Módulo 4. Seguridad

4.1. Protección de dispositivos

4.1.1. Amenazas en Internet

- Principales amenazas en Internet

"Contenido extra - Seminario ""Uso seguro de Internet: Precauciones y métodos de protección" "Publicado en Autoformación"

4.1.2. Mantén tus dispositivos protegidos

- Medidas básicas de protección
- Medidas específicas para dispositivos móviles

El vídeo: "Contenido extra - Seminario ""Seminario online ""Herramientas de Control parental" "Publicado en Autoformación" pasa al 4.1.3.

4.1.3. Amplía la seguridad de las aplicaciones y servicios

- Protege tus cuentas con doble factor de autenticación
- Cortafuegos y herramientas de control de navegación

"Contenido extra - Seminario ""Seminario online ""Herramientas de Control parental" "Publicado en Autoformación"

4.1.4. Protege tu conexión wifi

- Seguridad en tu wifi

4.1.1. Amenazas en Internet

- Principales amenazas en Internet

Son multitud las amenazas que podemos encontrar al navegar por Internet y la ciberseguridad abarca muchos conceptos que debemos tener claros si queremos hacer un uso seguro de la tecnología tanto en nuestra vida personal como en entornos laborales.

Para consultas y dudas acerca de Ciberseguridad existe el 017 del Incibe, una línea de ayuda con la que se puede contactar a través de WhatsApp, Telegram o por teléfono y que está disponible los 365 días del año de 9 de la mañana a 9 de la noche.

Además de herramientas como el 017, el disponer de conocimientos sobre Ciberseguridad es imprescindible para estar protegidos en el mundo digital en el que nos movemos.
A continuación, vamos a comentar algunos de los peligros que existen para poder prevenirlos.

Con el término *malware* se conoce de forma genérica a todos aquellos programas diseñados para provocar un daño o acción maliciosa en un dispositivo. Virus, troyanos, *ransomware adware*, *keyloggers* o *rootkits*, entre otros, no son más que distintos tipos de *malware*.

Contra estas infecciones encontraremos “vacunas” o remedios antimalware gracias a la tecnología. También podremos contrarrestar su efecto conociendo las técnicas de ingeniería social que utilizan los ciberdelincuentes para infectarnos y estando alerta sobre las campañas para su distribución. Para enfrentarnos a estas infecciones tenemos que conocer con más detalle cómo ocurren estos incidentes de seguridad, cómo evitar ser víctimas y qué hacer en caso de que ocurran.

El *malware* hace referencia a los programas diseñados para instalarse de forma no autorizada en los dispositivos de las víctimas.

Es necesario diferenciar llegados a este punto entre dos términos: hacker y cracker. Los dos términos hacen referencia a personas que tienen nociones avanzadas sobre informática, pero sus ideas son completamente distintas.

Los hackers tienen un código ético que no poseen los crackers. El propósito de un cracker informático es romper la seguridad de las computadoras y las redes. Es una actividad ilegal. Hacen uso de su conocimiento para obtener beneficios personales y violar la seguridad en todas las redes.

4.1.2. Mantén tus dispositivos protegidos

- **Medidas básicas de protección**

La cantidad de información que almacenamos en nuestros dispositivos y el acceso a diferentes servicios a través de los mismos, hace imprescindible que los protejamos de las principales amenazas de las que pueden ser objeto como, por ejemplo: malware o software malicioso (entre los que se encuentran los virus informáticos), accesos no autorizados a cuentas o servicios en los que estemos dados de alta y un largo etcétera.

Por ello, vamos a hablar a continuación de algunas de las medidas de protección a tener en cuenta como:

- **Uso de contraseñas**. Utiliza contraseñas fuertes o robustas para acceder a dispositivos, correo electrónico y demás plataformas online, es recomendable que sean diferentes en función al servicio que utilicemos. Pero… ¿cómo debe ser una contraseña para que se considere fuerte o robusta? Pues que al menos

contenga 8 caracteres y combinarlos entre mayúsculas, minúsculas, letras, números y algún carácter especial como puede ser el símbolo del dólar, la almohadilla, etc.

Además de tener en cuenta el que sean seguras, es recomendable utilizar contraseñas diferentes en función a cada servicio y si esto te supone un problema a la hora de recordar cada una puedes usar un gestor de contraseñas como LastPass. Este gestor dispone de una versión gratuita te permitirá guardar las diferentes contraseñas de los servicios que utilices pero solo será necesario que recuerdes la contraseña con la que te hayas creado la cuenta en el mismo.

- **Instalación y activación de antivirus**. Además de tener precaución con las descargas que hacemos y en el caso de programas y apps hacerlo siempre desde las tiendas oficiales, es necesario proteger nuestros dispositivos teniendo instalado y activado en los mismos un Antivirus. Lo que protegerá de posibles entradas de malware o software malicioso que son utilizados con múltiples funcionalidades como: extraer datos personales o contraseña para acceder a cuentas bancarias o bloquear dispositivos.

- **Mantener los dispositivos limpios y actualizados**. En este punto nos referimos a debemos mantenerlos limpios de software obsoleto, ficheros inútiles y errores que puedan aparecer en los mismos. Así también, es imprescindible que los mantengamos actualizados en cuanto al sistema operativo que tenga instalado como a las nuevas versiones de programas para que no solo tengamos nuevas funcionalidades, sino también para tapar posibles problemas de “agujeros de seguridad” que se hayan detectado en versiones anteriores.

- **Acceso seguro** a los diferentes dispositivos que manejamos. Ya sea a través de contraseñas según el usuario para abrir su sesión en ordenadores o un

patrón de bloqueo de pantalla o código numérico en, por ejemplo, teléfonos inteligentes, es imprescindible que el acceso a nuestros dispositivos esté restringido en caso de pérdida o robo de los mismos o si alguien intenta acceder a los mismos sin nuestro permiso.

- **Realización de copias de seguridad** de la información. Para evitar perder la información almacenada en nuestros dispositivos, un buen hábito es el de realizar copias de seguridad periódicas y así disponer de ella aunque surja algún imprevisto. Con Google Drive podemos hacer copias en ordenadores y, por ejemplo, para dispositivos móviles que utilicen sistema operativo Android, se puede configurar una copia accediendo a la configuración del mismo y en cuentas e indicar la cuenta de Google a la que queremos que se asocie la copia de seguridad para tener nuestra información guardada en dicho servicio.

- **Tener especial precaución con las descargas** que realicemos en nuestros dispositivos. Los ataques de ransomware, en muchas ocasiones proceden de alguna descarga que hacemos pensando que lo que vamos a descargar es, por ejemplo, una película. El ransomware afecta a un equipo cifrando y bloqueando el contenido del dispositivo y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado ransomware como WannaCry o Cryptolocker, y como ejemplo puede que te suene el famoso virus que simulaba venir de la Policía. Para evitarlo, debemos asegurarnos que todo el software que usamos en nuestros dispositivos está actualizado, incluyendo el sistema operativo, el navegador y cualquier complemento que usemos en la barra de herramientas. Para eliminarlo, los programas antivirus suelen incluir su detección y eliminación entre sus opciones. En el contenido del curso te indicamos algunos enlaces para la descarga de herramientas gratuitas de anti-ransomware para eliminarlo para eliminar los virus de ransomware y descifrar cualquier archivo que se haya cifrado durante el ataque.

- **Manejo de herramientas de localización** de dispositivos. En el caso de dispositivos móviles, puedes usar aplicaciones de localización que además te permiten bloquear el dispositivo o borrar la información almacenada aunque el mismo no se encuentre en tus manos. Un ejemplo de este tipo de herramientas de seguridad es el servicio gratuito que ofrece Google de “Encuentra tu móvil”. Con él podrás gestionar diferentes dispositivos y asociarlos a tu cuenta de Google para poder localizarlos y conocer su actividad en caso necesario. Accede a este servicio desde myaccount.google.com y en el apartado de seguridad verás la opción de “Tus dispositivos” para asociar los dispositivos que desees a este servicio.

Puedes consultar más recomendaciones sobre protección de dispositivos en la Guía “Privacidad y seguridad en Internet” que pone a tu disposición el INCIBE, la Agencia Española de Protección de Datos y la OSI.

Debemos tener presentes todas las recomendaciones comentadas y sobre todo que la precaución y el sentido común serán ¡tu herramienta de seguridad más importante!

● Medidas específicas para dispositivos móviles

Puede que no lo parezca, pero los teléfonos actuales son ordenadores en miniatura igual de vulnerables a los ataques de malware. El malware tiene como objetivo aprovechar las debilidades de la comunicación móvil mediante redes Wi-Fi, mensajería de texto y navegadores o sistemas operativos.

En estos dispositivos móviles se almacena mucha información, acceso a cuentas de redes sociales, correo electrónico, imágenes y todo tipo de datos. Por ello, es fundamental que conozcamos que existe malware específico para dispositivos móviles.

Entre las medidas que se recomienda seguir para mejorar la seguridad móvil estarían:

- **Crear una contraseña segura**. Ya sea a base de un PIN de bloqueo o de un patrón en la pantalla para que no se pueda desbloquear directamente el dispositivo.
- **Tener precaución con los mensajes de texto**. Es aconsejable no enviar por este medio datos confidenciales, como detalles de tarjetas de crédito o información privada importante.
- **Navegar por páginas con certificado de seguridad.** El icono del candado en la barra de direcciones del navegador indica que estás utilizando una conexión segura y de confianza. Comprueba la aparición de este icono cuando introduzcas datos personales, como tu dirección o información de pago, o cuando envíes correos electrónicos desde tu navegador móvil.
- **Verificar que tus aplicaciones provengan de fuentes de confianza.** Al instalar una aplicación en nuestro dispositivo, es recomendable usar los medios oficiales como son el App Store de Apple o Google Play de Android. Si nos descargamos la aplicación de una web de terceros, corremos el riesgo de que se nos instale malware.
- **Usar una aplicación de antivirus para móviles.** Al igual que en ordenadores, también hay aplicaciones destinadas a la protección de los dispositivos móviles como antivirus. Por ejemplo, los móviles con sistema operativo Android tienen instalado Google Play Protect y también se puede añadir una aplicación de terceros que incluye versiones gratuitas o versiones de pago que añaden más capacidades.

Proteger también nuestros dispositivos móviles supone que hagamos un uso más seguro de Internet.

4.1.3. Amplía la seguridad de las aplicaciones y servicios

● Protege tus cuentas con doble factor de autenticación

La información y los datos que tienen nuestras cuentas de correo, de redes sociales, cuentas bancarias y demás son un objetivo para los ciberdelincuentes.

Por ello, toda precaución es poca cuando hablamos de seguridad. Y una medida como el doble factor de autenticación nos permitirá agregar una segunda capa adicional de protección a la contraseña que empleamos para acceder a nuestras cuentas de todos los servicios que utilizamos.

Aunque nuestra contraseña de acceso sea “robusta” (mínimo 8 caracteres, combinando letras y números, mayúsculas con minúsculas y algún carácter especial), los ciberdelincuentes son capaces de averiguarla de varias formas como las filtraciones de datos, a través de algún software malicioso tipo Spyware que registra las pulsaciones de las teclas para saber lo que se escribe o a través de algún método de ingeniería social como el Phishing por el que se consigue que la persona revele su información personal.

Esta capa adicional de seguridad hace que para un ciberdelincuente sea mucho más difícil vulnerar el acceso a nuestros datos e información.

Pero ¿en qué consiste este doble factor de autenticación también llamado 2FA? Este tipo de autenticación añade un paso adicional para que iniciemos la sesión en un servicio evitando así que aunque alguien disponga de la contraseña de acceso al mismo no pueda acceder. Es decir, la primera capa de seguridad sería la contraseña de acceso y la 2FA incorpora otro dato más que es la segunda capa.

La capa adicional de autenticación puede ser uno de los siguientes factores:

- Algo que sabes, como la contraseña de acceso, un código PIN o las respuestas a preguntas de seguridad.
- Algo que tienes, que es normalmente un objeto físico como puede ser un teléfono móvil.
- Algo que es, que hace referencia a datos biométricos como puede ser la huella dactilar, el reconocimiento facial como el Touch ID y el Face ID de Apple, y el reconocimiento de retina.

El segundo dato que se requiere en la 2FA depende del servicio online. Por ejemplo, en una cuenta de correo del servicio de Gmail de Google, para usar la 2FA hay varias opciones, entre ellas:

- Con la aplicación Google Authenticator. Esta aplicación se instala en el teléfono y al iniciar sesión en la cuenta de correo electrónico aparece un mensaje en el teléfono que previamente se ha añadido asociado a esa cuenta. Para verificar que somos nosotros los que estamos accediendo hay que aceptarlo en dicho mensaje.
- A través de código de verificación. Con esta opción al intentar abrir sesión en Gmail, Google informa de la opción de escoger entre el envío de un mensaje de texto o SMS al número proporcionado o recibir una llamada de teléfono. A través de estos medios se proporcionará un código numérico que es necesario introducir como segundo paso en el acceso a la cuenta.

Para poder configurar la doble autenticación, lo primero es saber si el servicio dispone de ella para poder activarla. Por ejemplo, para activar la verificación en dos pasos de tu cuenta de Google:

- Accede a “Administrar tu cuenta de Google”
- En el menú de navegación selecciona Seguridad
- En la sección “Acceso a Google” selecciona Verificación en dos pasos y Comenzar

- Completa los siguientes pasos para indicar qué método usarás para la doble verificación para acceder a tu cuenta.

En Facebook, por poner otro ejemplo, puedes activar esta verificación de doble factor siguiendo estos pasos:

- Abre tu cuenta de Facebook
- Haz clic en el triángulo de la esquina superior derecha de la pantalla y selecciona “Configuración y Privacidad”. Después haz clic en “Configuración”
- En el menú de la parte izquierda selecciona “Seguridad e inicio de sesión” y haz clic en el botón de “Editar” de “Usar autenticación en dos pasos de la sección de “Autenticación en dos pasos”
- Aquí es momento de seleccionar el método de seguridad que usarás para el segundo paso.

Dado que el doble factor de autenticación supone dotar a nuestros accesos online una capa extra de seguridad sería recomendable activar la 2FA en todas las cuentas que podamos, especialmente en las relacionadas con banca en línea y otras cuentas confidenciales.

Y tú, ¿ya tienes activado el doble factor en tus cuentas?

● Cortafuegos y herramientas de control de navegación

Existen muchos tipos de medidas para protegernos a la hora de usar nuestros dispositivos informáticos. Incluso muchas están en funcionamiento sin que nos hayamos dado cuenta.

Un ejemplo de ello puede ser el Cortafuegos o Firewall, que es una medida de seguridad que es interesante conocer en qué consiste y cómo actúa en nuestros dispositivos.

De forma sencilla, se puede definir el cortafuegos en el mundo de la informática como un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de dicho ordenador con otros servicios autorizados.

El cortafuegos es una de las primeras medidas que se implantó en los ordenadores cuando surgió Internet a finales de la década de los 80 y cuando los primeros ciberdelincuentes vieron que Internet podría ser un medio para acceder a ordenadores de otras personas. Utilizándose no solamente para ordenadores de forma individual sino especialmente en redes locales también llamadas “Intranets”.

Existen dos tipos de cortafuegos:

- De hardware
- De software

Los cortafuegos tipo hardware o físicos pueden ser productos independientes o venir integrados en un aparato router. Los independientes normalmente están situados entre el punto de acceso a Internet y el switch que es el encargado de distribuir la conexión entre los ordenadores de una misma red. De esta forma, antes de que se produzca la distribución de la red entre los equipos ya se ha realizado la protección. Suelen ser los que usan las empresas y grandes redes aunque en ataques que vengan a través de otra aplicación como software malicioso tipo troyanos o las amenazas que se reciben a través de correos electrónicos fraudulentos pueden no ser infalibles.

Los cortafuegos tipo software son los que consisten en aplicaciones que pueden estar configuradas o instalarse en los ordenadores. Estos cortafuegos, además de interceptar intentos de acceso desde el exterior, también suelen incluir protecciones adicionales contra software malicioso como troyanos o virus de correo. En cuanto a

su desventaja es que únicamente protegen de manera individual a cada ordenador en el que está instalado.

Los dos tipos tienen como función situarse entre la red local e Internet para ser un medio de protección bloqueando el tráfico no solicitado o que se considere peligroso.

Se pueden instalar aplicaciones de cortafuegos de terceros pero si, por ejemplo, usas un ordenador con sistema operativo Windows debes saber que ya llevan integrado cortafuegos y muchos de los routers que hay en la actualidad tienen sus módulos para filtrar posibles amenazas de manera básica.

Aunque los cortafuegos sean una barrera de protección para los equipos siempre debemos tomar precauciones a la hora de navegar para ser el primer filtro de protección.

Otra medida de protección a la hora de navegar por Internet cuando de lo que estamos hablando es de menores que usan estos dispositivos, son aquellas medidas que podemos llamar de “Control Parental”.

La prioridad es que haya una comunicación fluida con los menores a nuestro cargo estableciendo unos límites de tiempo en el uso de las pantallas y unas pautas para el comportamiento responsable en la navegación por Internet. Pero las herramientas de control parental puede ser de ayuda para que las experiencias de los menores en Internet sean seguras.

Para escoger qué tipo de control es el más adecuado será necesario tener en cuenta las necesidades que se requieren entre, por ejemplo:

- Cambiar los ajustes del navegador para filtrar contenido inapropiado.
- Establecer el tiempo que se pasa frente a las pantallas o reducirlo en caso necesario.

- Revisar las páginas visitadas por los menores cuando navegan por Internet.
- O tener un control del uso que hacen de dispositivos móviles como puede ser el teléfono móvil.

Una vez detectadas las necesidades, los controles parentales pueden llevarse a cabo directamente a través de configuraciones en el propio dispositivo o usando alguna aplicación que sea necesario instalar. A continuación, vamos a nombrar algunas de ellas según las funciones que pueden realizar:

- Bloquear sitios web. Si se usa Google como motor de búsqueda en los dispositivos que se desee configurar el bloqueo de contenido explícito en resultados de búsqueda de webs, imágenes, etc.; se puede activar la utilidad de SafeSearch tanto en ordenadores como en dispositivos con sistema operativo Android e iOS. Para activar esta opción, puedes acceder a www.google.com/safesearch y activar su “filtro de resultados con contenido explícito”

- Bloquear sitios web, filtrar contenido y establecer límites de tiempo. Los sistemas operativos como Windows o MacOS, disponen dentro de sus “Ajustes” de controles parentales integrados para indicar las temáticas a las que los menores no tendrán acceso como juegos para adultos y similares. También permiten indicar la URL de las páginas a las que se bloquea el acceso y los horarios o tiempos en los que los menores pueden usar los dispositivos. En Windows esta opción está disponible para usuarios con el rol de “Administradores”en “Cuentas” y en la sección de “Familias y otros usuarios”. Será necesario “Agregar familia” y los usuarios que formarán parte de la misma. Después, al acceder a la información de cada usuario se indicarán pueden indicar el acceso que tendrá el menor a aplicaciones tiempo en pantalla, etc.

También pueden usarse aplicaciones como Qustodio tanto en ordenadores como en dispositivos móviles.

Por último, recordar que otras medidas de seguridad en el buen uso que hacemos de los dispositivos serían:

- Bloquear archivos con contraseñas. Para evitar que ciertos archivos sean abiertos por personas que no dispongan de la contraseña para acceder a su información. Por ejemplo, en documentos creados con aplicaciones de hoja de cálculo como Excel, se puede bloquear el documento desde la opción del menú "Archivo", "Proteger libro" y "Cifrar con contraseña".
- Cerrar las sesiones correctamente. El dejar abiertas las sesiones de los servicios que utilizamos puede ser un medio de acceso de personas ajenas a la información que contienen. Para ello es importante cerrar las sesiones de cada servicio cuando hayamos finalizado. Por ejemplo, si has estado revisando tu correo de Gmail para cerrar la sesión del mismo haz clic en el icono de tu cuenta y selecciona "Cerrar sesión". También si no recuerdas haber cerrado correctamente la sesión en otro dispositivo que en esos momentos no tengas en tus manos, los servicios online suelen disponer de la opción de cerrar la sesión de la cuenta escogiendo los dispositivos concretos.

Teniendo precaución a la hora de navegar con todo lo que se ha comentado lograremos una mayor seguridad en el uso que hacemos de Internet.

4.1.4. Protege tu conexión wifi

- **Seguridad en tu wifi**

La palabra **WiFi** significa *"fidelidad inalámbrica"* (*Wireless Fidelity)* y es una tecnología de transmisión de datos inalámbrica utilizada para conectarse a Internet.

En la mayoría de los casos se utiliza en el ámbito doméstico para la conexión de dispositivos en red local y que estos aparatos puedan acceder a Internet.

Es importante conocer que existen riesgos en la seguridad de la red inalámbrica. Ya que un ciberdelincuente podría, entre otras acciones:

- Interceptar los datos que envíes o recibas
- Acceder a tus archivos compartidos
- Secuestrar tu conexión a Internet y utilizar todo el ancho de banda o límite de descargas

Para evitar que esto pueda ocurrir, puedes poner en práctica las siguientes recomendaciones para proteger la red inalámbrica a la que te conectes:

- **Evita la utilización de la contraseña predeterminada. Esta clave suele aparecer en la pegatina situada en el propio aparato router.** Es muy fácil para un ciberdelincuente descubrir cuál es la contraseña predeterminada del fabricante de tu router inalámbrico y utilizarla para acceder a la red wifi. Por lo tanto, es conveniente que cambies la contraseña de administrador de tu router inalámbrico. A la hora de establecer la contraseña nueva, trata de elegir una serie compleja de números y letras, e intenta evitar la utilización de una contraseña que pueda adivinarse fácilmente.
- **Evita que el router indique su presencia**. Desactiva la difusión del identificador de red SSID (Service Set Identifier) para evitar que el dispositivo inalámbrico anuncie su presencia al mundo que te rodea.
- **Cambia el nombre SSID del dispositivo**. Es sencillo para un ciberdelincuente descubrir cuál es el nombre SSID predeterminado del fabricante del dispositivo y utilizarlo para localizar la red inalámbrica. Cambia este nombre predeterminado del router e intenta evitar la utilización de un nombre que pueda adivinarse fácilmente.

- **Cifra los datos**. En la configuración de la conexión, asegúrate de que activas el cifrado. Si el dispositivo es compatible con el cifrado WPA, utilízalo. En el caso de que no sea compatible, utiliza el cifrado WEP.
- **Protégete contra los ataques de malware.** Asegúrate de que instalas un programa antimalware eficaz en todos los ordenadores y demás dispositivos que se conecten a la red wifi. Con el fin de mantener actualizada la protección antimalware, activa la opción de actualización automática en el dispositivo.

Siguiendo estos consejos conseguirás proteger tu conexión wifi.

¿Notas que tu conexión wifi va lenta o no ofrece la calidad que debería? Aunque tu router esté conectado correctamente, existen distintas causas que pueden interferir en la conexión.
Entre las más habituales están:

- Que el aparato router esté colocado a demasiada distancia o en una mala posición.
- Que entre el router y los equipos conectados haya paredes. Materiales como el hormigón, ladrillo, piedra, mármol o el cemento actúan como una barrera que bloquea el paso de la señal wifi que emite el router. También muebles de metal o superficies reflectantes como espejos son materiales que actúan como barrera contra las ondas de la wifi.
- Que haya activas conexiones Bluetooth. Este tipo de conexiones utiliza la misma radio frecuencia de una conexión wifi de 2,4 GHz, pudiendo crear interferencias en tu señal.
- Que la conexión wifi de tus vecinos esté utilizando el mismo canal wifi de tu router y que sus señales estén interfiriendo con la tuya restándole algo de alcance.

Para sacarle el máximo partido a tu red wifi, puedes seguir estas recomendaciones:

- Encuentra el mejor sitio para colocar tu router. Sitúa el aparato router en una posición elevada y en una zona central de tu casa o del lugar donde se encuentre. De esta forma, la señal llegará a todos los rincones.
- No escondas el aparato router ni coloques obstáculos cerca de él como jarrones o marcos de fotos que puedan interferir en su señal.
- Evita posibles tirones del cable de fibra para que no afecte a la conexión. No coloques objetos pesados sobre el cable, ni aprisiones el cable con muebles o cualquier objeto. Tampoco lo dobles y procura que el ángulo en el que se conecta el cable al router sea lo menos pronunciado posible.
- Aleja el router de objetos del hogar que causan interferencias. Para obtener una mejor señal wifi es importante que alejes el router de objetos que pueden causar interferencias en tu wifi y atenuar la señal. Televisores, electrodomésticos, espejos y cristales, aparatos con conexión Bluetooth, agua como por ejemplo el que pueda contener una pecera, metales, teléfonos inalámbricos o aparatos como vigila bebés; pueden ser una causa por la que la señal wifi se vea afectada.

Además de tener en cuenta las recomendaciones comentadas, hay que tener presente algunas consideraciones para conseguir navegar a mayor velocidad, entre ellas:

- La compatibilidad de los dispositivos con el tipo de wifi al que se conecten. Los aparatos actualizados a su última versión del sistema operativo, los más modernos o de gama alta, suelen poder acceder a los distintos tipos de señales emitidas por el router y escoger la que ofrece una mayor velocidad.
- El uso de amplificadores para que la señal wifi llegue a zonas donde su alcance sin cable es menor.
- En el caso de tener muchos dispositivos conectados, para conseguir una mejor señal inalámbrica es recomendable distribuir los dispositivos conectados entre las redes wifi de 2,4 GHz y 5 GHz que los routers de nueva generación emiten.

Así como apagar o desconectar la wifi en los dispositivos que no estés utilizando.

- Decide a qué tipo de opción conectarás tus dispositivos, ya que la de 5 GHz ofrece mayor velocidad, menos interferencias, pero tiene menor alcance, es más susceptible a los obstáculos que pueda encontrar desde el aparato router al dispositivo conectado y solamente es compatible con los aparatos más modernos que estén habilitados para este tipo de conexión. En cambio, la convencional de 2,4 GHz es compatible con cualquier dispositivo.
- También puedes mejorar la velocidad de tu conexión optimizando el canal wifi al que estás conectado de la red. Ya que la wifi funciona en distintas frecuencias divididas a su vez en “Canales”. Por ejemplo, si estás conectado a la red wifi convencional de 2,4 GHz, puede que el canal en el que te encuentres esté saturado y por ello la velocidad de tu conexión se vea afectada. Accede a la aplicación de tu proveedor de Internet si dispone de ella para poder gestionar este cambio de canales y optimizarlo, si lo ves necesario, cambiando a otro canal más adecuado con menos interferencias y por lo tanto percibir una mejora en la conexión.

Poniendo en práctica estas recomendaciones seguro que conseguirás mejorar la calidad de tu conexión.

4.1.5. Seguridad e Inteligencia Artificial

La inteligencia artificial (IA) es una tecnología que puede tener grandes beneficios para la humanidad, pero también plantea importantes desafíos éticos.

La ética es fundamental en el uso y el desarrollo de la IA, ya que las decisiones que puedan tomar los sistemas de IA tendrán consecuencias importantes en la vida de las personas y en la sociedad en general.

Vamos a comentar algunos ejemplos como el de un sistema de IA capaz de tomar decisiones sobre a quién elegir para contratar en un puesto de trabajo o la toma de decisiones de a quién

conceder un préstamo. En estos casos, si estos sistemas no están diseñados correctamente, podrían tomar decisiones injustas o discriminatorias.

Por otro lado, los sistemas de IA pueden ser muy poderosos y causar incluso daño si no se utilizan de manera correcta. Por ejemplo, si un sistema de IA controla un vehículo autónomo y su diseño presenta errores imagina el daño que podría causar.

Por todo lo comentado, es necesario tener en cuenta la ética en todas las etapas del desarrollo y uso de la IA.

Se está avanzando en acordar unos principios éticos de la IA y algunos básicos que son aceptados en lo que se refiere al uso de la IA incluyen los siguientes aspectos:

- **Justicia**. Los sistemas de IA deben ser justos y no deben discriminar a ningún grupo de personas. Esto significa que deben ser diseñados para tener en cuenta las posibles fuentes de sesgo y para minimizar cualquier impacto injusto.
- **Transparencia**. Los sistemas de IA deben ser transparentes en cuanto a cómo toman decisiones. Esto significa que deben ser comprensibles para las personas y que debe ser posible entender cómo llegan a una determinada decisión.
- **Responsabilidad**. Debe haber responsabilidad en el desarrollo y uso de los sistemas de IA. Esto significa que debe haber mecanismos para responsabilizar a las personas y organizaciones que desarrollan y utilizan sistemas de IA.
- **Privacidad**. Los sistemas de IA deben respetar la privacidad de las personas y no deben recopilar ni utilizar datos personales sin el consentimiento adecuado.
- **Beneficio**. Los sistemas de IA deben ser diseñados para maximizar los beneficios y minimizar cualquier daño potencial.

Estos principios éticos sumado al concepto de “alineamiento” de la IA supone el proceso de asegurarse de que los sistemas de IA actúen de manera que estén alineados con los valores y objetivos humanos. Con ello, se asegura que sean beneficiosos para las personas y la sociedad en general.

Se plantean muchos desafíos éticos por parte de empresas y por los gobiernos. Como ejemplos de ello, la empresa Microsoft es una de las que está trabajando activamente para

abordar los desafíos éticos asociados con la IA. Esta empresa ha establecido un comité de ética de la IA compuesto por expertos en ética, derecho, ingeniería y otras disciplinas. Este comité revisa los proyectos de IA de la empresa y proporciona orientación sobre cuestiones éticas.

Además, Microsoft ha publicado un conjunto de principios éticos para la IA que guían el desarrollo y uso de la IA en la empresa. Estos principios incluyen la justicia, la inclusión, la transparencia, la responsabilidad y la privacidad.

La regulación de la Inteligencia Artificial (IA) ha tomado un papel central en la agenda de políticas globales dada la rápida evolución y adopción de estas tecnologías en múltiples sectores.

Las regulaciones están diseñadas para proteger los derechos y libertades fundamentales, como nuestra privacidad y no discriminación. Además, buscan fomentar la confianza en estas tecnologías, garantizando que se utilicen de manera responsable y beneficiosa.

Si hablamos de la UE, ésta ha sido líder en la regulación de la IA. Así se ha establecido un marco de clasificación para los sistemas de IA basado en el nivel de riesgo que representan, identificando áreas de alto riesgo y estableciendo requisitos especiales para sistemas de IA generativa.

La UE busca garantizar que los sistemas de IA sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. El 8 de diciembre de 2023, la Unión Europea aprobó la primera ley mundial de inteligencia artificial (IA), marcando un hito importante en la regulación de esta tecnología. La ley, que se espera entre en vigor a finales de 2026, busca garantizar la seguridad de los sistemas de IA y su alineación con los derechos y valores europeos. Se centra en la flexibilidad para regular tanto tecnologías actuales como futuras, incluyendo regulaciones específicas para modelos generativos como ChatGPT y sistemas de vigilancia biométrica, con prohibiciones y limitaciones estrictas para estos últimos. Además, establece un sistema de sanciones y la creación de una Oficina de IA independiente para supervisión.

En España, en 2022 se aprobó iniciar el procedimiento para establecer la sede física de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) en Galicia, convirtiéndose en el primer país de la Unión Europea con una agencia estatal de supervisión de la Inteligencia Artificial (IA), y adelantándose así a la entrada en vigor del futuro Reglamento europeo de IA, que establece la necesidad de que los Estados miembros cuenten con una autoridad supervisora en esta materia.

También la Organización Mundial de la Salud (OMS) ha publicado consideraciones clave para la regulación de la IA en el ámbito de la salud, proporcionando principios que los gobiernos y autoridades reguladoras pueden seguir para desarrollar o adaptar guías sobre IA a nivel nacional o regional. Entre estos desafíos y consideraciones estarían, riesgos de sesgo y discriminación, y las implicaciones en la privacidad y la seguridad, garantizar los derechos de los individuos, la cooperación internacional y la armonización de las regulaciones, que pueden ser clave para abordar los desafíos globales que presenta la IA.

La necesidad de regulación se está intensificando a medida que la IA se expande en industrias y geografías, y varios países han adoptado un enfoque proactivo hacia la regulación de la IA, publicando marcos, directrices y hojas de ruta que ilustran la futura regulación posible de la IA en estos países.

Esta regulación se enfoca a combatir también la desinformación y los deepfakes creados con tecnología de Inteligencia artificial. Los deepfakes son vídeos falsos generados con IA que pueden suplantar la identidad o la voz de una persona, alterando su imagen o su discurso. Estos vídeos pueden usarse para difundir noticias falsas, manipular la opinión pública, dañar la reputación de alguien o incluso provocar conflictos políticos o sociales. Se trata de un fenómeno que plantea graves riesgos para la veracidad, la confianza y la democracia. Por eso, es necesario establecer mecanismos de detección, verificación y denuncia de estos contenidos, así como educar a la ciudadanía para que sea crítica y responsable con la información que consume y comparte.

Por otro lado, la regulación también afecta al copyright o derecho de autor, que es el tipo de propiedad intelectual que protege la expresión original de una obra creativa, pero no la idea en sí. El copyright otorga al autor el derecho exclusivo de copiar, distribuir, adaptar, exhibir y producir su obra, generalmente por un tiempo limitado. Sin embargo, con el avance de la IA,

surgen nuevos desafíos para definir quién es el autor de una obra generada o asistida por una máquina, qué derechos le corresponden y cómo se deben respetar los derechos de los autores humanos. Además, se debe garantizar que la IA no vulnere los derechos de autor de otras obras al usarlas como fuente de inspiración o aprendizaje.

La evolución de la Inteligencia Artificial supone grandes desafíos como se ha comentado y está en la mano y criterio de todas las personas que la usamos el darle un correcto uso respetando la ética y seguridad.

MÓDULO 4
Área de Seguridad

Módulo 4. Seguridad

4.2. Protección de datos personales e identidad digital

4.2.1. Datos personales en Internet

- Protege tus datos personales en Internet

4.2.2. Privacidad y navegación por Internet

- Mecanismos que registran mi actividad
- Navegación de incógnito

4.2.3. Configurar la privacidad en nuestras aplicaciones y servicios:

- En los navegadores
- En mensajería instantánea y redes sociales
- En los dispositivos y aplicaciones móviles

4.2.4. Protección de datos personales en Internet

- Derechos sobre la protección de datos personales en Internet

4.2. Protección de datos personales e identidad digital

4.2.1. Datos personales en Internet

- **Protege tus datos personales en Internet**

Cada vez pasamos más tiempo conectados a Internet, ya sea para acceder al correo electrónico, a redes sociales, para hacer trámites online o también para comprar.

Pero ¿somos lo suficientemente precavidos en la protección de nuestros datos? ¿Los protegemos correctamente y conocemos el grado de privacidad de los mismos?

Cada vez que utilizamos un nuevo servicio web, en muchas ocasiones, es necesario que facilitemos nuestros datos ¿verdad? de ahí la importancia de proteger los mismos y llevar un control de la información que compartimos para que no lleguen a terceros que no deseamos.

Los principales problemas que puede suponer el no proteger nuestros datos adecuadamente son:

- **Fraudes**. Entre las técnicas que utilizan los ciberdelincuentes para hacerse con nuestros datos estaría el “Phishing” (obtención de información personal a través de diferentes medios, como por ejemplo, un correo electrónico que simula que viene de nuestro banco).

- **Suplantación de identidad**. Con el fin de, por ejemplo, realizar compras no autorizadas o acceder a nuestras cuentas bancarias.

- **Acceso a nuestras cuentas de correo electrónico o perfiles sociales**. Para enviar o publicar desde los mismos mensajes fraudulentos o SPAM.

Como recomendaciones para proteger nuestros datos y prevenir situaciones en las que seamos objetivo de acciones que pretendan obtener nuestra información, podemos citar las siguientes:

- Disponer de una cuenta de correo electrónico para utilizarla en el uso de cuentas como las del banco o para temas más serios o profesionales. Y otra cuenta secundaria para registrarnos en servicios de Internet en los que no conozcamos su reputación o en diferentes servicios que puede que nos envíen publicidad.

- Para prevenir el que nuestros datos sean captados por la técnica del “Phishing”, es recomendable nunca acceder a páginas cuya dirección esté indicada en un correo electrónico o en una publicación de redes sociales sin que previamente hayamos verificado la autenticidad del sitio web.

  Entre estas comprobaciones podremos ver si la información que se envía y recibe en el mismo está cifrada al disponer de un certificado válido. Esto puede verse si la dirección comienza por https y si al pulsar en el candado de color verde de la barra de direcciones aparece que el certificado es válido y los datos que se envían y reciben a través de la conexión están encriptados.

  Ten en cuenta que las entidades bancarias nunca se comunicarán con nosotros a través de email para solicitarnos datos como contraseñas o claves de acceso a nuestra cuenta. En estos casos concretos, en vez de seguir el enlace indicado en el correo electrónico, es aconsejable escribir directamente la dirección en el navegador o usar la aplicación móvil de la entidad bancaria para acceder.

También como ejemplos de fraudes para captar nuestros datos podemos citar los de cupones descuentos que podemos recibir y que solicitan nuestros datos personales y número de cuenta bancaria para canjearlos o el que la Agencia Tributaria nos devolverá dinero completando un formulario por un error que ha tenido en su sistema de gestión. ¡Mucha atención, porque son claramente fraudes!

- En los casos de rellenar un formulario online con nuestros datos, hay que verificar que la web es segura a través del certificado y que contenga en su dirección https así como leer el tratamiento de datos para conocer qué uso se hará de éstos.

- Es recomendable poner en práctica todas estas recomendaciones y por supuesto conocer que existe una Ley Orgánica de Protección de Datos que obliga a que las entidades soliciten nuestro consentimiento para usar nuestros datos de carácter personal. Asimismo, podemos ejercer nuestro derecho de solicitar que dejen de usarlos ejerciendo el derecho de cancelación y en caso de verse vulnerado, acudir a la Agencia Española de Protección de Datos para denunciarlo. Por ejemplo, en los correos electrónicos enviados por una entidad o empresa que disponga de nuestro email, es necesario que se indique la forma en la que podemos cancelar el seguir estando en la lista de envíos si no queremos seguir recibiéndolos.

Siguiendo estos consejos y recomendaciones contribuiremos a proteger nuestros datos y que no sean ¡pescados!

4.2.2. Privacidad y navegación por Internet

- Mecanismos que registran mi actividad

Mucha de la información que circula por Internet la hemos compartido directamente en las acciones que hemos realizado en nuestra navegación y en los permisos que hemos concedido a servicios y aplicaciones.

Mientras navegamos por Internet también estamos proporcionando mucha información directamente al navegador, ya que si usamos una ventana de las que se abren por defecto en el mismo, puede almacenar datos como:

- Las webs que visitamos en lo que es el historial de navegación
- Las contraseñas que usamos para acceder a los servicios online en los que tenemos una cuenta creada si aceptamos la opción
- Los datos que introducimos de formularios que completamos
- O las cookies que están configuradas en los sitios webs cuando accedemos a ellos y que se quedan guardadas en nuestro navegador.

Por ello, es recomendable que revisemos la información que tiene almacenada nuestro navegador web y borremos con cierta frecuencia la misma, ya que podría ser una entrada para que los ciberdelincuentes accedieran a través de ella y robaran la información almacenada. Por ejemplo, si accedieran y robaran las cookies que guardan información sobre nuestras contraseñas o de inicio de sesión, podrían acceder a nuestras cuentas en servicio bancarios.

Las cookies son paquetes de datos que intercambian los diferentes programas informáticos. De esta forma se consigue que los usuarios puedan utilizar con más facilidad tanto funciones aisladas como aplicaciones web tales como tiendas online, redes sociales o foros.

Si quieres gestionar la información que tiene guardado tu navegador si usas Google Chrome, puedes hacerlo accediendo desde el menú de la parte superior derecha de la pantalla de “Personaliza y controla Google Chrome” y selecciona “Configuración”.

En el menú de la configuración de tu navegador selecciona “privacidad y seguridad” y podrás:

- Borrar datos de navegación
- Cookies y otros datos de sitios
- Seguridad (Navegación segura frente a sitios peligrosos y otros ajustes de seguridad)
- etc.

Otro de los mecanismos que pueden registrar nuestra actividad es la “geolocalización”, que consiste en obtener la ubicación geográfica de un objeto como puede ser un teléfono móvil, un coche o una calle. Para ello se puede utilizar diferentes métodos como por ejemplo detectar la dirección IP de un equipo o el sistema GPS de nuestro teléfono móvil.

Para obtener la ubicación geográfica aproximada de un smartphone se utiliza un sistema de posicionamiento global. El sistema está formado por una red de satélites geoestacionarios que dan cobertura a toda la Tierra. Para obtener la ubicación, el dispositivo se conecta como mínimo con 3 satélites, de estos satélites recibe un identificador y la hora de cada uno ellos. El dispositivo calcula el tiempo que tarda en llegar la señal desde los satélites y gracias al retardo o “delay” resultante se obtiene la ubicación por medio de la triangulación.

La geolocalización y las aplicaciones de mapas son usados por los ciberdelincuentes para encontrar objetivos potenciales basándose, por ejemplo, en las publicaciones que hacemos en redes sociales o la información facilitada por mapas virtuales como Google Maps.

Y es que las aplicaciones y las redes sociales, en muchas ocasiones solicitan permiso para acceder a nuestra ubicación y aceptarnos sin pararnos a pensar qué información estamos facilitando realmente. Esta información que facilitamos de manera voluntaria

es almacenada y analizada por organizaciones como Google o Facebook (Meta) generalmente para mostrar publicidad personalizada, aunque pueden darle otros usos. Esto puede ser considerado una invasión de la privacidad, pero somos nosotros los que permitimos esta invasión cuando aceptamos sus condiciones.

En otras muchas ocasiones, directamente facilitamos nuestra ubicación. Cuando publicamos en cualquier red social una foto o un vídeo con la ubicación, la ruta que hemos hecho entrenando, etc.

También hay ocasiones en que la información la facilitamos de manera involuntaria, por ejemplo, con los "metadatos" en imágenes y vídeos. Los metadatos es información que va unida a un archivo y en la que se detallan diferentes aspectos del mismo entre ellos la ubicación. En algunas ocasiones los vídeos y fotos que hacemos y publicamos en redes sociales llevan consigo metadatos con los que se puede obtener la ubicación exacta de dónde fue realizado el vídeo o la foto.

El compartir información relacionada con la geolocalización puede suponer varios riesgos como:

- Revelar dónde se está en un momento dado
- Informar de dónde "no se está"
- Dar pistas sobre dónde se encuentran objetos de valor
- Mostrar información de personas que te acompañan

Para evitar que se rastree la información de nuestra ubicación podemos desactivar la función GPS de la cámara del teléfono inteligente, comprobar la privacidad que tenemos configurada en redes sociales, evitar compartir información en tiempo real para no informar de dónde nos encontramos en cada momento.

Son muchos los mecanismos que pueden informar de la actividad que realizamos en Internet y que afecta en gran medida a nuestra vida fuera del entorno online por lo

que es fundamental conocer qué formas hay para evitar dicho rastreo de información para que no deriven a otros problemas asociados. ¡Tener precaución es responsabilidad nuestra!

- **Navegación de incógnito**

Ya sea en Google Chrome, Firefox o Safari, todos los navegadores modernos ofrecen un modo de incógnito para la navegación privada.

El modo de incógnito es una ventana privada en el navegador desde la que se puede navegar en Internet sin que se guarde cierta información como:

- El historial en el dispositivo cuando cierre la sesión de navegación.
- Las cookies, que son fragmentos de datos de identificación que siguen nuestra navegación en Internet
- y otros rastros asociados al historial de navegación que una vez finalizada la sesión de navegación privada no se quedan guardados

El modo de incógnito permite navegar en Internet como si fueras un **nuevo visitante** en cada página que abras. Todas las páginas web que visites mientras navegues el modo de incógnito es como si nunca ha visitados la página antes. Esto significa que no habrá cookies, datos de inicio de sesión ni formularios web autorrellenados esperando en esta página, aunque la hayas visitado en anteriores ocasiones.

Por ejemplo, usar el modo de incógnito garantiza que los billetes de avión, por ejemplo, y otros artículos valiosos no aumenten de precio cuanto los busques en diferentes momentos.

Eso sí, hay que saber que si iniciamos sesión en alguna de nuestras cuentas, como la de Google cuando estemos navegando en el modo de incógnito, los datos se

guardan durante esa sesión. No se recordarán cuando dejes de navegar completamente, pero ayudarán a recopilar datos de tu navegación mientras tengas la sesión iniciada para fines publicitarios principalmente.

Normalmente, el modo incógnito o modo privado (llamado de distinta forma según el navegador), se usa cuando se quiere mantener el anonimato en Internet. Por ejemplo, si buscas un regalo para alguien que también use el mismo dispositivo y no quieres que se entere, buscar con el modo de incógnito garantizará la privacidad.

Aunque es una forma de navegación más privada, es fundamental conocer también sus limitaciones como por ejemplo que este modo de navegación privada sí guarda la dirección IP porque sigue siendo visible.

Entonces, ¿cuándo se podría usar el modo incógnito? Estas son algunas de las razones para usar este tipo de navegación:

- **Evitar que se guarden cookies.** Las páginas que visites no guardarán permanentemente tus datos de inicio de sesión ni la información de tu dispositivo. Esto significa que podrás iniciar sesión con varias cuentas simultáneamente o asegurarte de que los precios no suban en ocasiones que estés buscando información de algo que piensas comprar.
- **Ocultar el historial de búsqueda.** Aunque algunos motores de búsqueda pueden ver tu historial de búsqueda incluso en el modo incógnito, no podrán hacerlo otras personas que usen tu dispositivo.
- **Protección antiseguimiento.** Tu actividad en Internet está protegida en el modo incógnito, es decir, verás menos anuncios segmentados y menos sugerencias personalizadas siempre que no inicies sesión en tus cuentas personales.
- **Invitados.** Por ejemplo, si alguien te pide prestado su dispositivo, el modo de incógnito garantizará que no puedan iniciar sesión ni autorrellenar formularios con tus datos guardados. Así, la persona a la que le prestes tu dispositivo

también tendrá la tranquilidad de saber que sus datos no se guardarán en el mismo.

La navegación de incógnito puede ser de gran utilidad si deseas navegar de una forma más privada. ¿La has usado ya?

4.2.3. Configurar la privacidad en nuestras aplicaciones y servicios

● En los navegadores

Los navegadores web recopilan mucha información acerca del recorrido que hacemos en Internet, las páginas que visitamos, nuestros intereses y mucho más.

Todos los navegadores web, como Google Chrome, Firefox, Safari o Microsoft Edge, te permiten eliminar el historial de navegación web.

Pero, aparte de eliminar el historial de navegación, es recomendable configurar las opciones de privacidad en navegadores web. Para hacerlo, en función al navegador, puedes seguir los pasos que indicamos a continuación de los tres más usados:

- **En Google Chrome.**
  Para modificar la configuración de privacidad:
  - Haz clic en el menú de Chrome en la esquina superior derecha del navegador indicado como “Personaliza y controla Google Chrome”, luego selecciona “Configuración”.
  - Localiza y selecciona Mostrar configuración avanzada.
  - Las opciones de privacidad aparecerán. Para modificar la configuración de privacidad básica, como habilitar la protección contra malware, marca o desmarca las casillas junto a cada opción.

- Para modificar configuraciones específicas, como cuando las páginas web pueden guardar cookies o acceder a tu ubicación, haz clic en el botón Configuración de contenido

Para eliminar sitios específicos del historial:

- Haz clic en el menú de Chrome en la esquina superior derecha del navegador y luego selecciona “Historial”.
- Haz clic en la casilla de verificación junto a cada enlace que deseas eliminar de tu historial, luego elige “Eliminar” elementos seleccionados.
- Aparecerá un cuadro de diálogo. Haz clic en “Eliminar” para continuar.
- Los sitios web seleccionados se eliminarán de tu historial

- **En Mozilla Firefox**

Este navegador incluye la opción del bloqueo de contenido. A través de esta característica es posible bloquear automáticamente el contenido que rastrea los sitios que visitas y elabora perfiles. Puedes elegir entre los modos Estándar, Estricto y Personalizado, que te permiten bloquear:

- Rastreadores
- Cookies
- Cyrptominers
- Huellas dactilares

Para ajustar la configuración de bloqueo de contenido de Firefox, ve a Menú / Opciones / Privacidad y seguridad / Bloqueo de contenido y luego selecciona el modo que deseas usar.

Para deshabilitar el bloqueo de contenido para ciertos sitios de confianza, introduce la URL del sitio web, haz clic en el icono «i» a la izquierda de la barra de direcciones, luego en el botón gris para “Desactivar el bloqueo de este sitio”.

- **En Microsoft Edge**

Para modificar cómo Microsoft Edge maneja la configuración de privacidad para mantener segura la información sobre tus hábitos de navegación o identidad:

- Haz clic en el botón “Más acciones” y después en “Configuración”.
- Desplázate hacia abajo y haz clic en Ver configuración avanzada en Configuración avanzada.
- En el panel de Configuración avanzada, desplázate hasta la parte inferior del panel, más allá del encabezado Privacidad y Servicios.
- Haz clic en la lista desplegable debajo de Cookies, luego en Bloquear todas las cookies o Bloquear solo las cookies de terceros.
- También puedes usar la configuración Bloquear ventanas emergentes cerca de la parte superior del panel Configuración avanzada. Cuando se activa esta configuración en Microsoft Edge, se evita que se carguen ventanas emergentes cuando visitas un sitio. Si bien las ventanas emergentes generalmente muestran anuncios ofensivos o molestos, algunas pueden estar asociadas con esquemas de phishing o malware.

Configurar la privacidad y seguridad de los navegadores web que uses para acceder a Internet es una medida de prevención y protección que puedes poner en marcha ya mismo.

● En mensajería instantánea y redes sociales

En los últimos años, hemos visto cómo los medios más habituales para enviar información como el correo electrónico, se ha ido sustituyendo por otros como aplicaciones que usamos en nuestros teléfonos inteligentes o incluso las redes sociales.

La rapidez de hacerlo a través de estos medios puede ser una de las causas de que se haya incrementado el uso de estos medios frente al correo electrónico. La cuestión está en que en ocasiones se usa para enviar información o documentos importantes que podría tener consecuencias negativas relacionadas con la seguridad y privacidad.

Cuando hablamos de mensajería instantánea, nos referimos tanto a aplicaciones que pueden estar instaladas en nuestro móvil como WhatsApp, Telegram y similares como aquellas que cuentan con servicios de chat integrado vía web como en redes sociales como Facebook.

Un alto porcentaje de los ataques que ocurren cada día necesitan la interacción del usuario ya que se requiere una acción por parte de la víctima cometiendo un error al no prestar atención a lo que está ocurriendo y, por ejemplo, descargue algo que pueda suponer alguna amenaza.

En estos casos, nuestra privacidad puede estar en peligro y datos e información personal verse expuesta o ser utilizada como “moneda de cambio” vendida a terceros.

Por ello, vamos a comentar algunos consejos para mejorar la privacidad a la hora de usar aplicaciones de mensajería instantánea y redes sociales:

- **No enviar lo que se denomina “información sensible”**. A la hora de enviar o recibir documentos que contengan datos personales o información confidencial evitar hacerlo por estos medios.

- **Cuidado con los archivos que descargamos**. En el caso de los proveedores de correo electrónico, disponen de funciones para detectar posibles amenazas e informan en caso de que un archivo pueda ser peligroso llegando incluso a bloquearlo y aunque los servicios de mensajería instantánea también disponen de algunas medidas de protección, no son tan precisas.

- **Revisar a qué información estamos autorizando el acceso a otras aplicaciones**. Muchas plataformas de mensajería instantánea y de redes sociales permiten conectar otros programas que complementan o integran el uso que hacemos de ellas. Es necesario que conozcamos qué accesos estamos permitiendo y a qué datos pueden acceder. Además, a esto se suma que si hay algún problema de seguridad en la aplicación a la que hemos dado acceso, también puede afectar a nuestros datos compartidos a través de ella.

- **Evitar compartir demasiada información personal**. Normalmente las aplicaciones de mensajería y las plataformas de redes sociales permiten incluir datos personales como nuestra dirección de email, nombre, lugar de trabajo o incluso nuestro número de teléfono. Pero ¿realmente queremos que sean públicos? La realidad es que no es necesario exponer tanta información personal para usar este tipo de servicios online y que estén visibles.

- **Estar pendiente de los cambios en los permisos de privacidad**. Los permisos que aceptamos al usar aplicaciones de mensajería instantánea y redes sociales pueden cambiar y poner en riesgo nuestra privacidad. También es necesario estar pendiente de los complementos externos a estos servicios que tengamos instalados y que pueden cambiar su política de privacidad.

- **Precaución con los "bots"**. Los bots están presentes tanto en aplicaciones de mensajería instantánea como en redes sociales. Lo normal es que se hagan pasar por usuarios que intentan recopilar información por lo que debemos prestar atención para detectarlos.

Para conocer cómo configurar la privacidad en diferentes aplicaciones de mensajería instantánea como WhatsApp y en redes sociales, puedes consultar los vídeos que acerca de ello dispone la Agencia Española de Protección de Datos en su web.

Accede a su sección de vídeos y podrás informarte de las opciones de privacidad y seguridad de todos estos medios.

Por tanto, siguiendo estos consejos y configurando las opciones disponibles en estos servicios, podremos evitar riesgos que dañen nuestra privacidad.

● En los dispositivos y aplicaciones móviles

Los dispositivos móviles gracias a su conectividad y a sus funcionalidades nos facilitan el día a día. Hoy mismo, tal vez hayas usado tu teléfono móvil para consultar horarios de transportes, para localizar un restaurante, o para compartir los mejores momentos de tu vida en redes sociales.

Pero ¿sabes si estás poniendo en riesgo tu privacidad? Aunque la recopilación de datos en determinados casos puede ser muy positiva, por ejemplo, para saber las condiciones del tráfico, para optimizar rutas de transporte público, para hacer recomendaciones personalizadas o incluso para medir niveles de polución, también conlleva un riesgo.

Las Autoridades Europeas de protección de datos establecieron la obligatoriedad de que las aplicaciones móviles deben obtener el consentimiento informado y específico del usuario a la hora de usarlas.

Por ello, cuando instalemos aplicaciones móviles es recomendable seguir una serie de pautas que afectarán tanto al uso que hacemos de ellas como al dispositivo en el que realicemos la instalación:

- **Usar tiendas de aplicaciones oficiales.** Para reducir el riesgo de instalar aplicaciones que podrían suponer algún riesgo relacionado con la seguridad, es conveniente descargar las aplicaciones únicamente desde las tiendas de aplicaciones oficiales, como la tienda del fabricante del dispositivo o la tienda de aplicaciones del sistema operativo correspondiente. Además, se puede investigar al desarrollador de la aplicación antes de instalarla.

- **Averiguar a qué información tendrá acceso la aplicación.** Antes de descargar una aplicación, hay que leer la política de privacidad de la aplicación para ver cómo se utilizarán o se compartirán nuestros datos. ¿La política es poco clara sobre cómo compartirá tus datos la aplicación? En ese caso, o si no se indica claramente cómo se compartirá esta información, podemos buscar otra aplicación.

- **Revisar los permisos.** Para poder acceder a cierta información, como la ubicación, la agenda de contactos o a otras funciones de tu dispositivo, como la cámara o el micrófono, las aplicaciones necesitan tu permiso. Puede que te soliciten permiso cuando descargues la aplicación por primera vez, o cuando la aplicación trate de acceder a esa información o función por primera vez. Presta mucha atención a los permisos que te pida una aplicación. Por ejemplo, ¿realmente necesita acceder a tu ubicación o a tus fotos para poder funcionar?

En el caso de que las aplicaciones ya estén instaladas, podemos revisar algunas cuestiones para proteger la privacidad:

- **Revisar los permisos de la aplicación.** Para ello, podemos acceder a la configuración del dispositivo para controlar que la aplicación no tenga acceso a información o funciones innecesarias. Así, podremos desactivar los permisos innecesarios prestando especial atención a las aplicaciones que tienen acceso a la lista de contactos, cámara, almacenamiento, ubicación y micrófono.

- **Limitar los permisos de ubicación geográfica.** Algunas aplicaciones tienen acceso a los servicios de ubicación o localización de tu dispositivo. Si una aplicación necesita acceder a tus datos de localización para funcionar, piensa en restringir el permiso para que la aplicación acceda a esos datos únicamente cuando esté en uso.

- **No inicies sesión automáticamente en las aplicaciones con una cuenta de red social.** A menudo, el inicio de sesión en una aplicación con la misma información de tu cuenta de redes sociales permite que la aplicación recopile información de tu cuenta de redes sociales y viceversa. Si quieres evitarlo, usa tu dirección de email y una contraseña única para iniciar sesión en la aplicación.

- **Mantén actualizadas las aplicaciones.** Las aplicaciones con el software desactualizado pueden ser más vulnerables a ciberataques. Protege tu dispositivo contra los programas maliciosos instalando las actualizaciones de la aplicación cuando estén disponibles.
- **Elimina las aplicaciones que no necesites.** Para evitar la recopilación de datos innecesarios, elimina las aplicaciones que ya no estés usando.

Es fundamental conocer el acceso a la información que tienen las aplicaciones que usemos para evitar posibles riesgos de privacidad. ¡Controla el acceso a tus datos!

4.2.4. Protección de datos personales en Internet

- Derechos sobre la protección de datos personales en Internet

A la hora de navegar y usar los servicios disponibles en Internet, existen unas normas de protección de datos a nivel de la Unión Europea que garantizan la protección de nuestros datos personales en los casos que se recojan los mismos como por ejemplo, al comprar por Internet, presentar una solicitud de empleo o darnos de alta en algún servicio.

Estas normas se aplican tanto a empresas y organizaciones (públicas y privadas) con sede en la UE como a las que tienen su sede fuera de ella y ofrecen bienes y servicios en la UE, como Facebook o Amazon, siempre que dichas empresas soliciten o reutilicen datos personales de ciudadanos de la Unión Europea.

El formato en el que se recopilan los datos puede ser de distintos tipos pero siempre que se almacene o se trate información que te identifique directa o indirectamente como individuo, deben respetarse tus derechos en materia de protección de datos.

Así, cuando una entidad, organización o empresa solicite tu consentimiento para el uso de tus datos personales, tienes que indicar claramente tu autorización, por ejemplo mediante la firma de un formulario de consentimiento o la selección inequívoca de una opción "sí/no" en una página web.

No basta simplemente con marcar la casilla de que no deseas recibir correos electrónicos con fines comerciales. Debes aceptar y autorizar que tus datos personales se recojan y/o reutilicen con esa finalidad.

Antes de decidir si aceptas o no, debes recibir también la siguiente información:

- Información sobre la empresa/organización que vaya a tratar tus datos personales, en particular tus datos de contacto y los datos de contacto del delegado de protección de datos, en su caso.
- La razón por la que la empresa/organización utilizará tus datos personales
- Cuánto tiempo se conservarán tus datos personales
- Detalles de cualquier otra empresa u organización que recibirá tus datos personales
- Y la información sobre tus derechos en materia de protección de datos (acceso, rectificación, supresión, reclamación y retirada del consentimiento).

Toda esta información debe facilitarse de manera clara y comprensible.

Si ya has dado tu consentimiento a una empresa u organización para que utilice tus datos personales, puedes ponerte en contacto con el responsable del tratamiento (la persona u organismo que gestiona tus datos personales) y retirar tu consentimiento en cualquier momento. Una vez retirado el consentimiento, la empresa u organización ya no puede seguir utilizando tus datos personales.

Puedes ejercer tu derecho de oposición si una organización utiliza el tratamiento de tus datos personales para su propio interés legítimo o como parte de una misión realizada en interés público o para una administración pública. En algunos casos específicos prevalece el interés público y la empresa u organización podría estar autorizada a seguir utilizando tus datos personales. Por ejemplo, en el caso de investigación científica y de estadísticas, tareas realizadas dentro de las funciones oficiales de una administración pública.

Los correos electrónicos de comercialización directa que promocionan marcas o productos concretos requieren el consentimiento previo. No obstante, si eres cliente de una determinada empresa, puede enviarte mensajes de comercialización directa sobre sus propios productos o servicios similares. Eso sí, tienes derecho a oponerte

en cualquier momento a recibir mensajes de comercialización directa y la empresa debe dejar de utilizar tus datos inmediatamente.

En todos los casos, la primera vez que la empresa u organización se dirija a ti deberá facilitarte siempre información sobre el derecho de oposición a la utilización de tus datos personales.

Si tus datos personales ya no son necesarios o se utilizan de forma ilegal, puedes solicitar su eliminación. Es lo que se conoce como "derecho al olvido". Estas normas también se aplican a los motores de búsqueda, como Google, ya que también se consideran responsables del tratamiento. Puedes pedir que se supriman de los resultados de motores de búsqueda los enlaces a páginas web que incluyan tu nombre cuando la información sea inexacta, inadecuada, irrelevante o excesiva.

Si una empresa ha puesto a disposición en Internet tus datos personales y pides que se eliminen, la empresa tiene que comunicar también a todos los sitios web donde los haya compartido que has solicitado que se supriman tus datos y los enlaces correspondientes.

Para proteger otros derechos, como la libertad de expresión, es posible que algunos datos no se borren automáticamente. Por ejemplo, podrían no suprimirse declaraciones controvertidas realizadas en público si fuera mejor para el interés general mantenerlas online.

Cuando usamos servicios a través de Internet, es necesario ser conscientes de que aceptamos el que compartimos los datos que se requieren. Pero también conocer nuestros derechos sobre cómo poder protegerlos y los derechos que podemos ejercer como los que informa la Agencia Española de Protección de Datos en su web es responsabilidad de cada persona.

Módulo 4. Seguridad

4.3. Protección de la salud

4.3.1. Salud y uso de la tecnología

- Recomendaciones en el uso de la tecnología

4.3.2. Riesgos para la salud sobre el uso de la tecnología

- Riesgos y enfermedades asociados al uso de la tecnología

4.3. Protección de la salud

4.3.1. Salud y uso de la Tecnología

- **<u>Recomendaciones en el uso de la Tecnología</u>**

Debemos ser conscientes no solo de las posibilidades que nos brindan las tecnologías, sino también de los riesgos que nos pueden producir en nuestra salud.

Por ello, es fundamental que tomemos las precauciones necesarias para evitar, en la medida de lo posible, que ciertos hábitos o modos en que usamos la Tecnología nos influyan de forma negativa.

Vamos a comentar algunas de las recomendaciones de uso de la Tecnología que es necesario conocer y poner en práctica.

La protección y cuidado de nuestra vista será la primera recomendación que citemos, ya que el tiempo que pasamos mirando a pantallas que emiten luz es cada vez mayor y por ello los problemas relacionados con este sentido pueden aumentar. Para ello podemos realizar varias acciones:

- **Configurar el nivel de brillo de la pantalla para proteger nuestra vista**. Por ejemplo, adecuar la luz de la pantalla de nuestro dispositivo en función al momento del día en el que nos encontremos. Los dispositivos móviles como los teléfonos inteligentes disponen del llamado “filtro de luz azul” que ya muchos llevan incorporados de fábrica o que podemos utilizar a través de aplicaciones que realizan esta función y que encontramos en la tienda de aplicaciones correspondiente. Relacionado con la configuración de pantalla, el

adecuar el brillo de la misma será un aspecto a tener en cuenta para adecuar su intensidad a un nivel adecuado.

- **Realizar descansos periódicos**. Como precaución, siempre que pasemos tiempos prolongados mirando pantallas, debemos tener en cuenta hacer descansos cada cierto tiempo para que nuestra vista descanse. Lo recomendable es descansar los ojos al menos 5 minutos cada hora.

- Recordar también **parpadear**, asegurar que hay **suficiente luz** y **evitar los reflejos**.
- **Configurar el tamaño de letra en dispositivos móviles**. Aunque no nos demos cuenta de ello, puede que el tamaño de letra que aparece en nuestros dispositivos, como en el caso de nuestro teléfono móvil, sea pequeño y necesitemos ponerlo a un tamaño mayor. Para modificar este tamaño de letra, accede a la configuración del dispositivo y en “tamaño de fuente“ podrás adecuar este aspecto al que necesites para no forzar tu vista. La configuración de esta opción puede variar en función al dispositivo, pero la llevan incorporada para que podamos personalizarla en caso necesario.

- En el caso de los ordenadores, la distancia sería de unos 50 cm y en dispositivos como teléfonos inteligentes y tabletas a unos 25-30 cm.

Otro aspecto que debemos cuidar es el de la postura corporal a la hora de utilizar tanto ordenadores como dispositivos móviles. Entre estas recomendaciones citaremos:

- Situar el monitor de modo que el borde del mismo quede al nivel de tus ojos o un poco más abajo.
- Mantener la cabeza y el cuello en posición recta y los hombros relajados.
- Situar tus brazos, espalda y piernas formando un ángulo de 90º.

- Mantener los pies pegados al suelo o sobre un reposapiés.
- Si utilizas un ratón al manejar tu ordenador, procura mantener las manos, las muñecas y los antebrazos en una posición neutra y cómoda, paralela al plano de la mesa.

Entre las precauciones a tener presentes en relación al sentido del oído podemos citar:

- Evitar escuchar a un volumen demasiado alto el sonido que proviene de los diferentes dispositivos que utilizamos.
- No abusar del uso de auriculares, escuchar música, vídeos o hacerlo durante largos periodos de tiempo pueden dañar nuestros oídos y producir otros problemas de salud relacionados.

Pero no solo los riesgos relacionados con el uso de la Tecnología afectan a nuestro cuerpo de forma física, debemos también tener presente que un uso excesivo de las tecnologías pueden llegar a crear conductas adictivas, aislamiento por pérdida de socialización, sedentarismo, estrés, ansiedad e incluso los relacionados con el ciberacoso a través de Internet.

Cada vez son más frecuentes informaciones provenientes de estudios como el realizado por la Universidad Camilo José Cela "Uso y abuso de las Tecnologías de la Información y la Comunicación por adolescentes" que nos alertan del peligro que puede suponer el excesivo uso de las mismas.

Para una prevención adecuada podemos consultar recursos de interés como la "Guía de buenas prácticas TIC para las familias" de La Red de Escuelas Digitales de Castilla y León Siglo XXI en la que se indican recomendaciones ante los posibles riesgos y medidas a tener presentes para evitarlos.

Con todo lo comentado sobre el cuidado de nuestra salud a la hora de utilizar la Tecnología está en nuestra mano seguir las recomendaciones para prevenir posibles riesgos y hacer un uso correcto de la misma.

4.3.2. Protección de la salud

- **<u>Riesgos y enfermedades asociados al uso de la Tecnología</u>**

Gracias a la tecnología podemos hacer cosas antes impensadas, como estudiar o trabajar desde cualquier lugar en cualquier momento, comunicarnos a tiempo real con personas que estén al otro lado del mundo o dar respuesta a las dudas que nos surgen en nuestra vida de multitud de temas diferentes. Pero el excesivo uso de los dispositivos informáticos y la permanente conexión a Internet puede tener como consecuencia problemas de salud.

A continuación, vamos a comentar algunos problemas que van asociados al uso de la tecnología:

- **Nomofobia**. Esta fobia va asociada a la adicción al uso del teléfono inteligente. Consiste en experimentar sentimientos de ansiedad, inseguridad y hasta angustia cuando sales de tu casa y te olvidas del teléfono o cuando por algún motivo, como la falta de señal o el quedarse sin batería, impiden el uso de estos aparatos.

- **Síndrome FOMO** (siglas de 'fear of missing out'), está asociado a la tecnología y las redes sociales. Se trata de un tipo de ansiedad social causada por la impresión de que el resto del mundo está teniendo experiencias gratificantes y divertidas sin la persona que lo sufre. Esto provoca la necesidad de estar siempre conectado y un miedo irracional a la sensación de estar perdiéndose algo. Esta enfermedad, deriva del tradicional miedo a la exclusión, a no pertenecer al grupo, pero las nuevas tecnologías lo han agravado. Para los

jóvenes, y también para muchos adultos, es un síndrome que les mantiene pegados a las pantallas de sus dispositivos.

A través de las redes sociales estamos siempre conectados, viendo qué hacen los demás con su vida, los momentos más felices, los lugares más impresionantes y una imagen siempre positiva de la vida de cualquiera. Esta conexión nos hace sentir una pertenencia al mismo grupo, tanto con personas cercanas como con otras personas a las que no se conoce, como famosos e “influencers”. A raíz de esta serie de pensamientos**,** se generan sentimientos de soledad, aislamiento, baja autoestima y tristeza que también pueden acabar en angustia, ansiedad, adicción e incluso depresión.

Para saber si se padece FOMO, se pueden identificar los siguientes síntomas:

- Consultar las redes al despertarse y antes de dormir.
- Las redes sociales abarcan las principales actividades cotidianas.
- Se tiende a involucrarse cada vez más porque brindan recompensas y confort.
- Se experimenta sensación de autoeficacia, pertenencia y satisfacción en las redes sociales.
- Se empieza a ignorar las relaciones reales, cambiándolas por la interacción virtual.
- Hay una importante disminución del bienestar emocional.
- Aparecen sensaciones de inseguridad e irritación ante actividades reales.
- Mayor uso del móvil para no perderse otras experiencias.
- Aparecen la ansiedad, la sensación de soledad y abandono y exclusión por no participar.
- Estrés asociado a experiencias negativas con otros usuarios de redes sociales que pueden llegar a ser incluso “haters” o que realizan acciones de acoso.

El sufrir FOMO, sobre todo en generaciones más jóvenes, se puede evitar mediante educación, vigilancia y corrección además de fomentar las habilidades sociales y la autoestima desde la infancia.

- **Ciberacoso.** El estar permanentemente conectado también supone que el riesgo de sufrir acoso por medio de tecnologías digitales aumente. Ya que personas que buscan atemorizar, enfadar o humillar a otras personas usan estos medios para hacerlo.

- **Infoxicación.** El exceso de información, también conocido como “infoxicación”, es el fenómeno que surge por los avances tecnológicos en nuestra vida. Hace referencia a la excesiva cantidad de información que recibimos y que llega a superarnos y nos satura. Es decir, rebasa nuestra capacidad de asimilación y eso puede suponer un problema de salud.

  La infoxicación produce una serie de síntomas que en algunas ocasiones son fácilmente identificables y en otras no. Por ejemplo, podemos encontrarnos un momento de:

  - Estrés o agobio generado por consumir un gran volumen de datos.
  - Incapacidad de formar una opinión propia sobre algún tema en concreto.
  - Dar por hecho informaciones que no están contrastadas por ti mismo.
  - Incapacidad de manejar un volumen elevado de datos y contenidos.
  - Adicción al consumo de contenidos en las redes sociales.

  Para combatir la infoxicación se pueden seguir una serie de pautas como:

  - Selecciona pocas y buenas fuentes de información.
  - Fórmate al máximo y construye tu propio criterio.
  - Desconecta de vez en cuando.
  - Desactiva las notificaciones de las apps de tu móvil.

- Evita seguir la cultura de lo “inmediato”.

- **y el Doomscrolling.** Es el término utilizado para referirse a la acción de atracarse de noticias negativas. Sería una búsqueda compulsiva de información, pero siempre desde un punto negativo de la información.

Está claro que la Tecnología supone un amplio mundo de posibilidades, pero también es necesario que evitemos un uso inadecuado de la misma para evitar riesgos y enfermedades asociadas como las comentadas.

Módulo 4. Seguridad

4.4. Protección del entorno

4.4.1. Tecnología y ecología

- Consejos para un uso más eficiente y ecológico de nuestros dispositivos tecnológicos

4.4.2. Consumo energético

- Aplicaciones para ahorrar en tu consumo energético

4.4.1. Tecnología y ecología

- **Consejos para un uso más eficiente y ecológico de nuestros dispositivos tecnológicos**

Cada vez somos más conscientes de la eficiencia energética y el impacto medioambiental, cambiando nuestros hábitos para utilizar bombillas led o electrodomésticos de clase A+,… pero ¿Qué ocurre con nuestros dispositivos tecnológicos (ordenador, tablet, smartphone) ?

Cada vez adquirimos mayor número de dispositivos y de diferente tipología, por lo que su consumo energético y la huella ambiental asociada a ellos también crece. Utilizarlos de una forma eficiente y responsable con el Medio Ambiente no sólo contribuye a alargar su vida útil, sino también a ahorrar dinero.

Veamos **algunos consejos para utilizar nuestros dispositivos** de forma más eficiente y ecológica:

- En primer lugar, **elige el dispositivo más adecuado a tu necesidad y uso que vayas a darle**. Por ejemplo, para navegar por Internet quizá con una tablet sea suficiente. En el caso de un uso profesional continuado, probablemente la mejor opción será uno de escritorio. Ten en cuenta que el consumo energético de un portátil es menor que el de un ordenador de sobremesa, y una tablet consume menos que un portátil. Además, el etiquetado de los ordenadores y dispositivos (como por ejemplo, la conocida etiqueta Energy Star) puede darnos información muy importante a la hora de decidirnos por un modelo más ecológico.

- **Debes saber que la pantalla es lo que más energía consume**, por ello es importante que configures tus dispositivos para minimizar este impacto. Por ejemplo:

    - Configura el modo de ahorro de energía en el ordenador (hibernar, suspender, etc.) para que se ejecute automáticamente en momentos que no lo utilices.

- En el caso del teléfono, acorta el tiempo de espera para su bloqueo automático.
- Reduce el brillo de la pantalla. A más brillo y contraste, mayor gasto energético, tanto en el ordenador como en dispositivos móviles.

- **Otras medidas que contribuyen a consumir menos** son:
  - Desconectar completamente los dispositivos si no se usan. Tampoco hay que olvidarse de los periféricos (impresoras, escáneres, etc.) que se deben mantener apagados, salvo cuando se necesitan.
  - No dejar el móvil con cargador enchufado a la corriente durante largos periodos de tiempo y evitar cargar el dispositivo mediante un puerto USB.
  - Evitar abrir muchos programas a la vez, o tener aplicaciones activadas en segundo plano.
  - Desactivar las funciones que no estés usando como bluetooth, GPS, wifi, etc.
  - Procurar apagar el móvil cuando duermas o, en su defecto, utilizar el modo avión.

Por último, antes de sustituir nuestros dispositivos por otros nuevos, debemos valorar si es posible alargar su vida útil. Si se actualizan ciertos componentes, como la memoria RAM, o se añade más disco duro, se logrará que duren más tiempo, ahorrando dinero y generando menos residuos. Otra opción sería dárselo a un amigo o familiar que no necesite un ordenador o móvil tan potente o donarlo a una ONG.

Y en última instancia, cuando ya no funcionen, siempre reciclarlos llevándolos al punto limpio más cercano. Todos los dispositivos electrónicos están fabricados con componentes que no son biodegradables, pero que además en muchos casos son altamente contaminantes, como las baterías. Por eso, es muy importante que nos concienciemos de la importancia de deshacernos de ellos adecuadamente.

Como hemos podido ver, son recomendaciones y consejos sencillos que están en nuestra mano para conseguir hacer un uso más inteligente y responsable de la tecnología que nos rodea.

4.4.2. Consumo energético

- **Aplicaciones para ahorrar en tu consumo energético**

Los aparatos electrónicos, ya sean ordenadores u otros que podemos englobar dentro de lo que es la "domótica" (tecnologías que se orientan al control y la automatización inteligente de viviendas) o los objetos conectados del Internet de las cosas (IoT) consumen energía que dejan huella en el planeta.

En el caso de aparatos cuyo gasto energético sea a través de luz, existen aplicaciones móviles y otras herramientas que podemos usar para ahorrar en nuestra factura de la luz.

Estas aplicaciones permiten calcular el precio de la luz a tiempo real mostrando las tarifas de electricidad que mejor se adapten a nuestro perfil de consumo o incluso simular la factura de la luz para que a fin de mes no nos llevemos un susto.

Entre estas aplicaciones y herramientas para ahorrar en nuestro consumo de luz. Podemos citar las siguientes:

- **App "Ahorra en luz"**. Esta aplicación permite elegir la tarifa de luz del hogar, indicando el precio actual del KWh y el de la hora más barata del día. Así, conociendo el precio medio del día y el porcentaje de diferencia entre la hora más cara y la más barata podremos saber qué horario es el idóneo para usar ciertos aparatos en nuestro hogar.

- **Calculadora de consumo en "Stand by"**. Con esta aplicación de la Organización de Consumidores y Usuarios (OCU) se puede conocer el consumo de los aparatos que dejamos encendidos en las tomas de corriente o lo que se conoce como modo "reposo" o "standby" para saber cuál es el consumo real de luz y lo que se pierde a diario teniendo los dispositivos en este modo.

- **Comparador de mejores tarifas de gas y electricidad**. La OCU también dispone en su web de un comparador de tarifas de suministro de estas dos energías para poder elegir la opción que nos ayude a ahorrar en estos gastos.

Cuando imaginamos un aparato eléctrico solemos pensar en consumo de electricidad, pero también la tecnología puede ser una gran aliada para la mejora de la eficiencia energética. En este caso hablamos de los sistemas de domótica y sus aplicaciones para ahorrar energía.

Gracias al Internet de las Cosas o IoT, el disponer de las ventajas de la domótica desde un teléfono móvil o un reloj inteligente es ya una realidad.

El control domótico puede ayudar a ahorrar electricidad, combustible y agua a través de:

- **Control de la iluminación**. Con sistemas domóticos de iluminación existe la posibilidad de controlar el encendido y apagado de las luces en caso de que se nos haya olvidado apagar alguna luz o adaptar la intensidad de la luz en función de las condiciones ambientales y la época del año o elegir la tonalidad de la luz de las bombillas para iluminar de manera eficiente.

- **Sistemas de domótica para la climatización.** Si lo que buscamos es encontrar la temperatura ideal, existen soluciones domóticas que detectan la

temperatura ambiente para programar el aire acondicionado y la calefacción a través de termostatos inteligentes. Estos dispositivos “leen” la temperatura del exterior y de la estancia y deciden la temperatura idónea evitando derrochar energía.

- **Programación de los electrodomésticos**. Teniendo en cuenta los “tramos horarios de luz”, los sistemas domóticos son capaces de programar la hora de puesta en marcha de los electrodomésticos y así ponerlos en funcionamiento de manera automática en esos momentos concretos.

- **Control a través de teléfono móvil**. El manejar el sistema domótico se puede hacer a través de un dispositivo inteligente como un teléfono móvil o una tablet. Desde abrir y cerrar las persianas de las ventanas para aprovechar la luz solar hasta apagar las luces de cualquier lugar puede hacerse a través de un único dispositivo. Además, este control inteligente también puede detectar fallos y averías en los aparatos como fugas de electricidad como las que hacen saltar el diferencial.

- **Monitorización del consumo**. El conocer nuestros hábitos de consumo ayuda a crear un perfil del consumo de energía así como, por ejemplo, saber qué electrodomésticos consumen más.

Con todos estos recursos podremos mejorar tanto el consumo de forma eficiente como el ahorro a fin de mes.