarnos a ella con total confianza.

En el caso de tener una red *wifi* doméstica 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 conveniente 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. En algunos casos puede ser útil elegir un nombre que haga pensar que esa red está siendo monitorizada por alguna compañía (por ejemplo "wifipruebas", "wifitest", "wifitemporal" o similares). De esta forma, un ciberatacante no muy experimentado puede decidir que es mejor no intentar atacar esa red, por si acaso.

- **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 aparato. Se sabe que algunos *hackers* han logrado averiguar cómo generan las contraseñas ciertos fabricantes, por lo que será adecuado cambiar la contraseña que trae por una contraseña segura que elijamos.

- **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 WPA o el WPA2 (más seguro). Existe un WPA3 pero es más moderno y no todos los dispositivos móviles lo soportan.

- **Potencia de la emisión:** por defecto, el *router* o punto de acceso emite al 100% de su potencia pero si vamos a usar los dispositivos muy cerca de él, podemos reducir el porcentaje de potencia (siempre que no perdamos mucha velocidad de conexión) con el fin de que se reduzca el alcance de la red *wifi* y de esta manera, evitar que la señal llegue demasiado lejos de nuestra casa y obligar a un hipotético ciberatacante a estar muy cerca de nosotros para poder actuar.

- **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.

- **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 *hacker* capaces de falsear la dirección de una tarjeta y hacerla pasar por otra, pero puede aportar un elemento de seguridad más que junto con los otros, refuerce la seguridad. 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 nos ofrece un maravilloso mundo de conocimiento y de posibilidades de comunicación y de intercambio de ideas pero también es un entorno que esconde algunas amenazas con las que debemos tener cuidado.

La mejor manera de moverse por Internet con seguridad 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 usaremos unas aplicaciones creadas para tal fin llamadas, como no podría ser de otra manera, navegadores de Internet.

La función de los navegadores es cargar las páginas web que les vamos solicitando y permitir movernos por los contenidos de las mismas.

Los navegadores más usados son **Google Chrome**, **Mozilla Firefox** y **Microsoft Edge**, aunque existen en el mercado muchos más que podemos utilizar. Todos ellos son gratuitos pero mientras que algunos como Edge vienen junto con el sistema operativo, otros deben ser descargados e instalados por el usuario.

Como vimos anteriormente, la seguridad en la navegación debe empezar por tener nuestro navegador siempre actualizado, dado que es nuestra puerta al exterior y, por tanto, posible objetivo de ciberataques.

Aunque los navegadores ya traen una configuración por defecto suficientemente segura, nunca estaría de más revisar las opciones de configuración, aprender en qué consisten y modificar aquellas que estimemos oportuno para personalizar la seguridad y la privacidad.

Si tenemos nuestro navegador y nuestro antivirus actualizados y bien configurados, el simple hecho de cargar una página web no debería suponer ningún riesgo, aunque debemos tener en cuenta que ciertas páginas que tienen un buen "gancho" para atraer visitas pueden esconder "sorpresas" en la propia página o en los contenidos de descargas. Estas páginas suelen ser aquellas que tienen que ver con actividades poco éticas o directamente delictivas como, por ejemplo, páginas de descargas de materiales piratas, de pornografía o las que prometen enseñarnos a *hackear* cuentas de correo electrónico o de Facebook (un auténtico *hacker* no se dedica a hacer eso).

En cuanto a las descargas, recordemos que siempre debemos descargar aplicaciones desde la web oficial del desarrollador. También debemos fijarnos en las extensiones de los ficheros que

nos descargamos. Si nos ofrecen descargar un audio o un vídeo y el fichero resulta tener la extensión *.exe* propia de los programas, tengamos por seguro que no va a salir de ahí nada bueno y no lo descarguemos.

Donde sí deberemos prestar especial atención es en las páginas web en las que tengamos que intercambiar datos personales o bancarios, como pueden ser los sitios de la Administración o las tiendas de compras *online*. Siempre debemos fijarnos en la URL o dirección de la página web para saber si realmente es el sitio que esperábamos o es una falsificación de la página original. Si tenemos dudas, lo mejor es informarnos buscando en Internet y, si seguimos sin tenerlo claro, descartar la página.

También debemos fijarnos en si es una página segura o no antes de poner ningún dato personal o bancario en ella. Para saberlo, miramos si a la izquierda de la URL o dirección de la página web aparece un candado cerrado. Si aparece, quiere decir que la página es segura y que todos los datos que intercambiemos con ella estarán cifrados (independientemente de si nuestra conexión a Internet es por cable o por *wifi*). Si no aparece el candado o éste se muestra abierto, tachado o en rojo, quiere decir que la página no es segura del todo y debemos evitar enviarle datos confidenciales.

Si se trata de sitios web en los que nos hemos identificado con una cuenta de usuario, nunca debemos olvidar cerrar la sesión al terminar de trabajar con ella. No basta con cerrar el navegador sin más porque, en muchos casos, el sitio web mantiene la sesión abierta durante algún tiempo y, si el ordenador o dispositivo que hemos utilizado es público o de otra persona, cabe la posibilidad de que el siguiente usuario acceda al sitio web y se encuentre con nuestra sesión abierta, lo que le da la potestad de manipularla a su antojo con fines maliciosos contra nosotros o contra otros, haciéndose pasar por nosotros.

Además de seguir todos estos consejos, desde hace algunos años, los navegadores incluyen un modo de navegación llamado **navegación privada o de incógnito** que nos permite navegar sin que quede ningún dato guardado en el equipo o dispositivo y que puede sernos útil si estamos usando un ordenador público o que no sea el nuestro y no queremos que se guarde el historial de las páginas que hemos visitado. En el modo de navegación privada, también podemos abrir, a la vez, varias sesiones del mismo servicio con usuarios distintos (p. ej.: dos cuentas de correo distintas del mismo proveedor, dos cuentas de Facebook a la vez, etc.). Al salir del modo privado, desaparecerá toda evidencia de nuestra navegación.

Por último, es necesario tomar conciencia de una de las últimas problemáticas que ha surgido en Internet en los últimos años: la información falsa. Datos manipulados, bulos, *fake news*, etc. son, por desgracia, el pan nuestro de cada día en la Red.

Para evitar caer en el engaño de este tipo de desinformación, resulta útil indagar sobre ella, buscando en la propia Internet y tratar de localizar lo siguiente:

- **Origen:** de dónde vienen esos datos, cuál es la fuente original donde han aparecido.
- **Autor:** quién es el autor de esos contenidos o si éstos han aparecido de forma anónima.

- **Referencia:** si se trata de una opinión personal no contrastable o está basada en información fiable que se puede comprobar.
- **Vigencia:** si se trata de algo nuevo o se está intentando hacer pasar por actuales cosas del pasado que no son aplicables al momento presente.
- **Comprobación:** si esos datos son refutados o desmentidos en otros medios de comunicación reconocidos.

Como conclusión, vamos a resumir brevemente las recomendaciones y consejos para una navegación segura de las que hemos hablado en este apartado:

- 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 o 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*.

6.2. Seguridad en el correo electrónico.

Ya han pasado, afortunadamente, los tiempos en los que uno abría el e-mail y todo eran mensajes de publicidad no deseada (también llamado *spam*) y ficheros adjuntos maliciosos.

Los proveedores de correo electrónico actuales disponen de potentes filtros *antispam* y ya no permiten adjuntar ficheros que contengan código ejecutable, de tal forma que ahora el *spam* y los adjuntos maliciosos son algo difícil de ver.

Aún así, el correo electrónico no está exento de peligros y conviene tener en cuenta algunas recomendaciones sobre él:

- **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.

- **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.

6.3. Seguridad en las redes sociales.

Las redes sociales son el banderín de enganche de la llamada Web 2.0, una nueva Internet más social que se ha convertido en una parte importante de la vida de muchas personas. En algunos casos, quizá demasiado importante.

Debemos aprender a diferenciar entre nuestro "yo real" y el "yo digital" (conocido como **identidad digital**) y evitar transmitir públicamente demasiada información personal nuestra que luego pueda ser manipulada o utilizada de forma maliciosa por otras personas contra nosotros o contra terceros, haciéndose pasar por nosotros. Habremos de ser cuidadosos y pensar con atención antes de decidirnos a subir datos personales, fotos privadas, etc.

También es muy importante cuidar nuestra identidad digital ya que establece la imagen de nosotros que proyectamos hacia los demás en público. Nunca debemos usar las redes sociales para faltar al respeto, insultar o subir contenidos ofensivos para los demás, puesto que hacerlo puede dañar seriamente nuestra imagen en el presente y en el futuro.

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.

La netiqueta en Internet

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

1) 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.
2) Comportarse con educación, como lo haríamos en la vida real.
3) 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.
4) Respetar siempre el tiempo y el ancho de banda de otras personas. No somos el centro del ciberespacio.
5) Mostrar siempre nuestro lado bueno. Eso nos ayudará a crear una identidad digital respetable y bien considerada.
6) Compartir nuestros conocimientos con la comunidad. Difundir información útil y veraz nos proporcionará una buena fama en la Red.
7) 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.
8) Respetar la privacidad de los demás. No debemos publicar datos personales, fotos y otros contenidos que afecten a terceras personas, sin permiso de los mismos.
9) 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.
10) 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.

Las 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.

Si solamente los cogemos para crear contenidos de uso personal, no hay ningún inconveniente pero si queremos que esos contenidos que creamos se hagan públicos, esta forma de actuar puede acarrearnos problemas si el autor original nos denuncia por violación de la licencia de uso de sus contenidos.

Para evitar esto, conviene que nos informemos sobre el funcionamiento de las licencias de uso en Internet. Eso nos ayudará tanto a saber cómo podemos usar los contenidos de otros como a licenciar los nuestros propios.

Por lo general, los contenidos en Internet suelen emplear dos tipos de licencias: el **copyright** y las licencias Creative Commons. Conviene que dediquemos un rato a informarnos de en qué consisten éstas últimas.

Si un contenido está licenciado con copyright, no podrá ser utilizado de ninguna forma sin pedir permiso expresamente a su creador.

Si un contenido está licenciado con alguna de las licencias Creative Commons, tendremos que mirar de cuál de ellas se trata para saber qué podemos hacer o no con ese contenido sin tener que pedir permiso al creador original.

Como conclusión, vamos a resumir brevemente las recomendaciones y consejos para un uso seguro de las redes sociales que hemos visto en este apartado:

- Comportarse siempre con educación y respeto. Tratar a los demás como nos gustaría que nos trataran a nosotros.
- Cuidar nuestra identidad digital para crearnos una buena fama en Internet.
- Respetar la privacidad de los demás, evitando difundir datos personales o fotos de otros sin su permiso.
- Denunciar mediante las herramientas que proporcionan las redes sociales a aquellos usuarios que no respetan a los demás o incumplen las normas de la propia red social.
- Cumplir siempre las normas de netiqueta y las específicas del sitio web o la red social en la que estemos participando.
- Respetar las licencias de uso de los contenidos que otros publican en Internet, a la hora de utilizarlos como base para nuestros propios contenidos.

6.4. 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.

- **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 éstos 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. Salud.

Aunque los problemas de salud no están directamente relacionados con la seguridad en el uso de las TIC, estimamos conveniente dedicar un apartado a los riesgos que puede suponer para el cuerpo el uso excesivo de ordenadores y dispositivos móviles.

Los principales de estos riesgos son:

- **Problemas visuales:** derivados de la cantidad excesiva de horas delante de una pantalla. Para evitarlos, se recomienda tener la pantalla a una distancia adecuada (ni muy cerca ni muy lejos) y retirar la vista de la pantalla 5 ó 10 minutos por cada hora de uso.

- **Problemas musculares:** éstos pueden derivarse de mantener una postura incorrecta mientras se está usando el ordenador o dispositivo o de mantener una postura correcta pero durante demasiado tiempo. En el primer caso, se recomienda sentarse siempre en un asiento cómodo, con la espalda bien apoyada en el respaldo y situado a una altura que permita que las piernas mantengan un ángulo de aproximadamente 90 grados con respecto al suelo y los brazos otro también de aproximadamente 90 grados con respecto a la mesa. En cuanto al segundo caso, siempre es recomendable hacer pausas cada cierto tiempo en las que nos levantemos y estiremos las piernas un rato o hagamos algo de ejercicio. Para ayudarnos a realizar las pausas, tanto visuales como posturales, podemos usar un programa como Workrave que sirve para "invitarnos" a hacer una pausa cada cierto tiempo, bloqueando el teclado y el ratón hasta que pase el tiempo establecido para el descanso. Además, nos propone mientras tanto realizar unos pequeños ejercicios de estiramiento para relajar los músculos. Esta aplicación es libre, gratuita y se encuentra disponible para sistemas Windows y Linux.

- **Síndrome del túnel carpiano:** afecta a los nervios de la muñeca y provoca entumecimiento, hormigueo, debilidad e incluso dolor. Esta enfermedad puede estar causada por el uso repetitivo y excesivo del ratón del ordenador. Para evitarla, se aconseja apoyar siempre el antebrazo en la mesa a la hora de manejar el ratón, usar una alfombrilla con almohadilla para la muñeca y descansar de vez en cuando.