

Competencias digitales avanzadas

Pedro Mas Alique

Incluye más de

200
actividades

IFCT46



Competencias digitales avanzadas

Competencias digitales avanzadas

Pedro Mas Alique

Paraninfo

Competencias digitales avanzadas

© Pedro Mas Alique

Gerente Editorial

María José López Raso

Equipo Técnico Editorial

Paola Paz Otero
Sofía Durán Tamayo

Editora de Adquisiciones

Carmen Lara Carmona

Producción

Nacho Cabal Ramos

Diseño y maquetación

Eva Zuazua

Reservados los derechos para todos los países de lengua española. De conformidad con lo dispuesto en el artículo 270 del Código Penal vigente, podrán ser castigados con penas de multa y privación de libertad quienes reprodujeran o plagiaran, en todo o en parte, una obra literaria, artística o científica fijada en cualquier tipo de soporte sin la preceptiva autorización. Ninguna parte de esta publicación, incluido el diseño de la cubierta, puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este electrónico, químico, mecánico, electroóptico, grabación, fotocopia o cualquier otro, sin la previa autorización escrita por parte de la Editorial.

Todas las marcas comerciales y sus logos mencionados en este texto son propiedad de sus respectivos dueños.

COPYRIGHT © 2022 Ediciones Paraninfo, SA
1.ª edición, 2022

C/ Sierra de Guadarrama 35. Naves 2, 3, 4 y 5
Pol. Ind. San Fernando II,
28830 San Fernando de Henares
Teléfono: 914 463 350
clientes@paraninfo.es / www.paraninfo.es

ISBN: 978-84-283-5642-8
Depósito legal: M-19135-2022
(25.634)

Impreso en España
Printed in Spain

Cimapress
(Arganda del Rey, Madrid)

Paraninfo

El presente libro desarrolla el Módulo Formativo de **Competencias Digitales Avanzadas (Código: IFCT46)**, con una duración de 60 horas. Pertenece a la familia profesional de Informática y Comunicaciones, y está asociado al área profesional de Sistemas y Telemática.

La estructura organizativa de sus contenidos corresponde fielmente a la establecida por la normativa vigente y más concretamente a los contenidos del Módulo Formativo de **Competencias Digitales Avanzadas**.



Las unidades del libro se acompañan de multitud de **recursos didácticos** que ayudarán a la mejor comprensión de la materia de estudio:

- Desarrollo del currículo oficial.
- Lenguaje claro y sencillo que favorece la comprensión.
- Explicaciones exhaustivas y rigurosas, pero también amenas y asequibles.
- Gran cantidad de fotografías y tablas explicativas.
- Recuadros con información complementaria.
- Argot técnico con los términos más relevantes para facilitar su consulta.
- Actividades propuestas intercaladas con la teoría.
- Ejemplos reales para ilustrar los contenidos teóricos.
- Actividades finales de comprobación de tipo test y actividades de aplicación en todas las unidades.



Este libro cuenta con el **solucionario** de las actividades incluidas en el libro al que puede accederse previo registro, desde la ficha web de este libro en www.paraninfo.es.

Solucionario disponible en

www.paraninfo.es

Contenido



1. Configuración básica del sistema operativo	1
1.1. Actualizaciones automáticas	2
1.2. Instalación de nuevos programas	12
1.3. Instalación de drivers de periféricos	20
1.4. Instalación de certificados digitales	24
1.5. Configuración de redes de datos	28
Actividades finales	34
2. Tratamiento de la información	39
2.1. Técnicas avanzadas de búsqueda	40
2.1.1. Operadores de búsqueda en buscadores	44
2.1.2. Otras fuentes de información	47
2.1.3. Conclusiones	51
2.2. Curación de contenidos	54
2.2.1. Técnicas de detección de veracidad de la información	58
2.2.2. Fuentes de contenidos digitales abiertos	63
2.3. Almacenamiento de contenido en la nube (Dropbox, Google Drive, OneDrive de Microsoft)	67
2.3.1. Dropbox	68
2.3.2. Google Drive	70
2.3.3. OneDrive	71
Actividades finales	73
3. Comunicación	77
3.1. Compartir información	78
3.1.1. Foros, wikis, etcétera	79
3.1.2. Uso básico de redes sociales como medio de comunicación	84

3.2. Comunicación mediante tecnologías digitales	88
3.2.1. Comunicación textual: chats, sistemas de mensajería, etcétera	89
3.2.2. Comunicación audiovisual: videoconferencia (Skype, Google Hangouts, etcétera)	92
3.2.3. Herramientas colaborativas	93
3.3. Normas de conducta y peligros	100
3.3.1. Ciberacoso	104
3.3.2. Suplantación de identidad	105
Actividades finales	108
4. Creación del contenido	113
4.1. Herramientas ofimáticas (hoja de cálculo y base de datos)	114
4.1.1. Hoja de cálculo	118
4.1.2. Base de datos	121
4.2. Retoque básico de imágenes	123
4.3. Derechos de autor y licencias	131
Actividades finales	135
5. Seguridad	139
5.1. Protección del ordenador	140
5.1.1. Antivirus o antimalware	142
5.1.2. Firewall	148
5.1.3. Conclusión	151
5.2. Protección del dispositivo móvil	152
5.3. Protección de la red de datos	155
Actividades finales	162
6. Resolución de problemas	167
6.1. Detección y eliminación de virus y troyanos	168
Actividades finales	184



Configuración básica del sistema operativo

En esta unidad vamos a comentar las actualizaciones automáticas del sistema operativo (SO), que contribuyen a mantenerlo en condiciones óptimas de operatividad, así como la instalación de programas, periféricos y certificados digitales, para un mejor y más seguro uso del equipo.

Pero el uso de los equipos no sería el más adecuado si no supiéramos cómo configurar una red de datos para la interconexión, segura, con otros usuarios; también indicaremos cómo hacerlo.

Contenido

- 1.1. Actualizaciones automáticas
- 1.2. Instalación de nuevos programas
- 1.3. Instalación de drivers de periféricos
- 1.4. Instalación de certificados digitales
- 1.5. Configuración de redes de datos



1.1. Actualizaciones automáticas

Antes de comentar las actualizaciones del SO, conviene recordar las diversas definiciones de sistema operativo:

Sistema operativo, Programa o conjunto de programas que realizan funciones básicas y permiten el desarrollo de otros programas¹.

Un sistema operativo (SO) es el programa que, después de ser cargado inicialmente en la computadora, administra todos los demás programas de aplicación en esta. Además, los usuarios pueden interactuar directamente con el sistema operativo².

El sistema operativo es responsable básicamente del procesamiento de los programas por el computador y asegura, por ejemplo, que los recursos de software sean proporcionados cuando se les necesite³.

Para una mejor comprensión, vamos a utilizar la siguiente definición de SO:

Un SO es un programa, o conjunto de programas, que, una vez cargado en el ordenador, permite al usuario interactuar con él para hacer posible la ejecución de los demás programas del ordenador⁴.

Realmente, el SO es el programa que nos permite usar un ordenador.

RECUERDA

Cuando a lo largo de esta obra citemos el término ordenador, este se referirá exclusivamente a ordenadores personales, portátiles o de sobremesa, de cualquier tipo y marca, pero en ningún caso se hará referencia a los grandes ordenadores cuyo uso y comprensión del modo de funcionamiento caen totalmente fuera del alcance de la obra.

Hemos de ser conscientes de que tanto el hardware como el software evolucionan, por lo que el SO debe permitir el funcionamiento del equipo a lo largo del tiempo, pero también debemos tener en cuenta que los sistemas operativos tienen distintas versiones y que, llegado un momento, ese, a veces delicado, equilibrio entre hardware y software se rompe y tenemos que tomar decisiones que afectan tanto al equipo como a los programas.

Como siempre, recomendamos aprender de los mejores. Veamos lo que dice la Oficina de Seguridad del Internauta (OSI) sobre las actualizaciones:

¹ <https://dle.rae.es>

² <https://www.computerweekly.com/es/definicion/Sistema-operativo>

³ https://pcweb.info/sistema-operativo/#Que_hace_un_sistema_operativo

⁴ Mas Alique, P. (2022): *Competencias digitales básicas*. Madrid: Ediciones Paraninfo.

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Si no mantenemos nuestros equipos al día nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etcétera.

Por tanto, si queremos disfrutar de las ventajas de la tecnología debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de actualizaciones automáticas siempre que esté disponible.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad⁵.

Siguiendo las indicaciones de la OSI, veamos cómo proceder para configurar las actualizaciones automáticas de los distintos sistemas operativos.

Recordemos que los sistemas operativos más utilizados en ordenadores son Windows, macOS, Linux y Chrome OS, y en móviles y tabletas, iOS y Android.

Empecemos con Windows. En 2022 Microsoft ha lanzado Windows 11 y sigue actualizando Windows 10.



Figura 1.1. Windows 10 y 11 de Microsoft.

Supongamos que nuestro ordenador tiene instalado Windows 10; lo primero que vamos a hacer es comprobar si el equipo es compatible con Windows 11.

Buscamos en un buscador «Cómo instalar Windows 11» y llegamos a la pantalla que aparece en la Figura 1.2. Picamos en *Antes de comenzar* y nos lleva a la pantalla de la Figura 1.3.

⁵ <https://www.osi.es/es/actualizaciones-de-seguridad>



Figura 1.2. Windows 11.

En la pantalla de la Figura 1.3 picamos en *especificaciones de dispositivo de Windows 11* y llegamos a la pantalla de la Figura 1.4. Picamos en *comprobación de estado del PC*, descargamos el programa que nos indica, lo ejecutamos (Figura 1.5), y llegamos a la conclusión de que en este equipo no se puede instalar la versión 11 (Figura 1.6).

Por ahora no pasa nada, pero es un buen ejemplo de lo que puede suceder con determinados equipos al tratar de instalar la última versión de un SO.

Podemos seguir trabajando con la versión 10 y veremos cómo se actualiza; después comentaremos la situación de estos equipos.

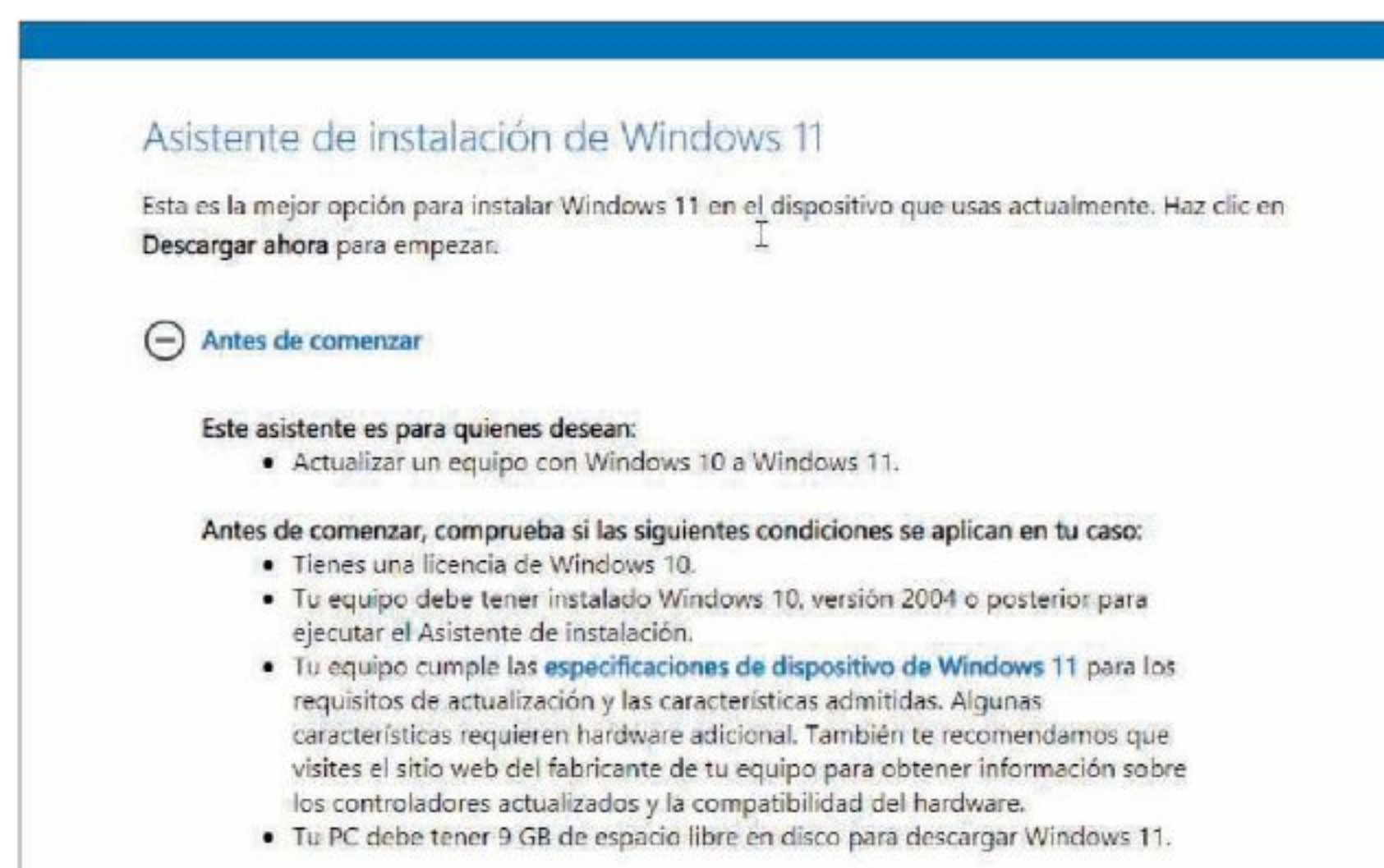


Figura 1.3. Windows 11.

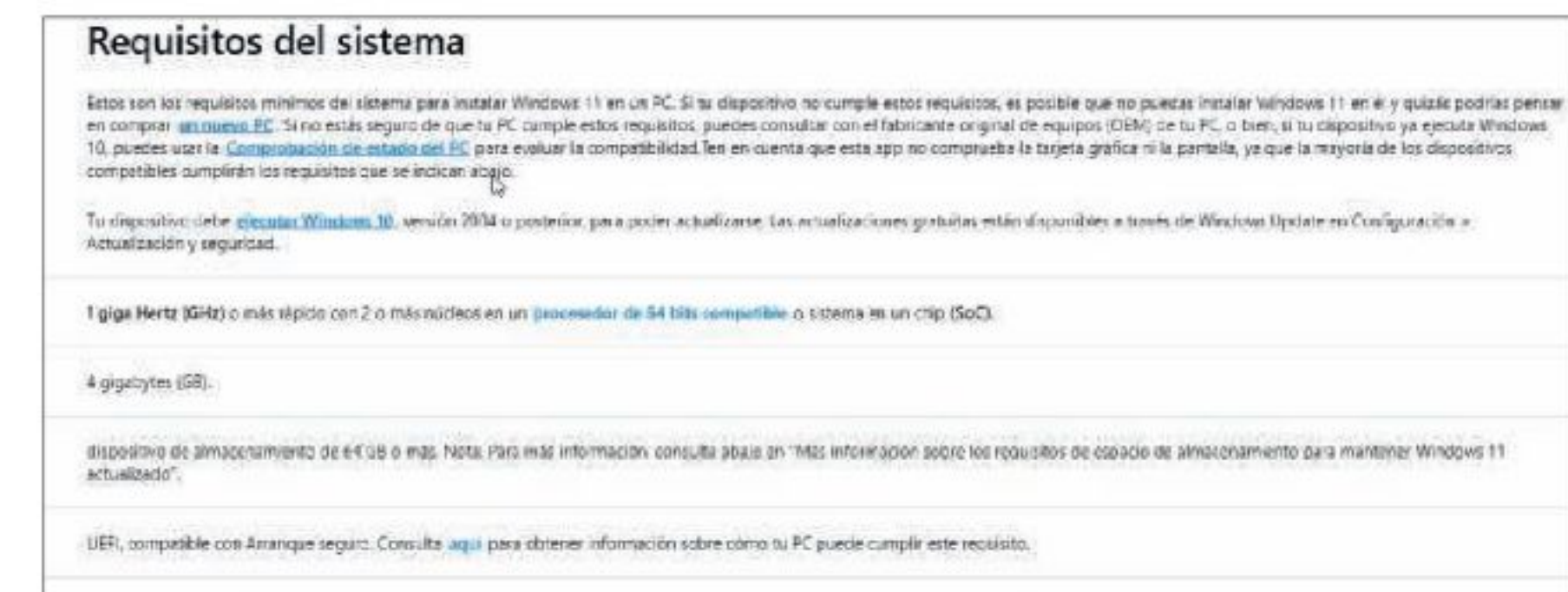


Figura 1.4. Windows 11.

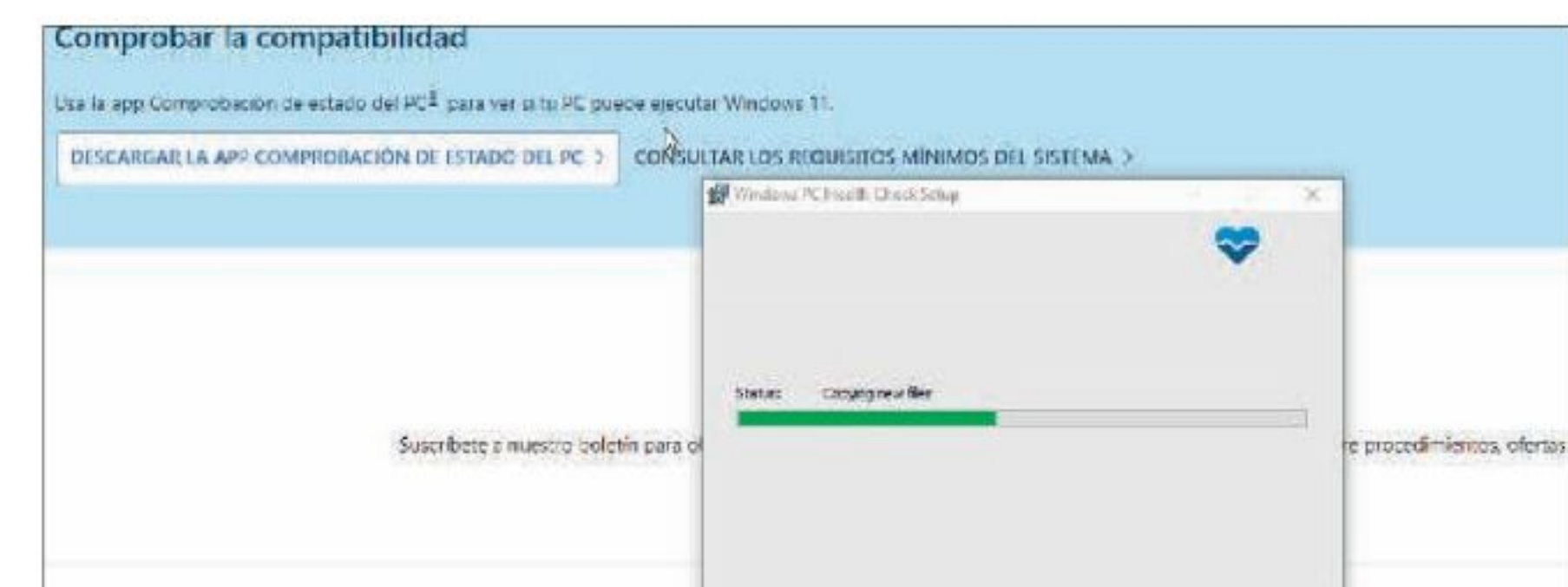


Figura 1.5. Windows 11.

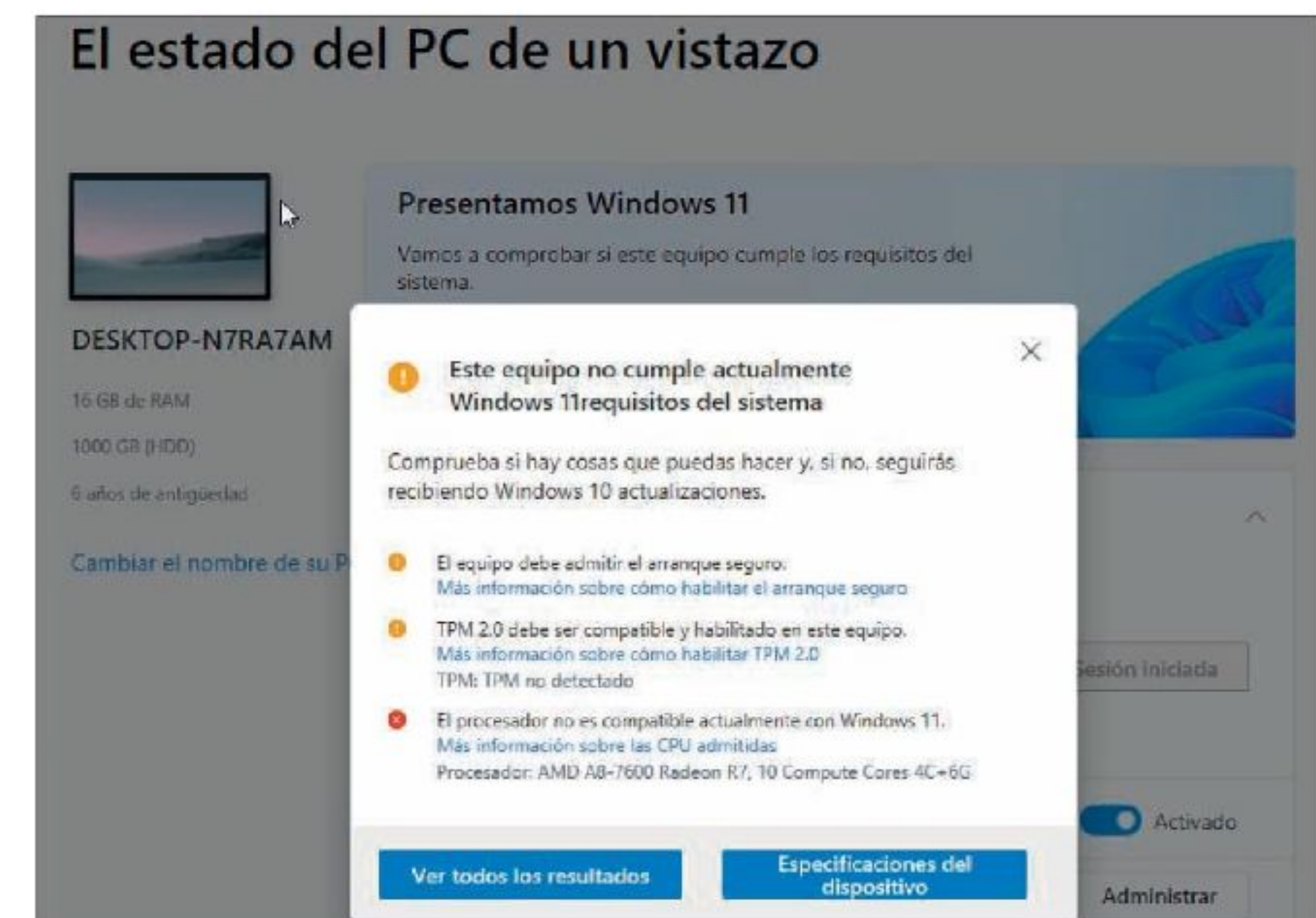


Figura 1.6. Windows 11.



Veamos las actualizaciones de Windows 10; en primer lugar, buscamos *Actualizaciones* en nuestro ordenador y aparece la pantalla de la Figura 1.7. Picamos en *Buscar actualizaciones* y, tras instalar la que hay pendiente, vemos la pantalla de la Figura 1.8.



Figura 1.7. Actualizar Windows 10.



Figura 1.8. Actualizar Windows 10.

Las actualizaciones son de dos tipos, las que el proveedor del SO considera importantes, que se actualizan automáticamente, y las menos importantes u opcionales que se instalan a criterio del usuario. Hay que revisar periódicamente la situación de actualización y la recomendación es instalar todas las pendientes.

No olvidemos que, para actualizarse, el equipo tiene que estar conectado a internet.

Hemos visto la situación de un equipo con Windows 10 que sigue actualizando su SO, aunque no admite Windows 11, lo cual sucede con las versiones a las cuales el proveedor del SO, en este caso Microsoft, da soporte, pero también podemos tener un equipo con versiones anteriores de Windows.

Las versiones anteriores a la 10 son la 8, de 2012, y la 7, de 2009. Aunque son bastantes años en la vida de un PC, vamos a ver la situación de ambas versiones.



Figura 1.9. Windows 7 y 8.

- **Windows 7:** Microsoft se comprometió a proporcionar 10 años de soporte técnico de producto para Windows 7 cuando se publicó el 22 de octubre de 2009. Este período de 10 años ya ha finalizado y Microsoft ha dejado de ofrecer soporte técnico de tecnologías más recientes y en ofrecer excelentes experiencias nuevas. El día específico en que finalizó el soporte técnico para Windows 7 fue el 14 de enero de 2020. La asistencia técnica y las actualizaciones de software de Windows Update que ayudan a proteger tu equipo ya no están disponibles para el producto. Microsoft recomienda firmemente que pases a Windows 10 para evitar situaciones en las que puedas necesitar servicio o soporte técnico que ya no esté disponible⁶.
- **Windows 8:** Windows 8.1 alcanzó la finalización del soporte estándar el 9 de enero de 2018 y la finalización del soporte extendido será el 10 de enero de 2023. Dada la disponibilidad general de Windows 8.1, los clientes que usaban Windows 8 tuvieron hasta el 12 de enero de 2016 para migrar a Windows 8.1 y poder seguir recibiendo soporte técnico. Windows 8.1 no cambia los requisitos de hardware en comparación con Windows 8 y las aplicaciones existentes de Microsoft Store funcionarán con Windows 8.1⁷.

Si estamos usando una de estas versiones, conviene que tengamos cuidado y veamos la posibilidad de pasar a la versión 10.

Como vemos, no debemos estar atentos solamente a las actualizaciones de una versión determinada, sino a la vida de esa versión y a la evolución recomendada por el proveedor del SO.

Para terminar con Windows, si nuestro equipo con Windows 10 es apto para trabajar con la versión 11, pensemos si merece la pena hacerlo, ya que las versiones más modernas suelen consumir más recursos.

Un comentario general antes de seguir con otros SO: si nuestro ordenador ha estado tiempo apagado, lo primero es comprobar si el SO está actualizado. Conviene tenerlo en cuenta antes de empezar a trabajar con él.

⁶ <https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962>

⁷ <https://docs.microsoft.com/es-es/lifecycle/faq/windows>



Vamos a comentar las actualizaciones de macOS, pero antes una pequeña historia de las distintas versiones, con alguna curiosidad:

Aunque públicamente se usan nombres de felinos, internamente en la empresa se utilizan nombres de vinos (a excepción de OS X 10.6 y macOS 10.13, los dos sistemas que no tuvieron ningún nombre en código).

Incluso después de que Apple cambiara los nombres en código a sitios de California en 2013 siguieron utilizándose nombres de vinos internamente hasta el año 2014. En 2015, Apple volvió a cambiar los nombres en código esta vez por nombres de tipos de manzana.

Un año después, en 2016, la empresa de la manzana decidió unificar la marca de sistemas operativos de Mac OS X a macOS, unificándose así con sistemas operativos de otros productos Apple como iOS, tvOS o watchOS.

A continuación, te ofrecemos una lista completa con los nombres en código públicos de las versiones de OS X, junto con los nombres en código que se utilizaron internamente (en caso de que se utilizara alguno).

Nombres en código de Mac OS X & macOS:

- OS X 10 beta: Kodiak - 13 septiembre 2000.
- OS X 10.0: Cheetah - 24 marzo 2001.
- OS X 10.1: Puma - 25 septiembre 2001.
- OS X 10.2: Jaguar - 24 agosto 2002.
- OS X 10.3 Panther (Pinot) - 24 octubre 2003.
- OS X 10.4 Tiger (Merlot) - 29 abril 2005.
- OS X 10.4.4 Tiger (Chardonnay).
- OS X 10.5 Leopard (Chablis) - 26 octubre 2007.
- OS X 10.6 Snow Leopard - 28 agosto 2009.
- OS X 10.7 Lion (Barolo) - 20 julio 2011.
- OS X 10.8 Mountain Lion (Zinfandel) - 25 julio 2012.
- OS X 10.9 Mavericks (Cabernet) - 22 octubre 2013.
- OS X 10.10: Yosemite (Syrah) - 16 octubre 2014.
- OS X 10.11: El Capitan (Gala) - 30 septiembre 2015.
- macOS 10.12: Sierra (Fuji) - 20 septiembre 2016.
- macOS 10.13: High Sierra (Lobo) - 25 septiembre 2017.
- macOS 10.14: Mojave (Liberty) - 24 septiembre 2018.
- macOS 10.15 Catalina (Jazz) - 7 octubre 2019.
- macOS 11 Big Sur - 12 noviembre 2020.
- macOS 12 Monterey - octubre 2021⁸.

⁸ <https://www.macworld.es/articulos/software-mac/nombres-versiones-mac-os-x-macos-3685567>



Como vemos hay prácticamente una versión por año, y para actualizar a la versión Monterey, hay que seguir las instrucciones de la web de Apple (Figura 1.10).



Figura 1.10. macOS Monterey.

La forma de proceder es enteramente similar a la descrita para el paso de Windows 10 a 11: se trata de seguir las instrucciones del fabricante.

Para obtener información sobre versiones, actualizaciones y compatibilidad de equipos, lo mejor es visitar la web de Apple, pues además de sacar una versión nueva cada año, hay constantes actualizaciones.

La forma de actualizar los distintos SO es similar en cuanto al método, por lo que se planteará una actividad recomendada para que las personas interesadas en los demás sistemas operativos puedan practicar.

Al igual que los SO de los ordenadores se actualizan, también lo hacen los de los móviles y tabletas.

Pero a la hora de comparar la evolución de sistemas operativos tipo Android con los de los ordenadores personales hay que tener en cuenta que la utilización del ordenador personal, cuando no se usa para trabajar, suele ser para navegar por internet y para jugar; de hecho, hay toda una gama de ordenadores para jugar (lo que en cierta publicidad se denomina ordenadores de gaming) que requieren unas características determinadas cuyos usuarios conocen bien. En la Figura 1.11 se muestra un ordenador de gaming OMEN de la marca HP cuyo precio está por encima de los 3000 €; por ese precio, conviene saber lo que se compra.



Figura 1.11. Ordenador para juegos.

Una buena opción para el usuario que no juega o que no lo hace habitualmente es adquirir un ordenador de gaming de gama baja, pues suelen tener una gran capacidad de RAM, que facilita las tareas cotidianas.

El aumento del teletrabajo hace que puedan surgir nuevas necesidades en los ordenadores personales, al tener que trabajar en remoto y conectados a diversas aplicaciones con mayores requerimientos de seguridad y administradas por las empresas, pero es simplemente cuestión de definir bien las características del equipo, pues ese tipo de equipos ya están en el mercado.

En el caso de los móviles y de las tabletas la situación es un poco distinta, pues cada vez se incluyen más funcionalidades en estos equipos; por ejemplo, las relacionadas con el coche conectado.

En la Figura 1.12 se muestra una captura de pantalla de la web de Android, en la que podemos apreciar que se hace referencia al móvil y a la tableta, pero también a la TV, al reloj y al coche.

Las actualizaciones se vuelven cada vez más críticas para hacer funcionar todo el universo Android.



Figura 1.12. Android.



Google lanzó en 2021 la versión 12 de Android. Para ver la situación de nuestro dispositivo, lo mejor es ir a la web de ayuda de Google⁹, desde la cual podemos ir a la web de Android 12¹⁰.

No todos los dispositivos soportan las continuas actualizaciones, por lo que hay que tener claro el uso que le queremos dar; así evitaremos el continuo cambio de móvil, que muchas veces es puro consumismo.

Lo mismo sucede dentro del entorno Apple. En su web de soporte¹¹ se indican las últimas versiones y cómo proceder, y, al igual que en la web de Android, también hace referencia a los relojes, televisión (Apple TV), móviles y tabletas.

► ACTIVIDAD PROPUESTA 1.1

Actualizar los sistemas operativos

Busque la lista de los sistemas operativos más utilizados. Puede eliminar Windows y macOS, ya comentados, y elegir los tres siguientes más utilizados en ordenadores.

Una vez elegidos los tres SO que se va a estudiar, proceda de la siguiente manera:

- Busque información sobre las versiones lanzadas en los últimos 10 años, o en el periodo que considere adecuado.
- Estudie los requisitos necesarios en los equipos para que soporten las distintas actualizaciones.
- Saque las conclusiones pertinentes.

► ACTIVIDAD PROPUESTA 1.2

Sistemas operativos para móviles

Aunque Android e iOS cubren una gran parte del mercado, no son los únicos SO utilizados en teléfonos móviles.

- Busque información sobre otros SO, los más utilizados sin tener en cuenta iOS y Android.
- Estudie su aplicación, vigencia, actualizaciones, etcétera.
- Saque las conclusiones pertinentes.

⁹ <https://support.google.com/android/answer/7680439?hl=es#zippy=%2Ccu%C3%A1ndo-se-activan-las-actualizaciones>

¹⁰ <https://www.android.com/android-12>

¹¹ <https://support.apple.com/es-lamr/HT201222>

1.2. Instalación de nuevos programas

Para hacer el uso deseado de nuestros equipos necesitamos programas que ejecuten las tareas necesarias; al comprar un ordenador suele venir con el SO instalado (aunque no siempre, es algo que hay que comprobar al adquirirlo), y puede incorporar algunos programas.

Pero, sea cual sea la situación del equipo, es habitual tener que instalar nuevos programas; de ahí la necesidad de aprender a hacerlo.

Antes de seguir hay que hacer una reflexión sobre las diferencias entre programa y aplicación, pues al igual que se instalan nuevos programas se instalan aplicaciones, sobre todo en los dispositivos móviles.

Sin entrar en demasiados detalles, podemos decir que un programa es más general que una aplicación, hace más cosas y suele necesitar más recursos: no es lo mismo descargar e instalar el paquete Microsoft Office completo en un ordenador que instalar la aplicación de tratamiento de textos en un móvil. Además, los programas incorporan archivos ejecutables para su instalación.

Pero tanto en un caso como en otro hay que tomar una serie de precauciones antes de instalar nada en nuestros dispositivos.

Los programas y las aplicaciones pueden ser gratis o de pago, y en ambos casos deben ser originales y descargarse desde sitios de confianza.

Usar software pirata, además de ser delito, es peligroso para la seguridad personal y de los equipos.

Lo recomendable es descargarlos desde la web del proveedor del programa o aplicación o desde la Play Store o el Apple Store.

En las Figuras 1.13 y 1.14 vemos capturas de pantalla de la Play Store de Google y de la Apple Store de Apple, que también están disponibles en el móvil o en la tableta.

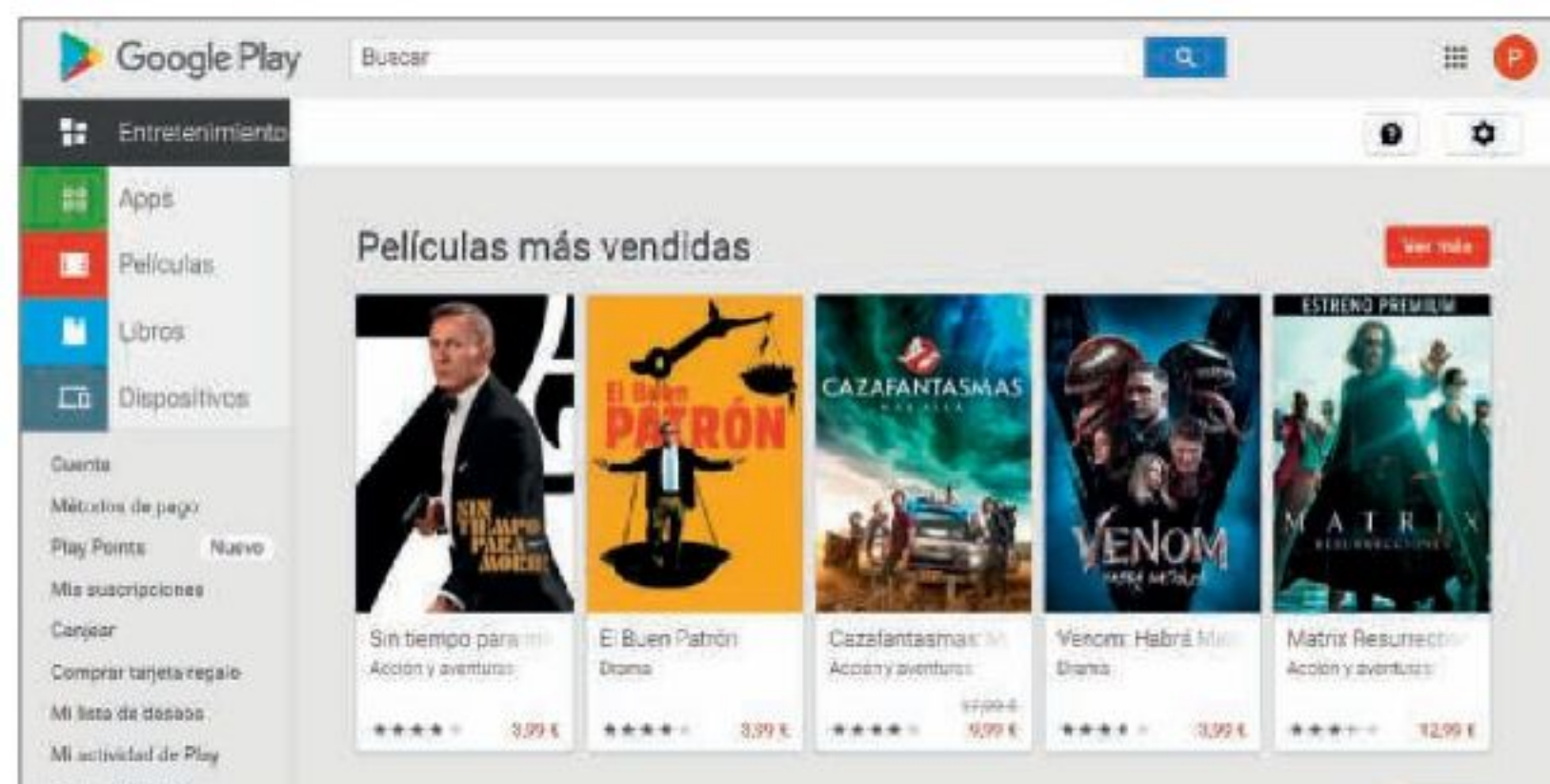


Figura 1.13. Play Store.



Figura 1.14. Apple Store.

Como ejemplo de instalación de un nuevo programa vamos a instalar Acrobat Reader, que es un programa que permite leer documentos en formato PDF; mucha información disponible en la red y muchos libros electrónicos libres están en este formato, por eso hemos elegido este ejemplo.

Lo primero es buscar el programa en internet, ir al sitio y proceder a la descarga. En la Figura 1.15 podemos ver la búsqueda que hemos hecho en Bing. Hay que buscar la web original del programa, en este caso Adobe, pues en primer lugar no aparece esta, sino otras que ofrecen programas similares que no son el que buscamos. Como en este caso hay distintas alternativas, vamos a la que indica *España*, es lo más adecuado.



Figura 1.15. Buscar Adobe Acrobat Reader.

Picamos en el enlace y aparece lo que se ve en la Figura 1.16 y siguientes. Basta con seguir las instrucciones, pero recomendamos seguir atentamente la secuencia de figuras y leer los comentarios que figuran a continuación antes de instalar el programa, ya que hay detalles que conviene tener en cuenta.

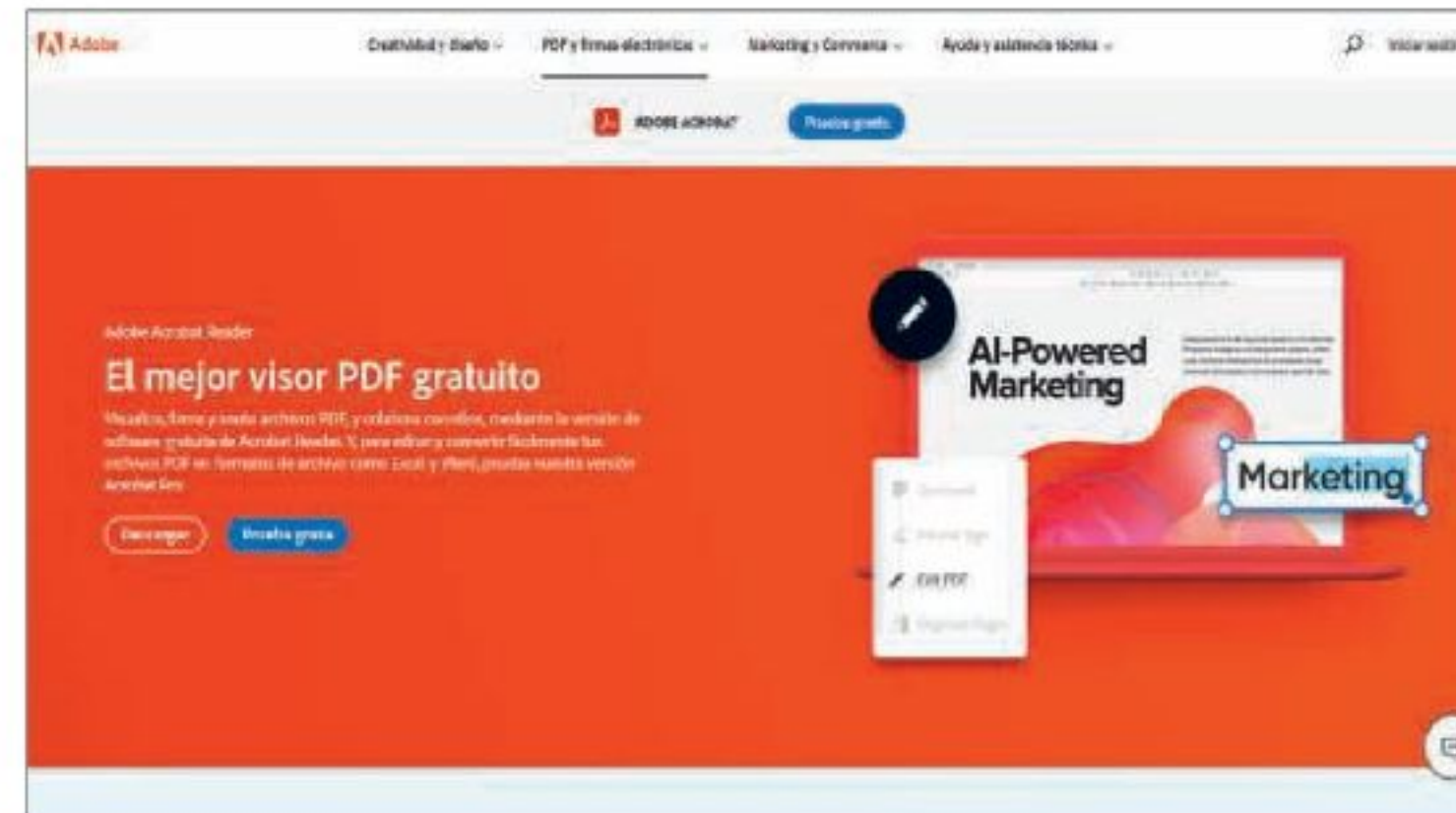


Figura 1.16. Instalar Adobe Acrobat Reader.



Figura 1.19. Instalar Adobe Acrobat Reader.

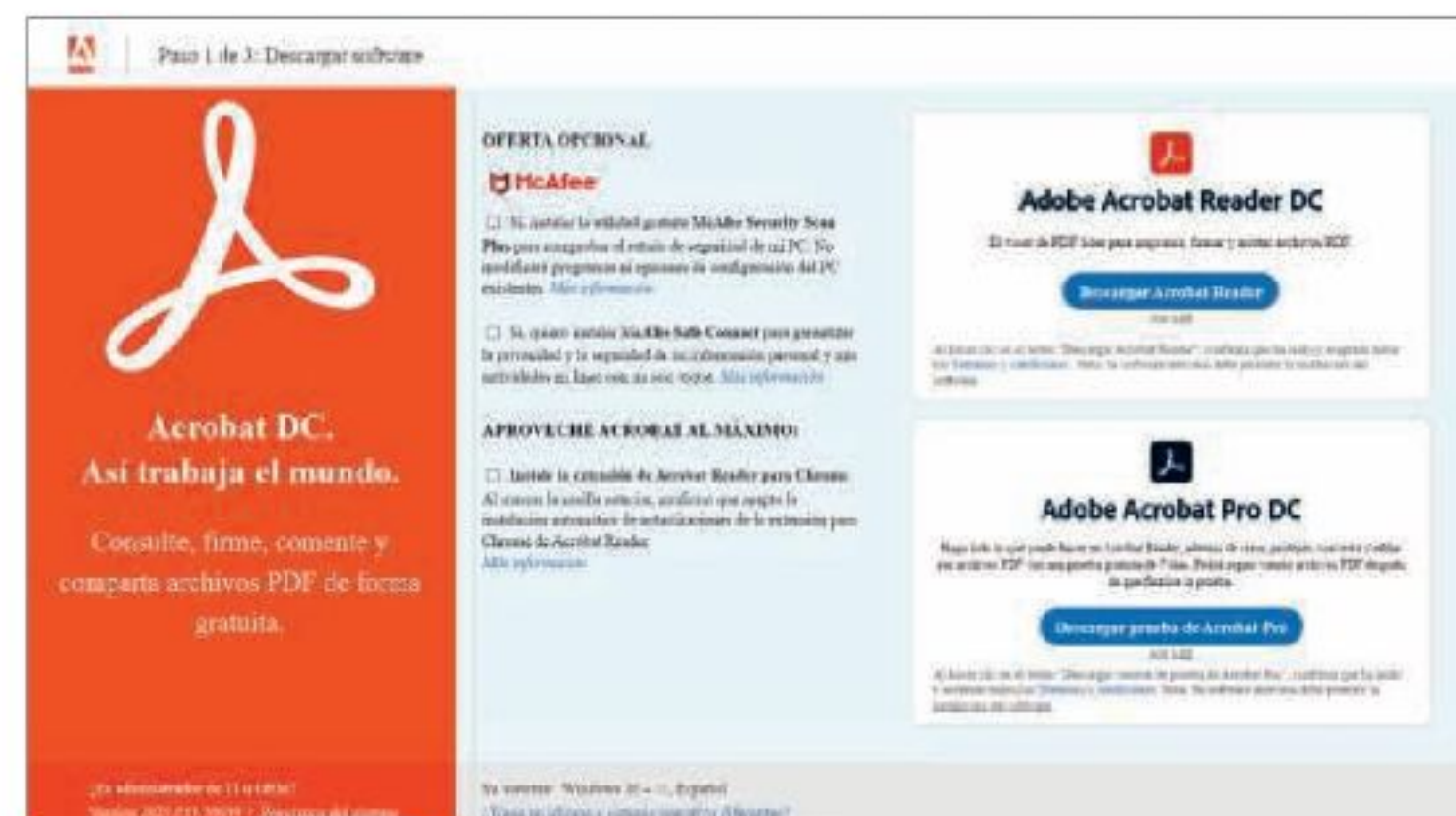


Figura 1.17. Instalar Adobe Acrobat Reader.



Figura 1.20. Instalar Adobe Acrobat Reader.

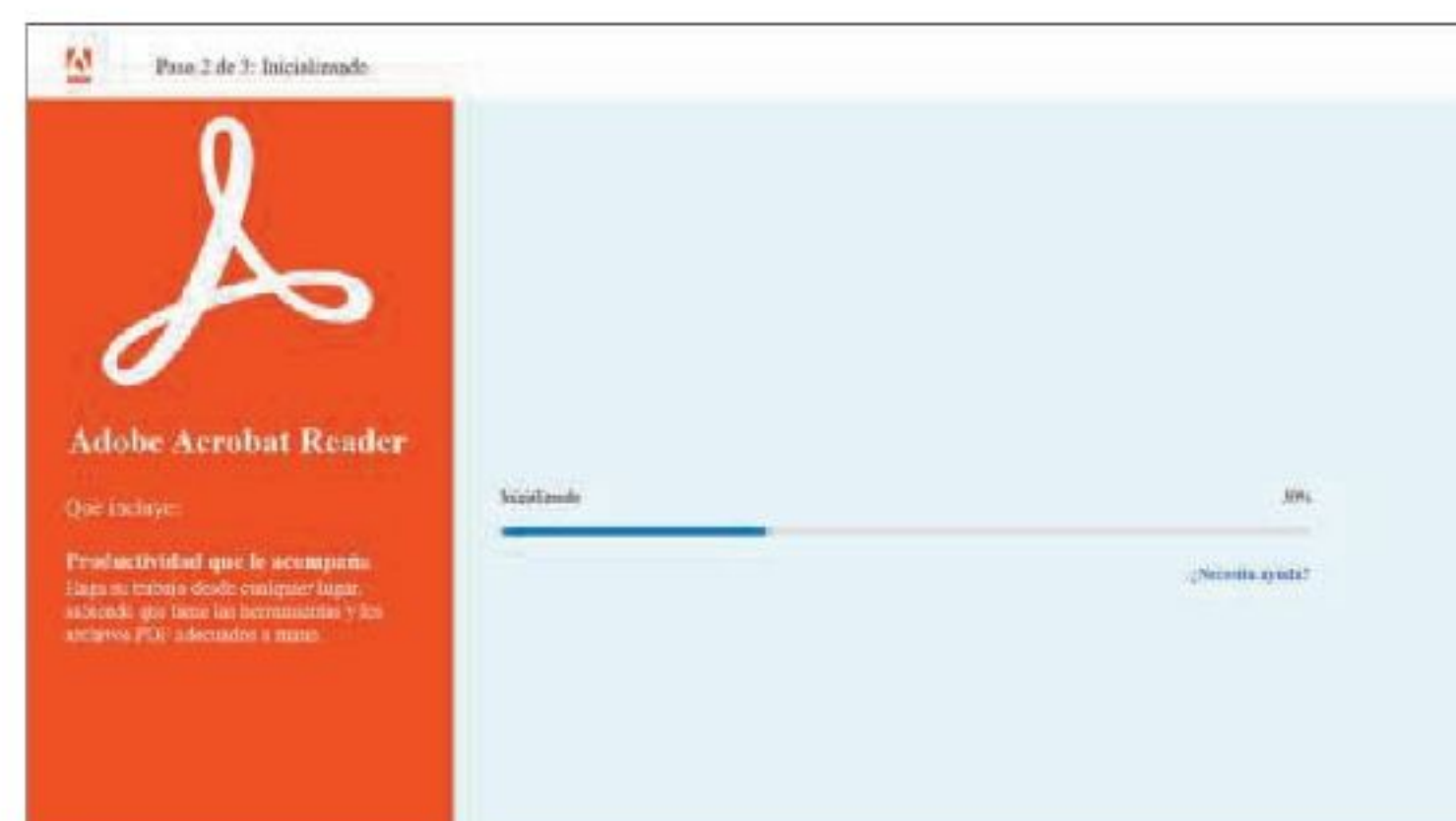


Figura 1.18. Instalar Adobe Acrobat Reader.



Figura 1.21. Instalar Adobe Acrobat Reader.

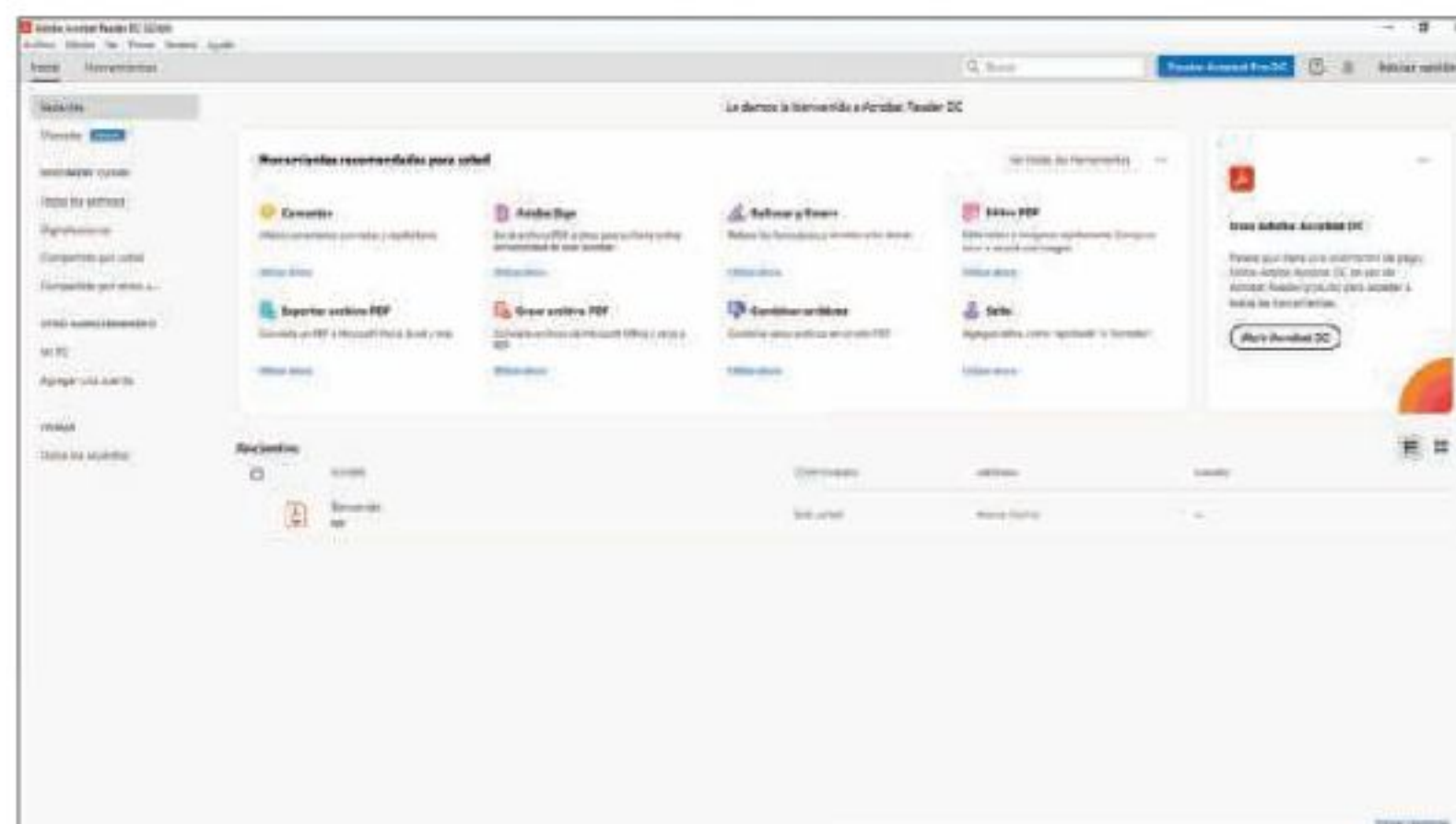


Figura 1.22. Instalar Adobe Acrobat Reader.



Figura 1.23. Instalar Adobe Acrobat Reader.

Una vez familiarizados con la secuencia de imágenes, vamos a comentar algunas cosas.

En la Figura 1.16, hay que picar en *Descargar*. Adobe ofrece todo un paquete de programas de pago y pruebas gratuitas, pero lo que queremos es descargar Acrobat Reader; no nos dejemos desviar de lo que realmente queremos hacer.

Lo mismo hay que tener en cuenta en la Figura 1.17, lo que queremos es descargar Acrobat Reader. Picamos en *Descargar Acrobat Reader*. La instalación o no de la extensión para Chrome es optativa y basta con marcarla; en este caso no se ha hecho para no perder generalidad. Una vez hecho esto, empieza el proceso de descarga.

Una vez terminada la inicialización (Figura 1.18), en la carpeta de descargas aparece el archivo ejecutable para la instalación del programa, según mostramos en la Figura 1.19, en la que hemos superpuesto la vista de la carpeta de descargas a la de la instalación del programa.

Picamos en el ejecutable y empieza la instalación propiamente dicha (Figura 1.20); cuando esta termina, el programa lo indica (Figura 1.21) y picamos en *Terminar*. El programa está instalado y si picamos en *Bienvenida* (Figura 1.22) se abre un documento explicativo (Figura 1.23).

Ya hemos instalado el programa y hemos conseguido sortear los intentos de vender-nos algo que, en este momento, no queremos, lo que es habitual en la instalación de programas gratuitos de cualquier tipo.

Dependiendo de cómo tengamos configurado el ordenador, nos ofrecerá definir Acrobat Reader como lector predeterminado de documentos en PDF. Recomendamos hacerlo.

Para el ejemplo hemos elegido Acrobat Reader por ser un programa gratuito y muy útil, en su uso y como puerta de entrada a Adobe Acrobat; pero también podemos querer probar durante un tiempo un programa de pago; es una opción que se ofrece muy a menudo y la planteamos en las actividades propuestas.

La instalación de los programas de uso habitual en los ordenadores para uso personal es similar a la descrita. Recordemos: descargar solo de sitios de confianza, siempre que sea posible de la web del proveedor del programa; usar software original, nada de piratear; y seguir nuestro camino, hacer lo que queremos aunque nos sugieran otras cosas, que suele ser para vendernos algo.

Ahora hablemos de cómo instalar aplicaciones en el móvil o en la tableta. Lo vamos a hacer desde dos puntos de vista: descarga desde el ordenador o descarga directa en el dispositivo.

Lo primero que hay que tener en cuenta es que no todas las aplicaciones están en la Play Store (o su equivalente en Apple). Las hemos citado como indicativo de sitios seguros, pero el mundo no se acaba ahí. En todo caso, si la aplicación está en la Play Store, lo recomendable es bajarla directamente de ahí, ya que es lo más fácil y lo más rápido.

Basta con buscar la aplicación en la Store y cuando aparece la opción *instalar*, pulsarla. El resto se hace solo (son smartphones o teléfonos inteligentes) y, una vez instalada, aparece el icono en la pantalla.

Para instalar una aplicación desde el ordenador hay que buscar la web correspondiente y seguir las instrucciones, siempre que tengamos el correspondiente dispositivo vinculado, como veremos al hablar de redes de datos. Esta es una buena forma de comprobar si determinada información está disponible en una aplicación para el móvil, dado el cada vez más frecuente uso del móvil.

Veamos un ejemplo. Supongamos que queremos saber si el Servicio de Salud de Castilla y León tiene una aplicación que nos permita llevar los datos de vacunación y medicación en el móvil. Primero, vistamos la página web correspondiente y en la Figura 1.24 podemos ver que figura el símbolo de un móvil y el nombre de la aplicación, *SACYL Conecta*; picamos ahí y nos lleva a la pantalla de la Figura 1.25.



Figura 1.24. Aplicación SACYL.

En la Figura 1.25 aparece SACYL CONECTA para iPhone y Android. Aplicación oficial; picamos y nos lleva a la pantalla de la Figura 1.26, que a su vez nos lleva a la Play Store. En la Figura 1.27 aparece la palabra *Instalada* en un recuadro verde, pues ya la tenemos instalada, pero cuando la aplicación está sin instalar esta pantalla indica *Instalar* y debemos picar en dicho recuadro.

Como vemos, basta con seguir las instrucciones de la web, pero como hemos indicado antes, para poder hacerlo hay que tener vinculado el teléfono móvil a la cuenta de Google para que lo reconozca al instalar la aplicación.

En este caso todo ha funcionado, pero también puede suceder que no se pueda instalar la aplicación, algo que le ha sucedido al autor al intentar instalar la App de Amazon en su móvil: el eterno problema de actualizaciones, versiones, etcétera.



Figura 1.25. Aplicación SACYL.



Figura 1.26. Aplicación SACYL.



Figura 1.27. Aplicación SACYL.

► ACTIVIDAD PROPUESTA 1.3

Ejemplo de aplicación

¿Conoce la aplicación Mi DGT?

Como otros muchos intentos de facilitar el uso de la información por parte de las Administraciones públicas, la Dirección General de Tráfico hace ya tiempo que ha lanzado su aplicación. Le proponemos las siguientes actividades:

- Vaya a la página web de la DGT y busque la aplicación.
- Instálela en su móvil.

Entrará en el mundo de la clave PIN y demás métodos de identificación habitualmente usados en los trámites con la Administración pública.

► ACTIVIDAD PROPUESTA 1.4

Instalar versión de prueba

Hemos comentado que algunos programas ofrecen versiones de prueba gratuitas. Estas versiones tienen una validez limitada, pero puede ser interesante trabajar un tiempo con ellas para ver si el programa se ajusta a nuestras necesidades; de ahí que se proponga la siguiente actividad:

- Vaya a la página web de Adobe y busque la versión de prueba de Adobe Acrobat.
- Compruebe las condiciones de la descarga, tiempo de validez, posibilidades de uso, etcétera.
- Instálela en su ordenador.

Recomendación: si una vez terminado el plazo de validez no va a instalar la versión de pago, revise que no quede nada en su ordenador. Para ello, hay que ir al panel de control y, en el apartado *Programas*, quitar lo que haya de ese programa, si es que hay algo.

1.3. Instalación de drivers de periféricos

Para empezar, necesitamos conocer las definiciones que figuran a continuación y, una vez que sabemos lo que es un periférico y un driver o controlador, debemos entender el concepto de plug and play, que se puede traducir por conectar y usar.

Empezaremos por recordar cuales son los periféricos comunes en los ordenadores de uso personal, y al final del apartado comentaremos dispositivos periféricos que, cada vez más, se usan desde el móvil o la tableta.

ARGOT TÉCNICO

- **Periférico:** aparato auxiliar e independiente conectado a la unidad central de una computadora u otro dispositivo electrónico¹².
- **Driver o controlador:** programa que hace de intermediario entre el sistema operativo y el hardware del ordenador.
- **Plug and Play:** es un estándar para añadir hardware que requiere que un dispositivo se identifique a sí mismo al conectarse. La mayoría de los sistemas informáticos de hoy en día se diseñan para ser plug and play, de modo que puedas comprarlo, llevártelo a casa, enchufarlo, y utilizarlo. Esto hace que más gente pueda utilizar un ordenador, ya que no necesitan instalar los dispositivos o configurarlos, el ordenador hace la mayoría del trabajo¹³.

¹² <https://dle.rae.es>

¹³ <https://www.masadelante.com/faqs/plug-and-play>

En la Figura 1.28 mostramos ejemplos de periféricos convencionales de uso habitual. Nos referimos a ellos como convencionales dado el auge de dispositivos susceptibles de conectarse a un ordenador para actividades que van más allá del uso del ordenador para ofimática, compras etc., como puede ser enviar contenido a la televisión.



Figura 1.28. Periféricos.

El uso de los periféricos que mostramos en la Figura 1.28 requieren de controladores (drivers) para su funcionamiento; ahora bien, si hace unos años era habitual que con ciertos dispositivos se entregase un CD para su instalación, en el que iban incluidos los drivers, en ciertos aparatos ya no es así; por ejemplo, el autor compró hace poco unos cascos con micro, un ratón y un teclado y no hizo falta instalar nada: son dispositivos plug and play, se conectan al ordenador y funcionan directamente; como mucho, algunas veces hay que reiniciar el equipo tras la conexión.

Pero eso no quiere decir que no necesiten sus respectivos controladores, sino que no necesitan instalar los dispositivos o configurarlos porque el ordenador hace la mayoría del trabajo.

Por otra parte, como cada vez más ordenadores, sobre todo portátiles, carecen de lector de CD, en caso de tener que descargar los drivers habría que hacerlo desde la web indicada por el fabricante del dispositivo.

La instalación es igual que las descritas en el apartado anterior para los programas, hay que seguir las instrucciones del fabricante.

Hay dos aspectos de los drivers que conviene conocer, uno los errores y otro las actualizaciones.

En la Figura 1.29 mostramos la típica pantalla que aparece en Windows cuando hay un error de algún driver; no suele ser grave, pero conviene conocerlo pues los drivers, a veces, fallan.



Figura 1.29. Pantalla de error de drivers en Windows.

Los drivers, como otros muchos programas, se actualizan, pero este proceso no siempre es conocido por el usuario. Veamos como actualizarlos.

Trabajaremos con Windows 10. En el Panel de Control vamos a *Administrador de dispositivos* (Figura 1.30) y en la parte izquierda aparece la lista de dispositivos. Picamos, por ejemplo, en *Teclados*, *Dispositivo de teclado HID* y aparece el cuadro *Propiedades: Dispositivo de teclado HID*. Picamos en *Controlador*, *Actualizar controlador* y en el cuadro de la derecha aparece *¿Cómo quieres buscar controladores?*, y picamos en *Buscar controladores automáticamente*. Podemos ver el resultado en el cuadro de la derecha de la Figura 1.31.

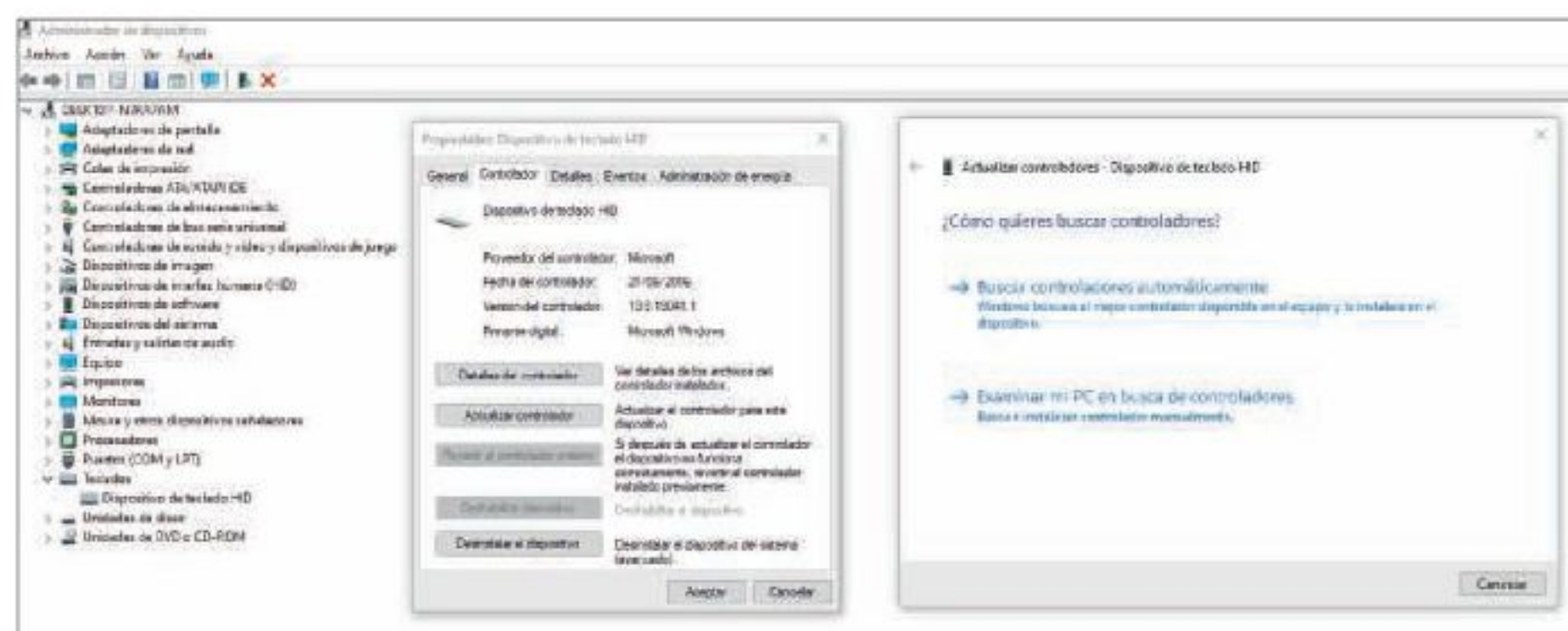


Figura 1.30. Actualizar controladores.

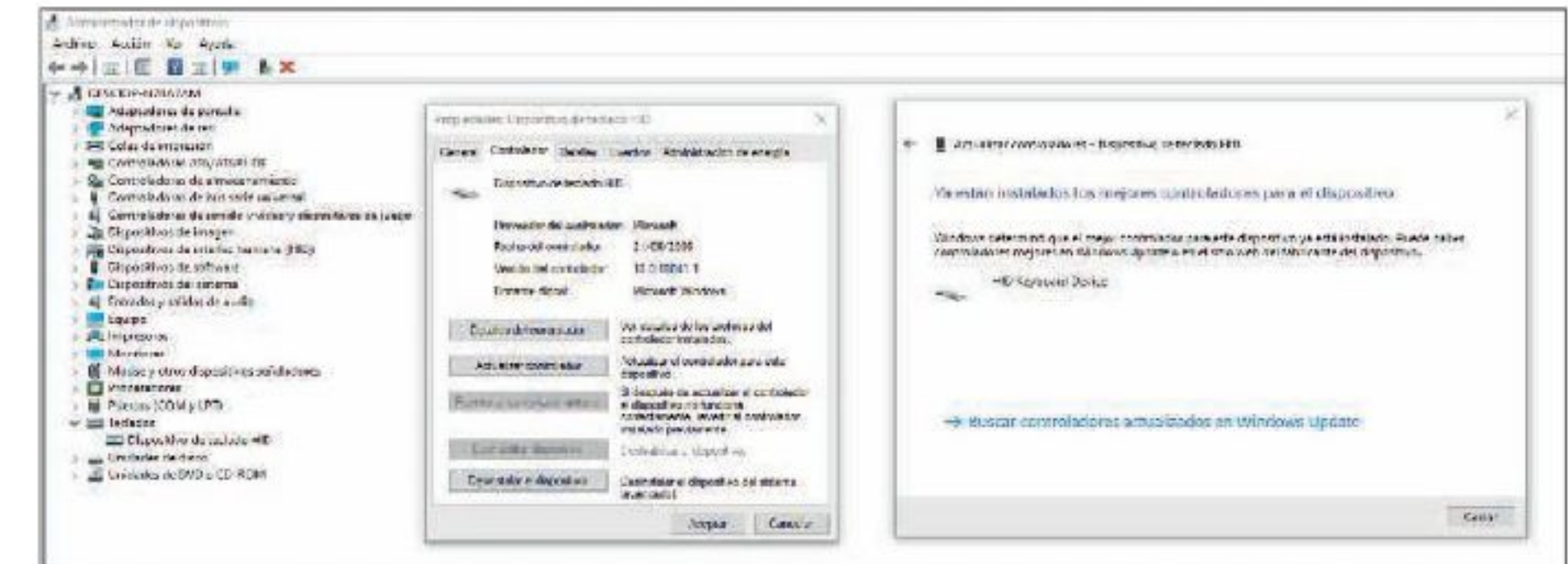


Figura 1.31. Actualizar controladores.

En este caso, el controlador ya está actualizado; si no fuera así, nos guiará para saber cómo proceder.

Según la definición de periférico, todo aquello que conectemos al ordenador o al móvil, sea mediante cables, señal telefónica, wifi o bluetooth, podría considerarse periféricos y cada vez hay más posibilidades de interconexión entre dispositivos, como veremos en el Apartado 1.5 Configuración de redes de datos.

Veamos unos ejemplos. Podemos conectar el móvil al ordenador mediante cable USB para transferir archivos o ver lo que hay en el teléfono, enviar contenidos a la televisión desde el móvil vía wifi, controlar una webcam desde el móvil o una alarma. El concepto de periférico, instalado mediante controladores, se queda corto pues estas conexiones o bien se hacen mediante aplicaciones específicas o los dispositivos son plug and play que no requieren instalación por parte del usuario. Pero esto no quiere decir que no haya que estar al tanto de las actualizaciones, pues el software con el que funcionan también se actualiza y los fabricantes ponen en el mercado nuevas versiones de los aparatos.

En resumen, cada vez más periféricos convencionales son del tipo plug and play, pero debemos estar atentos a la actualización de los drivers o controladores. Las diferentes posibilidades de conexión entre equipos y dispositivos varios se suelen hacer mediante aplicaciones específicas, pero que también pueden requerir actualizaciones; como siempre, hemos de seguir las instrucciones del fabricante.

► ACTIVIDAD PROPUESTA 1.5

Drivers en macOS

Hemos explicado los controladores, o drivers, su uso y su actualización tomando como referencia el PC con sistema operativo Windows, pero conviene saber cómo se comporta macOS a este respecto. Para ello, se propone la siguiente actividad:

- Busque información sobre los controladores en ordenadores de Apple con macOS. Tenga en cuenta que Apple tiene sus propios ratones, teclados, etc., pero que también se pueden usar periféricos diseñados para Windows.

**► ACTIVIDAD PROPUESTA 1.6****Más cosas**

Quizás no sea muy ortodoxo considerar una alarma instalada en nuestra casa, que puede ser controlada por el ordenador, la tableta y el móvil, como un periférico o las distintas posibilidades que ofrece la domótica, pero es algo habitual y conviene saber cómo funcionan. Para aumentar sus conocimientos, haga las siguientes actividades:

- Busque información sobre domótica, para ver qué es, qué puede hacer, qué equipos necesita y cómo se instala.
- Como ejemplo concreto, busque información sobre alarmas, las aplicaciones que las controla, actualizaciones, etcétera.

1.4. Instalación de certificados digitales

En este apartado vamos a tratar dos temas similares y muy relacionados: la firma electrónica y el certificado digital.

Para saber lo que son ambas cosas recurriremos a los expertos, como viene siendo habitual. En este caso, al Portal de Administración Electrónica, Ministerio de Asuntos Económicos y Transformación Digital, Secretaría General de Administración Digital¹⁴:

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- *Identificar al firmante de manera inequívoca.*
- *Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación.*
- *Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.*

La base legal de la Firma electrónica está recogida en la Ley 59/2003 de Firma Electrónica y se desarrolla en más profundidad en la sección Base legal de las Firmas. La sección también explora, bajo qué circunstancias la ley equipara la firma electrónica a la firma manuscrita, añade notas respecto a la normativa europea y hace distintas referencias legales a firmas con sellos de tiempo y avanzadas.

¹⁴ <https://firmaelectronica.gob.es>

Quizás no sepamos lo que es un sello de tiempo, *el sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces. El sellado de tiempo cualificado proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, ésta habría sido proporcionada por una de las partes, cuando lo recomendable es que la marca de tiempo sea proporcionada por una tercera parte de confianza*¹⁵.

El certificado electrónico es *un documento electrónico expedido por una Autoridad de Certificación e identifica a una persona (física o jurídica) con un par de claves.*

Tiene como misión validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.

Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.

*La Autoridad de Certificación da fe de que la firma electrónica se corresponde con un usuario concreto. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación*¹⁶.

La firma y el certificado electrónicos sirven para identificar a una persona y el sello de tiempo autentifica el contenido de un documento. La utilidad del sello de tiempo está clara y con eso nos basta, por ahora.

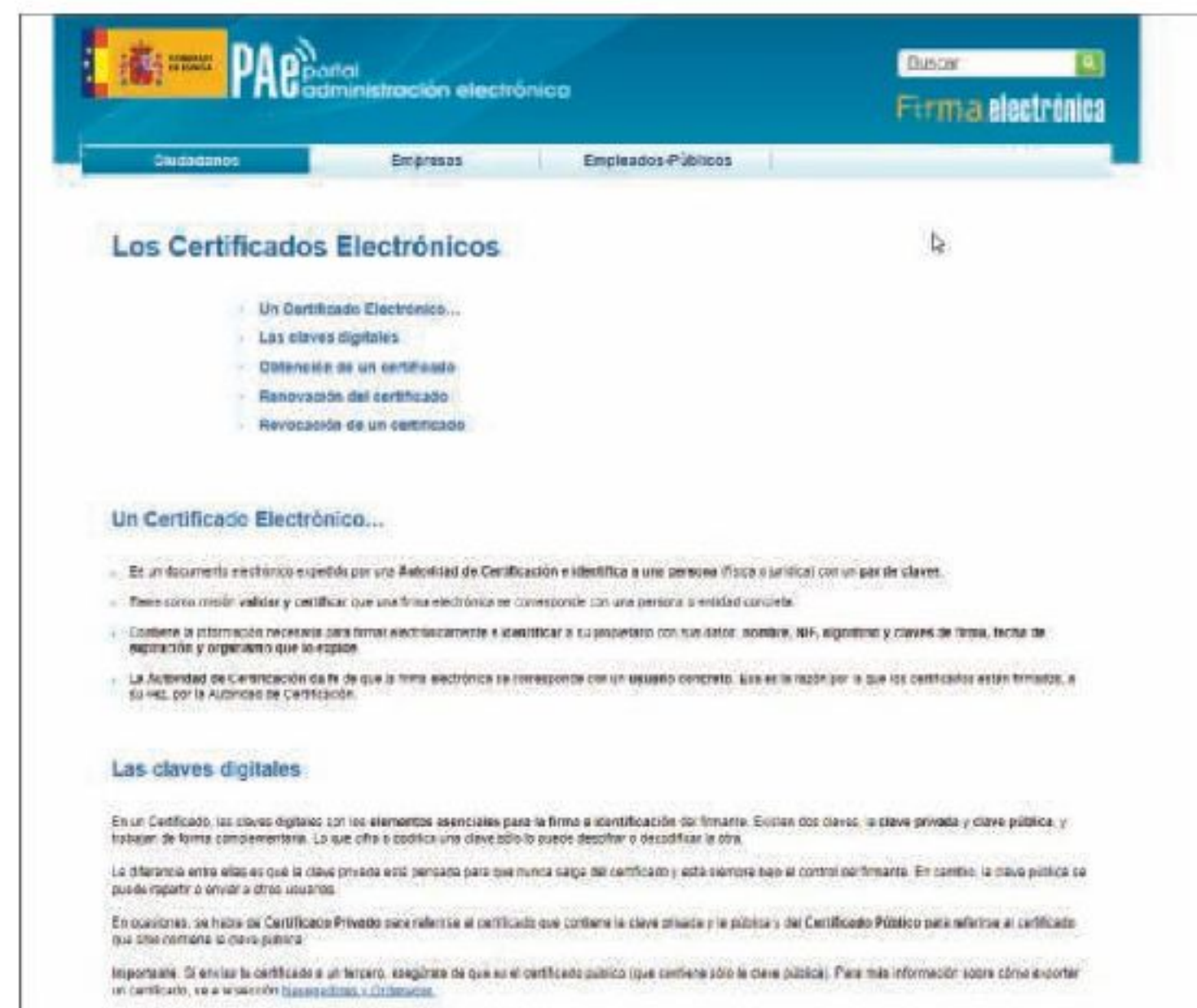
La firma electrónica identifica a las personas en cuanto personas físicas, pero no hace referencia a su pertenencia a ninguna organización, mientras que el certificado electrónico sí permite hacer eso.

Al presentar la declaración de la renta tenemos que identificarnos como declarante, por ejemplo, y podemos utilizar la firma electrónica para ello, pero si lo que necesitamos es identificarnos como miembro de una organización, debemos utilizar el certificado. El autor es profesor de universidad y para firmar las actas tiene que identificarse personalmente como miembro de esa universidad, pues el pertenecer al profesorado es lo que le capacita para la firma de actas; la identificación se hace mediante certificado (usuario y PIN).

Para instalar la firma electrónica y el correspondiente certificado hay que seguir las instrucciones que mostramos en las Figuras 1.32 y 1.33.

¹⁵ <https://www.cert.fnmt.es/catalogo-de-servicios/sellado-de-tiempo>

¹⁶ <https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>

Figura 1.32. Firma electrónica¹⁷.Figura 1.33. Certificado electrónico¹⁸.

En caso de querer obtener la firma digital, lo mejor es ir a la web indicada y seguir sus instrucciones pues se requieren distintas acciones, alguna de las cuales hay que hacerlas presencial y personalmente.

Si necesitamos instalar un certificado de una empresa privada lo mejor es seguir las instrucciones de la propia empresa. En la Figura 1.34 mostramos la web de una de estas empresas.



Figura 1.34. Certificado electrónico.

Una vez que sabemos lo que es el certificado y la firma digitales y donde se pueden obtener, es recomendable estudiar con atención los procesos. Para ello, recomendamos realizar la Actividad propuesta 1.7.

Para más información, y para saber cómo se gestionan los certificados en el navegador, se recomienda visitar los sitios web de Firmaelectronica.gob.es¹⁹ y Xataka.com²⁰.

¹⁷ <https://firmaelectronica.gob.es>¹⁸ <https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>¹⁹ https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html#instalar_certificados_windows²⁰ <https://www.xataka.com/basics/certificado-digital-que-que-tipos-hay-como-solicitarlo-activarlo>

► ACTIVIDAD PROPUESTA 1.7

Certificados y firmas

La obtención de certificados y firmas digitales requiere aportar datos personales, por lo que hemos preferido que cada alumno siga el proceso con sus propios datos. Es mejor desde el punto de vista didáctico y, sobre todo, más discreto.

- Vaya al sitio indicado en las páginas <https://firmaelectronica.gob.es>²¹ y <https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>²² y estudie el proceso necesario para obtener la firma y el certificado; si no tiene firma electrónica, consígala, es muy útil para las gestiones con la Administración.
- Vaya a los sitios indicados en las páginas https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html#instalar_certificados_windows²³ y <https://www.xataka.com/basics/certificado-digital-que-que-tipos-hay-como-solicitarlo-activarlo>²⁴. Es información útil e interesante.

1.5. Configuración de redes de datos

Veamos lo que es una red de datos:

El término *red* hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas, dos ordenadores conectados entre sí ya pueden considerarse una red.

Las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras. En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes se encuentran:

- *Personal Area Networks (PAN)* o red de área personal.
- *Local Area Networks (LAN)* o red de área local.
- *Metropolitan Area Networks (MAN)* o red de área metropolitana.
- *Wide Area Networks (WAN)* o red de área amplia.
- *Global Area Networks (GAN)* o red de área global.

²¹ <https://firmaelectronica.gob.es>

²² <https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>

²³ https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html#instalar_certificados_windows

²⁴ <https://www.xataka.com/basics/certificado-digital-que-que-tipos-hay-como-solicitarlo-activarlo>

La conexión física en la que se basan estos tipos de redes puede presentarse por medio de cables o llevarse a cabo con tecnología inalámbrica.



Figura 1.35. Tipos de conexión de red.

Personal Area Network (PAN)

Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarse ad hoc a una red. Esto puede realizarse por cable y adoptar la forma de una Personal Area Network (PAN) o red de área personal, aunque las técnicas de transmisión más habituales son la memoria USB. La variante inalámbrica Wireless Personal Area Network (WPAN) se basa en técnicas como Bluetooth, y otras. Una Personal Area Network inalámbrica que se lleva a cabo vía Bluetooth recibe el nombre de Piconet. El ámbito de acción de las redes PAN y WPAN se limita normalmente a unos pocos metros y, por lo tanto, no son aptas para establecer la conexión con dispositivos que se encuentran en habitaciones o edificios diferentes.

Local Area Network (LAN)

Si una red está formada por más de un ordenador, esta recibe el nombre de Local Area Network (LAN). Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa. Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN. Un estándar muy frecuente para redes de área local por cable es Ethernet. La transmisión de datos tiene lugar o bien de manera electrónica a través de cables de cobre o mediante fibra óptica de vidrio.

Si se conectan más de dos ordenadores en una red LAN, se necesitan otros componentes de red como hubs, bridges y switches, es decir, concentradores, puentes de red y conmutadores, los cuales funcionan como elementos de acoplamiento y nodos de distribución. El tipo de red conocido como LAN o red de área local fue desarrollado para posibilitar la rápida transmisión de cantidades de datos más grandes, las redes LAN permiten un intercambio de información cómodo entre los diversos dispositivos conectados a la red. Por ello, en el entorno empresarial es habitual que varios equipos de trabajo puedan acceder a servidores de archivos comunes, a impresoras de red o a aplicaciones por medio de la red LAN.

Si la red local tiene lugar de manera inalámbrica, se puede hablar en este caso de una Wireless Local Area Network (WLAN) o red de área local inalámbrica. Las redes locales inalámbricas ofrecen la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial²⁵.

Ya sabemos lo que es una red de datos y cuál es su función. En la Figura 1.36 mostramos un esquema de red LAN, que puede ser el de una pequeña empresa. La conexión a internet se hace mediante rúter (dispositivo que distribuye el flujo de paquetes de información entre redes de la manera más eficaz²⁶). De ahí, por cable va al conector múltiple (hub switch) y a un nuevo rúter inalámbrico por wifi (sistema de conexión inalámbrica, dentro de un área determinada, entre dispositivos electrónicos, y frecuentemente para acceso a internet²⁷), que se conecta a los ordenadores de sobremesa (cliente), a portátiles (laptop) y a tabletas; mientras que otros ordenadores, los servidores (unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red²⁸), se conectan al switch por cable, así como la impresora y algún otro ordenador.

Como podemos apreciar, hay conexiones por cable e inalámbricas. Veamos cómo podemos configurar una red doméstica.

Supongamos que tenemos un rúter que admite conexión por cable y wifi. Podemos ver un ejemplo ver en la Figura 1.36: un ordenador principal, de sobremesa, un portátil, móviles, tabletas y televisión y una impresora.

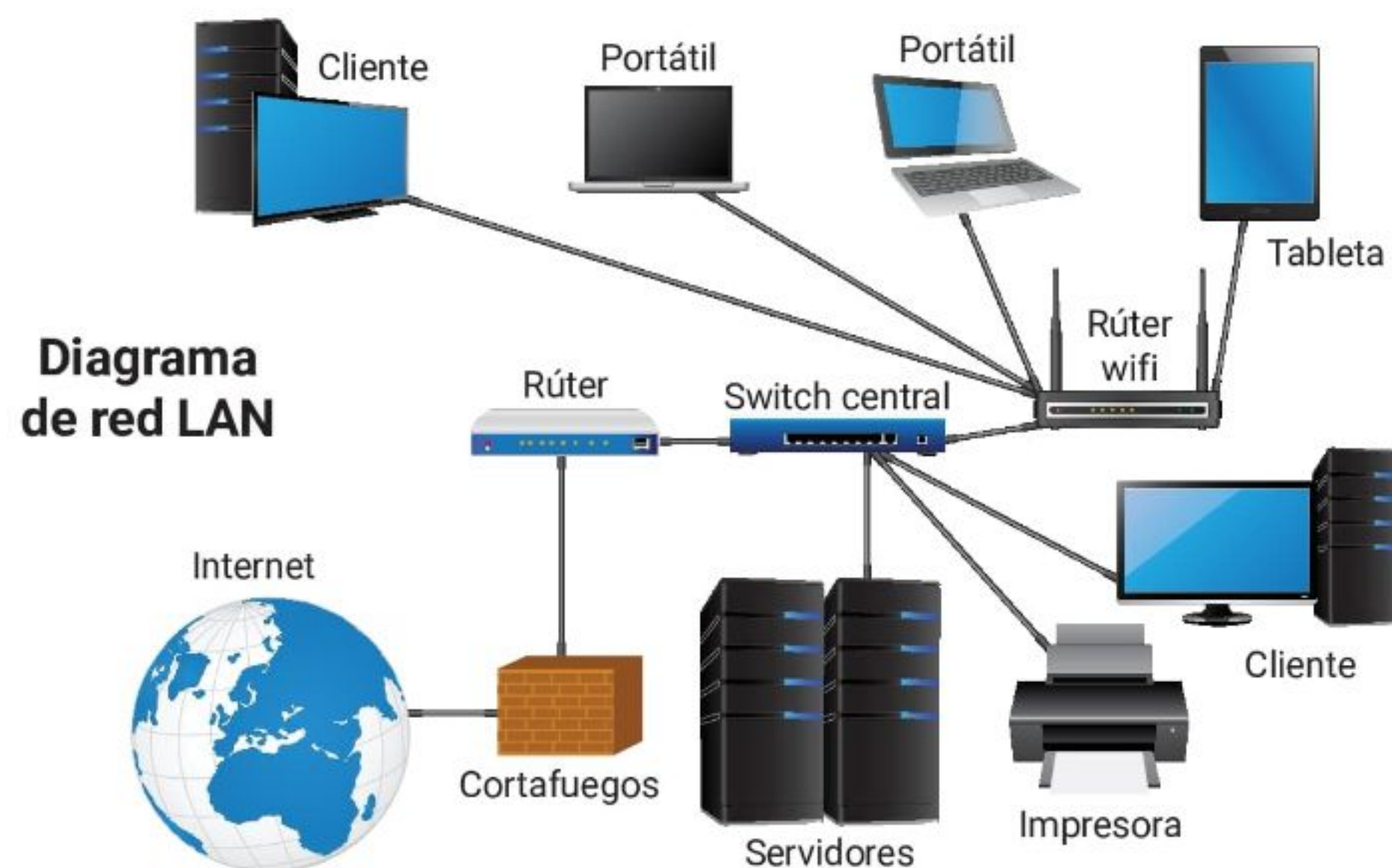


Figura 1.36. Red LAN.

²⁵ <https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos>

²⁶ <https://dle.rae.es>

²⁷ <https://dle.rae.es>

²⁸ <https://dle.rae.es>



Figura 1.37. Rúter.

El ordenador principal se puede conectar por cable o por wifi. La conexión por cable se hace con un cable de red, que tiene dos conectores como el de la Figura 1.38: uno que va al rúter y otro al ordenador, y la conexión wifi puede estar incorporada, como es habitual en los portátiles, o se puede hacer mediante un adaptador USB, como el de la Figura 1.39.



Figura 1.38. Cable de red.



Figura 1.39. Adaptador wifi.

En cualquier caso, hay que configurar el ordenador, para lo cual tenemos que ir al panel de control, redes e internet y configurar la conexión. Es similar a la instalación de cualquier programa, por lo que la proponemos como actividad para el lector.

El portátil se conecta igual que el ordenador de sobremesa, teniendo en cuenta que los portátiles actuales suelen llevar incorporada la posibilidad de conexión wifi.

La impresora también se puede conectar por cable o wifi, lo único que hay que hacer es instalarla en ambos ordenadores para poder usarla desde cada uno de ellos. Conectarla por cable a un ordenador no quiere decir que no se pueda usar desde el otro por wifi, si admite ambas posibilidades.

Los móviles y las tabletas se suelen comunicar entre sí por wifi. Recordemos que estamos hablando de una red doméstica, con lo que evitaremos gastos innecesarios de datos, y se pueden conectar a los ordenadores por wifi o por cable (USB).

En cuanto a la televisión, puede recibir la señal de internet por cable y podemos enviar contenidos desde los ordenadores o desde los móviles y tabletas vía wifi.



Pero el cable y la conexión wifi no son las únicas formas de conectar dispositivos. Otro modo de conectar, principalmente las tabletas y los móviles, es el bluetooth, que es una conexión inalámbrica de corto alcance; por ejemplo, en casa el teléfono está en red, pero lo conectamos a la bicicleta estática por bluetooth. Como vemos, hay muchas posibilidades de conexión en nuestra red doméstica.

Antes de ver la utilidad de la red que hemos montado hay que hacer algunas consideraciones relativas a la seguridad (ciberseguridad) y al alcance de las señales que es limitado, pero, salvo que vivamos aislados del mundo, la señal de nuestros dispositivos se recibirá en las casas cercanas y en la nuestra se recibirá la de los vecinos.

Como dato orientativo, el alcance de la señal wifi puede ser 15 a 45 metros en interiores y de 30 a 90 metros en exteriores, dependiendo del tipo de señal y del router, entre otros factores.

Las paredes de ladrillo y los objetos metálicos pueden reducir el alcance en un 25 %. Normalmente los hogares suelen estar divididos en habitaciones, tienen techos, suelos y suelen estar decorados con espejos y otros muebles o complementos que obstruyen la libre circulación de las ondas wifi.

Una buena forma de sortear este tipo de problemas estructurales consiste en instalar uno o varios repetidores wifi en las zonas donde la señal empieza a debilitarse. No existe una regla de oro: puede que en una casa con un solo repetidor sea suficiente, y en otra de las mismas dimensiones necesitemos 2 o incluso 3 extensores para obtener un resultado similar²⁹.



Figura 1.40. Amplificador wifi.

Como vemos, el alcance de la señal permite que llegue a los edificios o pisos adyacentes, pero está limitado por el tipo de local, su decoración y la disposición de enseres y puede necesitar de un amplificador para llegar a donde se necesite.

Por cierto, la señal wifi se lleva muy mal con los microondas, cuando funciona el microondas genera interferencias en la señal wifi.

El alcance de la señal bluetooth es de unos 10 metros, y también se ve afectado por factores varios.

²⁹ <https://elandroidefeliz.com>



La señal telefónica no suele tener problemas de alcance, salvo zonas de sombra y áreas escondidas, como garajes y similares.

Conocer y manejar adecuadamente los alcances de los tipos de señal que utilizamos nos permite optimizar el funcionamiento de nuestra red doméstica, pero, como hemos visto, también posibilita que las señales lleguen a otros usuarios, por lo que hay que ser cuidadosos; no es casualidad que las claves de acceso de algunos routers tengan 20 posiciones, con letras mayúsculas y minúsculas, y números.

Un consejo, no debemos compartir nuestras claves de acceso a la red si se van a utilizar fuera del domicilio, por ejemplo, por un vecino. Conviene que seamos prudentes, muy prudentes, con estas cosas.

Veamos unos ejemplos de utilización de la red. Uno es muy conocido, instalamos una aplicación en el móvil y podemos enviar, por wifi, los contenidos a la televisión; el móvil y la televisión están en red, conectados al mismo router.

Otra utilidad de la red, quizás no tan conocida, es poder acceder a un ordenador desde otro, lo cual permite hacer determinadas cosas desde un ordenador en otro; por ejemplo, arreglar un problema que el usuario del segundo ordenador no sabe cómo resolver. El autor utiliza esta funcionalidad con los técnicos de soporte de la universidad donde da clase, pues ahora teletrabaja desde casa. Para hacer eso hay una serie de programas y Microsoft tiene el servicio de Asistencia Rápida al que se puede acceder desde la barra de herramientas.

► ACTIVIDAD PROPUESTA 1.8

Configuración de acceso a la red

Supongamos dos posibles situaciones:

- No tiene acceso a internet. Visite las páginas de proveedores de internet, vea qué tipo de router le ofrecen, qué instalación requiere, tipo de línea, etc., y, según la información, estime si necesitaría un amplificador.
- Sí tiene acceso a internet. Revise las condiciones del acceso, clave de acceso, alcance etc., vea la configuración del router y a la conexión idónea.

► ACTIVIDAD PROPUESTA 1.9

Acceso remoto

- Estudie la funcionalidad de Microsoft Asistencia Rápida y haga un simulacro con dos ordenadores conectados a la misma red.
- Busque información sobre programas de acceso remoto y vea su utilidad.



DE COMPROBACIÓN

- 1.1. Programa, o conjunto de programas, que, una vez cargado en el ordenador, permite al usuario interactuar con él para hacer posible la ejecución de los demás programas del ordenador:**
- Buscador.
 - Explorador.
 - Navegador.
 - Sistema operativo.
- 1.2. Añadidos o modificaciones realizadas sobre los sistemas operativos instalados en los dispositivos cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad:**
- Actualización.
 - Antivirus.
 - Programa.
 - Sistema operativo.
- 1.3. Hay que evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad:**
- Depende del programa.
 - Falso, conviene hacerlo, es más barato.
 - Al ejecutar los programas.
 - Principalmente por motivos de seguridad.
- 1.4. Hay que actualizar los drivers o controladores:**
- Falso.
 - No es necesario.
 - Es solo para profesionales.
 - Verdadero.
- 1.5. Conjunto de datos electrónicos que acompañan a un documento electrónico y que permiten identificar a una persona de manera inequívoca:**
- Demasiado engorroso.
 - Firma electrónica.
 - Solo para las Administraciones públicas.
 - Solo para las empresas privadas.



- 1.6. Método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces:**
- Documento oficial.
 - Carpeta de archivos.
 - Sellado de datos.
 - No es posible hacerlo.
- 1.7. Aparato auxiliar e independiente conectado a la unidad central de una computadora u otro dispositivo electrónico:**
- Software.
 - Periférico.
 - No se deben conectar aparatos al ordenador.
 - Solo funcionan con Windows.
- 1.8. Conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, y que necesitan conexión física y lógica de los sistemas:**
- Se hace para evitar dañar los dispositivos.
 - Red de datos.
 - No se pueden conectar dispositivos distintos.
 - Solo se aplica a las conexiones por cable.
- 1.9. Documento electrónico expedido por una Autoridad de Certificación que identifica a una persona (física o jurídica) con un par de claves:**
- Documento público.
 - Documento privado.
 - Certificado electrónico.
 - Carece de utilidad.
- 1.10. Los programas incorporan archivos ejecutables para su instalación:**
- Verdadero.
 - Solo los programas muy grandes.
 - Falso.
 - Depende.
- 1.11. Plug and Play:**
- Conectar y usar.
 - Dispositivo que se identifica a sí mismo al conectarse.
 - No necesita instalación por el usuario.
 - Las tres respuestas anteriores son correctas.

**1.12. Driver:**

- a. Archivo.
- b. Conductor.
- c. Controlador.
- d. Carpeta.

1.13. Para poder descargar aplicaciones desde el ordenador al móvil deben estar vinculados y se recomienda hacerlo con ambos en red:

- a. Estando en red se evita consumo de datos móviles del móvil.
- b. Así es seguro.
- c. Verdadero.
- d. Las tres respuestas anteriores son correctas.

1.14. Un programa es más general que una aplicación, hace más cosas y suele necesitar más recursos:

- a. Solo para determinados archivos.
- b. Verdadero.
- c. Especialmente en Chrome OS.
- d. Falso.

1.15. Si su ordenador ha estado tiempo apagado, lo primero es comprobar si el SO está actualizado; conviene tenerlo en cuenta antes de empezar a trabajar con él:

- a. No hace falta.
- b. Solo en los ordenadores con Windows.
- c. Verdadero.
- d. Es una pérdida de tiempo.

1.19. ¿Qué contraseñas o sistemas de identificación utiliza en sus dispositivos? Busque información sobre sistemas de identificación que impliquen el uso del móvil.**1.20. Buscar información sobre periféricos plug and play, marcas, precios, etc. ¿Qué conclusiones obtiene, con lo aprendido hasta ahora?****1.21. Revise la situación de sus periféricos respecto a los drivers, según se indica en el Apartado 1.3.****1.22. ¿Tiene Gmail? Active la doble verificación para entrar en la cuenta. Para ello hay que utilizar el móvil; es otra de las utilidades de la red doméstica.****1.23. Haga un esquema de su red doméstica, analice las distintas conexiones. Si ha tenido incidencias, estúdielas para ver si encuentra la solución; si no tiene ninguna red, piense cómo le gustaría configurarla.****1.24. Busque información sobre el uso de software pirata, aspectos económicos, legales y de seguridad. Haga un resumen, le servirá para hablar con ciertos desaprensivos.****1.25. ¿Cuándo hay que utilizar bluetooth y cuando wifi? Ponga ejemplos de su vida cotidiana.****1.26. Practique enviando contenidos del móvil a la televisión, de la tableta a la televisión y del ordenador a la televisión.****1.27. Vaya a la página de Camerfirma (Figura 1.31) y vea los servicios de certificación y similares que ofrece. ¿Los considera útiles?****1.28. Vea las opciones de firma y autenticación de documentos en Word y Acrobat. Si no los tiene, descargue las versiones de prueba; le servirá como práctica de descarga de programas.****1.29. Busque información sobre sitios en los que se pueden descargar drivers. ¿Le parecen fiables? Puede buscar consejo en sitios como Xataka, por ejemplo.****1.30. Busque información sobre la evolución del paquete Microsoft Office. Vaya cinco años hacia atrás y analice los principales cambios. No se preocupe si hay cosas que no entiende, las distintas versiones no tienen solo aspectos técnicos. Vea la relación con las versiones de Windows.****DE APLICACIÓN****1.16. Compare las características más importantes de Windows 10 y 11. ¿Qué objetivo tiene, en su opinión, la actualización?****1.17. Busque información sobre la evolución de Android y la influencia que tienen las nuevas utilidades, como las relativas al coche conectado, las mejoras de seguridad, la doble verificación del correo, etcétera.****1.18. Elija dos o tres programas que le gustaría tener, busque el que tenga versión de prueba e instálela; revise el proceso según se indica en la Unidad.**



Tratamiento de la información

Conforme vamos teniendo un mayor conocimiento de la red y del tratamiento de la información nos pueden surgir preguntas sobre la forma de mejorar nuestras búsquedas, sobre cómo trabajar y gestionar la información obtenida, los contenidos digitales y si es conveniente trabajar en la nube y cómo hacerlo de forma sencilla (y barata).

Eso es lo que vamos a aprender en esta unidad: a buscar mejor, a gestionar contenidos de forma legal y veraz y a trabajar en la nube.

Contenido

- 2.1. Técnicas avanzadas de búsqueda
- 2.2. Curación de contenidos
- 2.3. Almacenamiento de contenido en la nube (Dropbox, Google Drive, OneDrive de Microsoft)

2.1. Técnicas avanzadas de búsqueda

Antes de comentar las técnicas avanzadas de búsqueda, conviene que nos preguntemos si realmente sabemos buscar información en la red y, de paso, recordar unas definiciones.

RECUERDA

- Los navegadores son programas instalados en los distintos dispositivos para acceder a los sitios web que existen en la red. Google Chrome y Microsoft Edge son navegadores.
- Un buscador es un sitio web al que llegamos con el navegador, que permite encontrar información diversa. Google y Bing son buscadores.

¿Qué hacemos los no expertos para buscar información?

Lo habitual es abrir el navegador y escribir en el buscador lo que queremos buscar. A veces el resultado es el esperado y hemos terminado el proceso, pero no siempre es así, lo que implica volver a buscar con otras palabras. Este tipo de búsqueda, que podemos definir como búsqueda mediante palabras clave, no es nada eficiente, pues en determinadas ocasiones no encontramos lo que buscamos y tenemos que ir saltando de un sitio a otro, con la consiguiente pérdida de tiempo, y no siempre con éxito.

Podemos mejorar el método utilizando distintos navegadores y buscadores; por ejemplo, si no lo encontramos en Bing, podemos ir a Google o a otro buscador.

¿Cuánto tiempo pasamos buscando información en la red, sea por trabajo o a título particular?

Todo parece indicar que merece la pena aprender a buscar mejor, pues evitaremos pérdidas de tiempo, además de tener más éxito en las búsquedas.

Precisamente de eso va a tratar este apartado: vamos a aprender a buscar y vamos a mejorar la técnica de búsqueda de información en internet.

¿Qué se entiende por técnicas avanzadas de búsqueda?

El servicio de bibliotecas de la Universidad de Extremadura ofrece la siguiente definición: *la búsqueda avanzada nos permite combinar términos y operadores que nos devolverán resultados más próximos a nuestros intereses. Por otra parte, permite también seleccionar el tipo de formato, la colección, ubicación, idioma y acotar las fechas de nuestra búsqueda. Se trata de una búsqueda más refinada en donde nosotros tenemos que ir marcando previamente los límites de nuestra búsqueda¹.*

¹ <https://biblioguias.unex.es/c.php?g=572092&p=3944859>

Otras fuentes indican que la búsqueda avanzada implica hablar al buscador en su propio lenguaje. Este lenguaje tiene una estructura lógica, por lo que si aprendemos a utilizar los recursos adecuados, la búsqueda será mucho mejor en términos de exactitud del resultado y del tiempo invertido.

Para familiarizarnos con el tema, vamos a aprender a hacer búsquedas avanzadas en Google. En la captura de pantalla que mostramos en la Figura 2.1, hemos escrito «búsqueda avanzada» (se ha escrito, por error, sin tilde en la primera u pero Google ha identificado la palabra correcta). Aparecen una serie de resultados, pero queremos hacer una búsqueda avanzada, picamos donde indica la flecha y aparece la pantalla de la Figura 2.2.

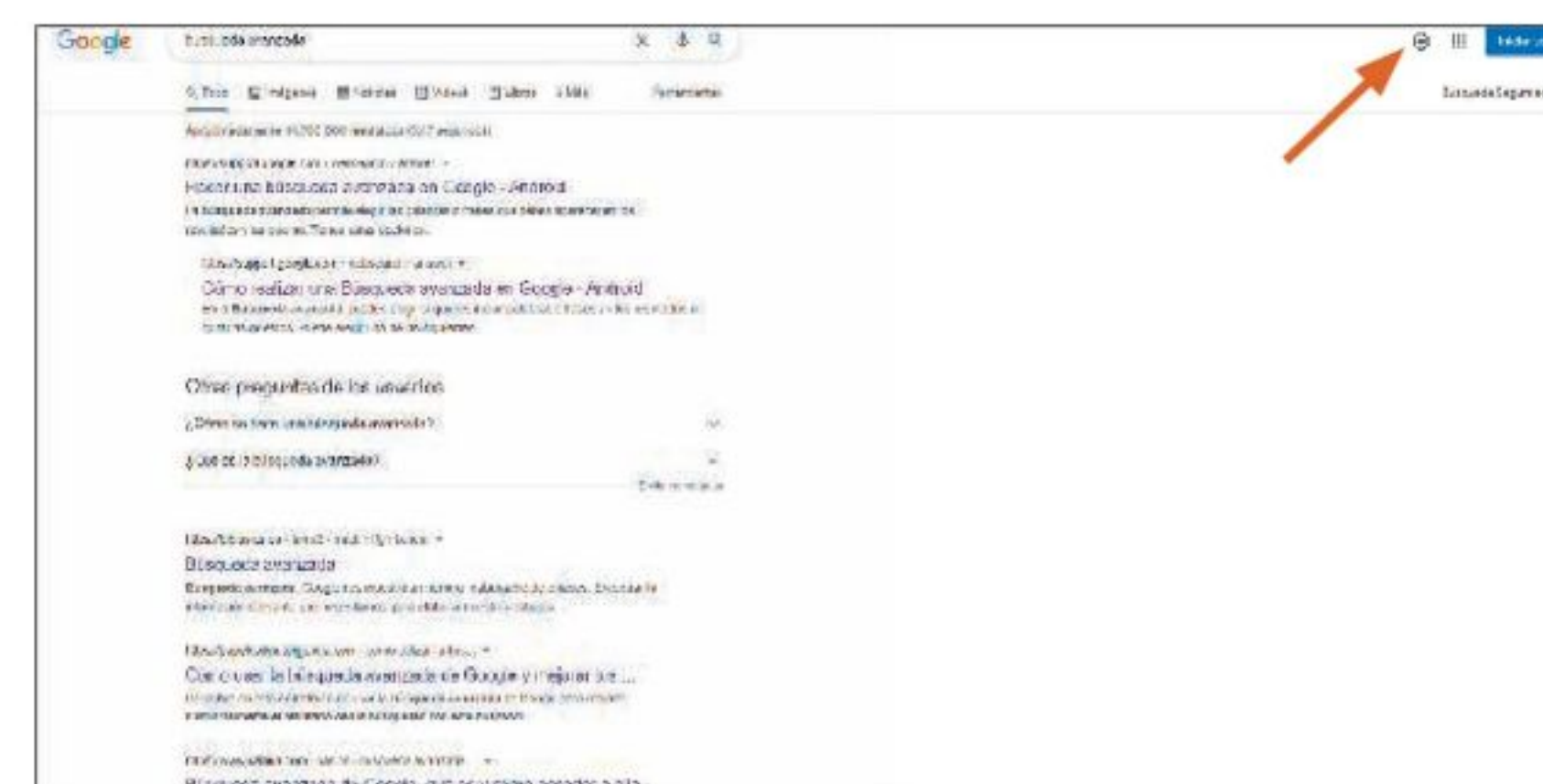


Figura 2.1. Búsqueda avanzada en Google.

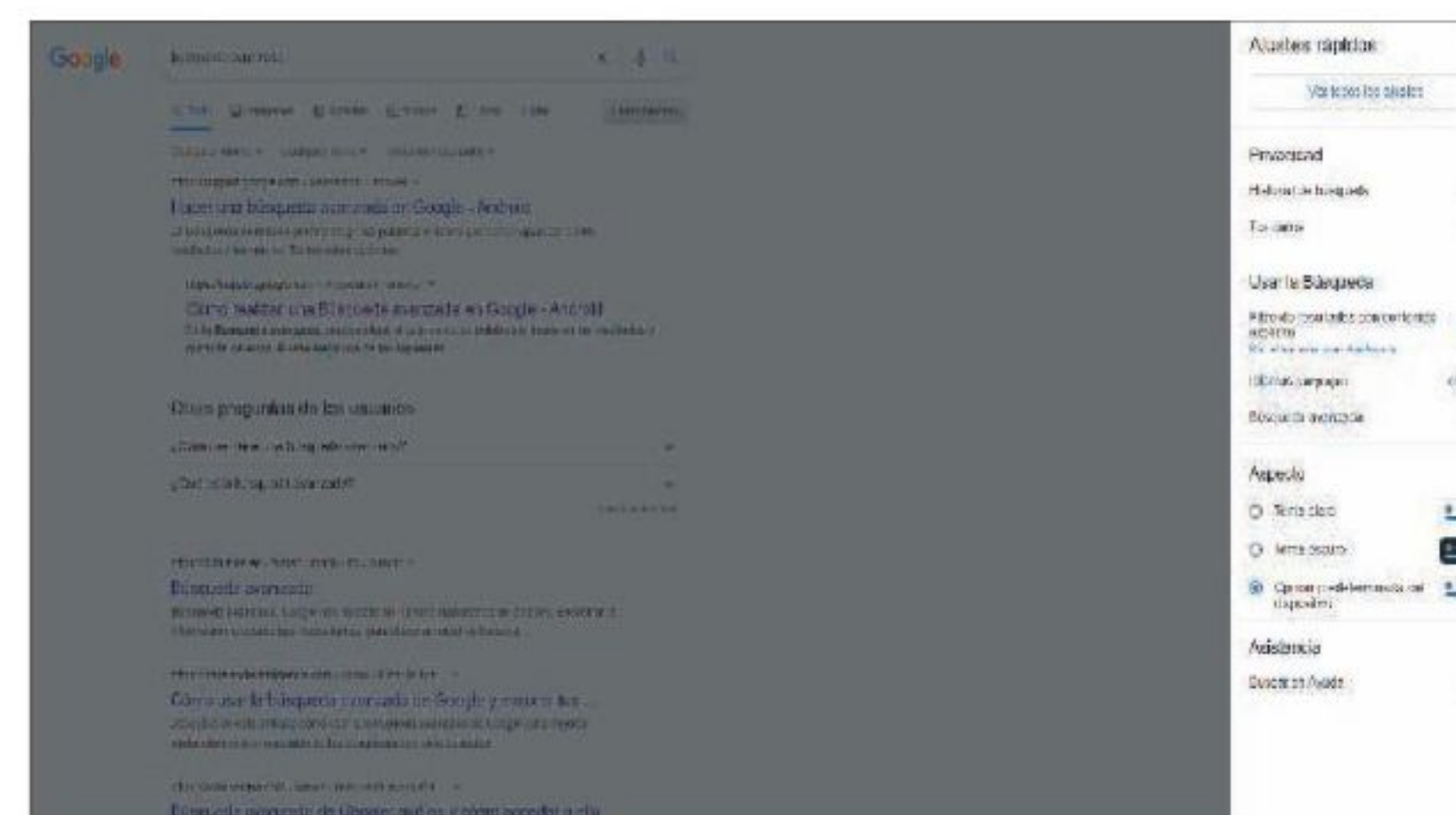


Figura 2.2. Búsqueda avanzada en Google.

Picamos en *Búsqueda avanzada* y aparecen los cuadros de diálogo de la Figura 2.3, que permiten afinar la búsqueda definiendo los criterios con más exactitud.



Figura 2.3. Búsqueda avanzada en Google.

Como hemos visto, Google permite hacer búsquedas avanzadas de forma sencilla, y como la forma de aprender es practicar, proponemos una actividad de búsqueda.

De la misma forma que se pueden hacer búsquedas avanzadas en Google en el ordenador, se pueden hacer en dispositivos con Android².

En Google también se pueden afinar las búsquedas sin recurrir a la funcionalidad *Búsqueda avanzada*. Veamos unos ejemplos:

Google guarda en su interior un potente algoritmo que pretende optimizar la experiencia de usuario de cualquier ciudadano que se conecte a su buscador. Para ello, trata de sacar el mayor partido a nuestros intereses. Es decir, intenta conocernos bien, saber qué solemos buscar y por qué temáticas nos sentimos atraídos. Por eso pretende personalizar al máximo cada búsqueda que se haga.

Pero como estudiantes o profesionales de alguna temática en particular, requerimos de búsquedas avanzadas que no siempre tienen por qué coincidir con nuestros intereses. Por eso es importante conocer estas técnicas de localización de información que nos permitan encontrar aquello que requerimos sabiendo que los datos aportados son reales y contrastados.

Búsqueda con entrecomillados, es un método sencillo y cómodo. Si quieres evitar errores, a pesar de que Google aplique corrección ortográfica y búsqueda de sinónimos, también permite que localices una palabra o frase exacta si la escribes entrecomillada en la caja de búsqueda. Es tan simple como, por ejemplo, escribir: «universidad pública en Perú». Los resultados incluirán la frase exacta.

Inclusión de signos + y -, a veces, Google localiza demasiados términos por comparativa. Por ejemplo, en marcas de smartphone. Por eso puedes añadir el término + para reforzar y el - para excluir. Imaginemos que buscas las características de un celular Huawei. Podrías buscar: Huawei +características.

Uso del comodín, es el famoso asterisco, que Google usa como comodín. Si lo pones al final de la búsqueda, te ayudará a refrescar la memoria si no recuerdas el nombre exacto. Por ejemplo: universidad *.

Búsqueda masiva y genérica, puedes utilizar dos términos y añadir entre ellos 'OR' o '|', así el motor del buscador te ofrecerá una ingente cantidad de información. Por ejemplo: universidad OR instituto.

Rangos numéricos, si buscas una información concreta entre dos cifras, por ejemplo, precios, años, etc., puedes usar los puntos suspensivos. Veamos un ejemplo: población Perú año 1950... 2000. El motor irá directo al contenido que te interesa entre los años especificados.

Buscar en un site concreto, si quieres localizar una información específica en un sitio web concreto, para coger ideas o saber qué han escrito sobre algún tema, puedes realizar búsquedas como: site: universia.net/pe liderazgo.

Búsqueda de documentos, otra opción interesante para buscar información en Google es ir directamente a algún tipo de documento. Por lo general, los estudios e investigaciones suelen estar publicados como PDF. Además, se pueden añadir PowerPoint, Excel, etc. Así pues, el tipo de archivo se podrá incluir para que solo veamos presentaciones, etc. Por ejemplo: filetype: pdf investigación cáncer.

Búsqueda de contenidos similares, si quieres buscar contenidos similares a los que hay en una web, pero no los de esa web en particular, también puedes localizar sites interesantes con esta posibilidad. Veamos un ejemplo si necesitas investigar sobre cine: related: www.imdb.com.

Búsqueda con una dirección o título concreto, en este caso se añade el término 'in' para incluir una palabra que irá en el título o la dirección web. Veamos un par de ejemplos: Marie Curie intitle: radioactividad. O bien: inurl: smartphone.

Búsqueda de imágenes libres de derechos, por último, veamos una opción interesante para buscar imágenes que puedas utilizar sin pagar por ellas. Para cumplimentar esta opción, busca un término, por ejemplo, Albert Einstein. Luego, clicas en la opción Imágenes y después, en el desplegable al pinchar en Herramientas, usa Derechos de uso —Licencias Creative Commons. Con una mención del autor podrás utilizar la fotografía para tu proyecto o web.

Como ves, buscar información de calidad en Google es relativamente sencillo si sabes cómo. Aprovecha estas técnicas para mejorar tus trabajos y estudios, tu profesión o incluso tu web³.

³ <https://www.universia.net/pe/actualidad/orientacion-academica/10-tecnicas-para-buscar-informacion-en-google.html>

² <https://support.google.com/websearch/answer/35890?hl=es-VE&co=GENIE.Platform%3DAndroid>

Ya sabemos lo que es una búsqueda avanzada y cómo hacerla utilizando ciertas herramientas, pero hay más posibilidades que veremos en el siguiente apartado.

2.1.1. Operadores de búsqueda en buscadores

En este apartado vamos a recurrir a un sitio que tiene mucha, y buena, información sobre tecnología en general y sobre tecnologías de la información en particular, Xataka.

Los operadores de búsqueda son una serie de símbolos y comandos que sirven para acotar los resultados de las búsquedas que realizas. Algunos de ellos incluyen símbolos como el de puntuación, que Google siempre ignora en el caso de que no pertenezcan a un operador concreto.

Te traemos una lista con 39 operadores de búsqueda de Google con los que puedes acotar lo que quieres encontrar de acuerdo con determinados parámetros. Si quieres que cuando busques un producto se muestren resultados con un determinado precio, o que los resultados incluyan varias palabras con o sin ninguna otra en medio, los operadores te pueden ayudar a ello.

Son como filtros añadidos, solo que en vez de estar en las opciones que ves debajo de la barra de búsqueda de Google cuando te muestra los resultados tienes que incluirlos en la propia búsqueda acompañando al término que quieras encontrar. Hay incluso algunos que sirven como enlace para poder utilizar más de uno a la vez.

La forma en la que funcionan es muy sencilla. Lo único que tienes que hacer es escribir un texto en la barra de búsqueda de Google en el que se incluya el operador que quieres utilizar. Habrá veces en las que este operador estará entre comandos de búsqueda o al final de cada uno, dependiendo de lo que quieras hacer con él⁴.

La lista de operadores figura en la Tabla 2.1. En ella se incluye el operador, un ejemplo y su función.

Tabla 2.1. Operadores

Operador	Ejemplo	Qué hace
OR	Pelota OR palo OR paso	Muestra resultados que contengan cualquiera de las palabras que hayamos incluido.
AND	Xataka and Basics	Busca páginas que incluyan los dos términos especificados.
" "	"Xataka Basics" o "Liga de fútbol femenino"	Muestra resultados donde aparece el término o los términos exactos que hayamos añadido entre los " .

⁴ <https://www.xataka.com/basics/operadores-busqueda-para-google>

Operador	Ejemplo	Qué hace
-	Xataka -Basics	Muestra resultados donde se excluya la palabra que hayamos puesto detrás del - .
*	"Liga de * femenino"	Un comodín que puede coincidir con cualquier palabra en la búsqueda.
#..#	Móvil 200..500 euros	Muestra resultados donde se añade el intervalo de números que especifiquemos.
()	("redes sociales" OR "plataformas sociales") -Twitter	Permite combinar operadores. En el ejemplo buscaremos redes sociales o plataformas sociales, pero excluyendo Twitter de los resultados.
AROUND	Trucos around(3) Instagram	Resultados donde aparecen las dos palabras especificadas, pero con el número de términos entre ellas que determinemos.
EN	300 dólares en euros	Sirve para convertir unidades de un mismo tipo de medida.
MAP	map:Castellon	La búsqueda nos devuelve resultados con mapas del sitio donde le digamos.
DEFINE	define:trampear	Busca la definición de una palabra que no conozcamos.
SITE	Smartphone site:www.xataka.com	Busca los resultados dentro de una web que hayamos especificado.
INFO	info:www.xataka.com	Muestra resultados donde se ofrezca información sobre una página web.
RELATED	related:www.xataka.com	Muestra en los resultados otras páginas similares a la que hemos escrito.
LINK	Teléfonos link:www.xataka.com	Muestra en los resultados páginas que tienen enlaces a la web que hayamos especificado.
CACHÉ	cache:www.xataka.com	Muestra la copia de la página que hay en el caché de Google.
FILETYPE	filetype:pdf presupuestos 2019	Busca resultados que contengan archivos con el formato que hayamos especificado.
ALLINTEXT O INTEXT	allintext:"móviles baratos"	Encuentra páginas que incluyan en su texto algunos o todos los términos que hayamos incluido en el comando.
ALLINTITLE O INTITLE	allintitle:precio y disponibilidad	Muestra páginas que tengan algunos o todos los términos que hayamos incluido en el comando en su título.



Operador	Ejemplo	Qué hace
INURL O ALLINURL	inurl:"apple iphone" allinurl:"apple sfera"	Muestra páginas con algunos o todos los términos que hayamos incluido en el comando.
ALLINANCHOR O INANCHOR	allinanchor:"móviles baratos"	Resultados con páginas donde se incluya un enlace con un texto anclado donde se incluya uno o varios términos especificados.
STOCKS	stocks:Facebook	Busca el estado actual de la empresa que busquemos en bolsa.
WEATHER	weather:Valencia,es	El tiempo en la ciudad elegida. Después del nombre de la ciudad podemos poner una coma y el país para concretar más.
TIME	time:Nueva York	Muestra la hora en una localidad concreta.
MOVIE	movie:Reservoir Dogs	Muestra resultados relacionados con una película.
@	@Xataka	Busca etiquetas sociales asociadas con Twitter.
#	#Xataka	Busca términos publicados con hashtags en redes sociales que tengan sistema de hashtags.
\$	iPhone 500\$	Muestra resultados donde se incluyan precios de productos en dólares en el rango que hayamos especificado.
€	iPhone 500€	Muestra resultados donde se incluyan precios de productos en euros en el rango que hayamos especificado.
+, -, X O /	3x4	Abre la calculadora y calcula sumas, restas, multiplicaciones o divisiones.
** O ^	3^4	Abre la calculadora y calcula matemáticamente la operación del primer número elevado al segundo.
% DE	21% de 900	Abre la calculadora y calcula el porcentaje establecido en la cifra que añadamos.
LG	lg(28)	Abre la calculadora y calcula logaritmos en base 2.



Operador	Ejemplo	Qué hace
LOG	log(200)	Abre la calculadora y calcula logaritmos en base 10.
LN	ln(24)	Abre la calculadora y calcula el logaritmo neperiano.
!	3!	Abre la calculadora y calcula operaciones factoriales.
SQRT	sqrt(16)	Abre la calculadora y calcula la raíz cuadrada.
NTH ROOT OF	3th root of 27	Abre la calculadora para calcular la raíz a la n-ésima del número elegido.
SIN(N) COS(N) TAN(N) SEC (N) COT(N) CSC(N)	cos(0)	Abre la calculadora y calcula operaciones de trigonometría.

Los operadores de búsqueda no solo se pueden utilizar en Google, por lo que proponemos una actividad para aprender a utilizarlos en los demás buscadores. Recordemos que para aprender hay que practicar; no debemos preocuparnos si las cosas no salen bien a la primera, sino insistir.

Hasta ahora hemos restringido la búsqueda a los buscadores, que es la forma habitual de actuar, pero hay otras fuentes de información, dentro y fuera de Google, que comentaremos en el siguiente apartado.

2.1.2. Otras fuentes de información

Para situarnos, vamos a comentar dos herramientas de Google que permiten obtener información en ámbitos concretos, información que sería muy difícil encontrar en un buscador convencional.

Nos referimos a Google Ngrams y Google Académico.

Google Ngrams (<https://books.google.com/ngrams>) indica de qué tratan los libros que Google tiene almacenados y que van del año 1800 hasta nuestros días. El nombre oficial es «Google Books Ngram Viewer».

Lo podemos utilizar para saber cuándo aparece un término en la literatura. Si queremos saber cuándo aparece el término feminismo, hacemos una búsqueda en Ngrams y nos muestra lo que vemos en la Figura 2.4 (tengamos en cuenta que la búsqueda se ha hecho como un mero ejemplo).

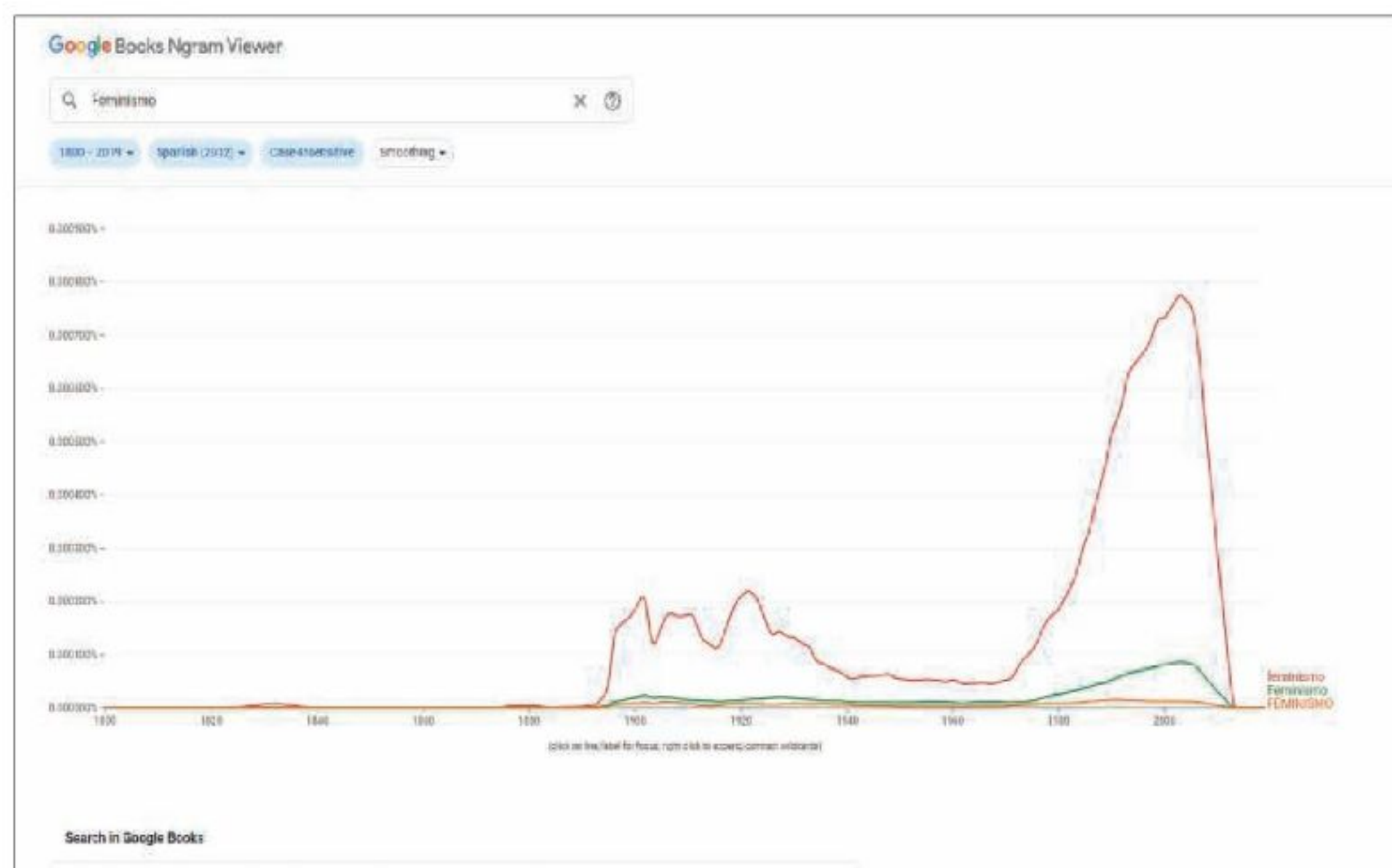


Figura 2.4. Búsqueda en Google Ngrams.

Otra herramienta es Google Académico (Google Scholar en inglés). Si en Google buscamos Google Académico aparece la pantalla que vemos en la Figura 2.5, y si buscamos «feminismo» aparece lo que se muestra en la Figura 2.6. Este buscador busca en bases de datos académicas artículos y trabajos publicados sobre el tema de interés, y en otras bases de datos como por ejemplo Research Gate.



Figura 2.5. Búsqueda en Google Académico.

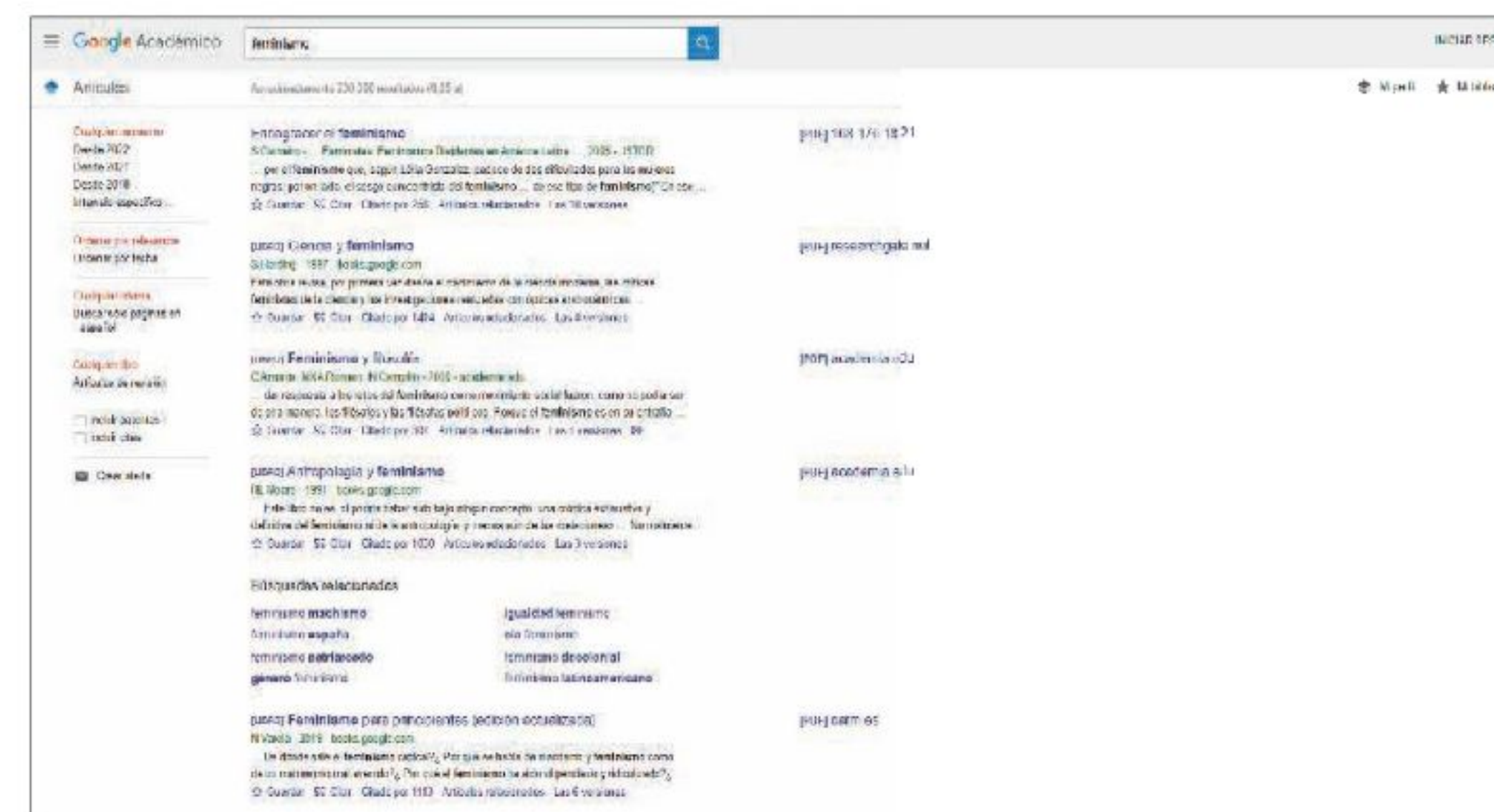


Figura 2.6. Búsqueda en Google Académico.

Los ejemplos anteriores nos indican que hay otras maneras de buscar, además de los buscadores convencionales, es decir, se puede buscar información en otros sitios de la red. Vamos a hacer un somero recorrido por ellos, para lo cual antes veremos lo que nos dice la fuente consultada, que, sin quitarle el mérito a Google, propone otras alternativas para buscar.

Cómo identificar fuentes de información relevantes sobre cualquier temática sin utilizar Google.

Todos tenemos tan interiorizado Google como recurso para identificar fuentes de información relevantes que apenas nos damos cuenta o nos molestamos en investigar otras opciones. Sin embargo y a pesar del buen servicio que nos presta el buscador, existe una manera más rápida y segura de identificar información relevante sobre un tema.

No me malinterpretes, Google sigue y seguirá siendo una estupenda herramienta de búsqueda y localización de información.

De hecho, la compañía de Mountain View está en el negocio de darte la información que buscas cada vez con mayor precisión. De ahí los constantes esfuerzos en la mejora de los resultados ofrecidos por su buscador.

La misma fuente cita otras formas de buscar información (el texto se ha retocado para adaptarlo mejor al contexto del apartado):

- *Identificando fuentes de información relevantes a través de personas.*
- *Aprovechando las redes sociales para identificar fuentes de información relevantes.*
- *Medios no convencionales para identificar fuentes de información relevantes:*



- **Identificando fuentes de información relevantes a través de personas**, utilizando el conocimiento o la ayuda de personas en la red. Mi equipo y yo utilizamos hasta tres maneras que funcionan relativamente bien. No siempre ¡Ojo!
- **Foros**: es la forma nativa de relación en internet por excelencia y para algunos sectores y páginas siguen funcionando bastante bien.
- **Quora**: si tuviera que definir Quora diría que es la red social de las preguntas. Por así decirlo creas tu perfil de usuario, sigues a otras personas y sueltas tus preguntas, esencialmente te permite aprovecharte de las preguntas de otros usuarios. Puedes ver las respuestas, las personas que han visto las respuestas, preguntas relacionadas y los seguidores de la pregunta. Si estás interesado también puedes seguir la pregunta, claro.

Como ves estas alternativas te permiten contar con el conocimiento de otras personas en la red preguntando directamente o aprovechándote de las respuestas de terceros para encontrar nuevos recursos de información.

Aprovechando las redes sociales para identificar fuentes de información relevantes.

En la era del internet no nos podíamos olvidar de nuestras amadas y odiadas redes sociales. Aquellas donde personalmente estamos obteniendo mejores resultados son:

- **LinkedIn**: es una herramienta estupenda para localizar fuentes de información de tu interés. Sobre todo, si participas en los grupos de LinkedIn. Al suscribirte a estos obtienes información que postean sus usuarios sobre una temática determinada que puede llevarte a dar con buenas fuentes de información para tu actividad.
- **Twitter**: es probablemente una de las redes sociales más concurridas y febriles que existe. A pesar de que es imposible seguir su actividad con detenimiento, siempre ofrece la posibilidad de recuperar auténticos recursos de información.
- **Slide Share**: es la red social de las presentaciones. Su punto fuerte es que no está tan contaminada de información irrelevante y te permite no solo encontrar buenas piezas de información sino también autores y fuentes de información relevantes para ti.
- **Facebook, YouTube, Reddit, etc.** también pueden usarse para obtener fuentes de información relevantes para tu sector. Una advertencia: En las redes sociales tendrás que hacer frente a los problemas de la falsa información porque el volumen de informaciones que se mueve es brutal y es complicado limpiar y extraer lo bueno de lo inútil.

Medios no convencionales para identificar fuentes de información relevantes:

Veamos por último otras alternativas menos convencionales para localizar fuentes de información de gran interés para nosotros. Por lo general puedes emplear estas cuatro:



- **Talkwalker**: en realidad este es un servicio de alertas sobre nuevos resultados de búsqueda de una palabra clave en Google. Así que no deberíamos incluirlo, pero... Permite crear un canal RSS de la búsqueda de información que queramos y los nuevos resultados irán apareciendo en nuestro lector o servicio de feeds.
- **Boletines de novedades**: es una buena forma de obtener nuevas fuentes de información sin esfuerzo directamente en tu buzón de correo electrónico.
- **Páginas web de asociaciones**: muchas asociaciones disponen un apartado en su web con recursos o enlaces de interés. Son por lo general fuentes de información relevantes gracias a que alguien ya se ha tomado la molestia de curarlas por nosotros.
- **Estudios de servicios gratuitos**: muchos estudios realizados por instituciones tienen un apartado claro de fuentes de información que pueden resultar de gran interés⁵.

Antes de extraer conclusiones hay que introducir un concepto que ya conocemos, pero al que hemos llamado de otra manera: al documentarnos sobre buscadores y fuentes de datos en internet nos encontramos con los motores de búsqueda; pues bien, un motor de búsqueda es un buscador.

En textos anteriores ya se introdujo el concepto de metabuscador⁶, que es un buscador de buscadores, no tiene bases de datos propias, pero consigue y muestra la información de otros buscadores⁷. La ventaja es precisamente esa, que mediante una búsqueda se accede a la información de muchas bases de datos que si hubiera que consultar de una en una llevaría mucho más tiempo. Por ejemplo, si buscamos un hotel en Booking o en Tripadvisor estamos utilizando metabuscadores (es posible ampliar la información en la referencia citada).

2.1.3. Conclusiones

Hemos empezado hablando de los buscadores que podríamos denominar convencionales: Google, Bing, etc., y hemos introducido el concepto de búsqueda avanzada, tanto las propias de los buscadores como las efectuadas mediante operadores de búsqueda, para afinar estas.

Pero estos buscadores no son la única manera de obtener información en internet. Hemos dado una serie de ejemplos de fuentes alternativas a los buscadores más habituales: algunas son herramientas proporcionadas por el propio buscador, como Google, y otras son fuentes de lo más variado que permiten obtener información de muchos tipos.

⁵ <https://papelesdeinteligencia.com/como-identificar-fuentes-de-informacion-relevantes-sin-google>

⁶ Mas Alique, P. (2022): *Competencias digitales básicas*. Madrid: Ediciones Paraninfo

⁷ <https://www.arimetrics.com/glosario-digital/metabuscar>

También hemos abordado los metabusadores, de uso habitual, pero que no siempre sabemos lo que es.

Estamos ante una caja de herramientas; el problema es que, cuando la abrimos y vemos su contenido, puede que no sepamos cómo usar lo que vemos. Por otra parte, no es raro que, ante la gran cantidad de información que hay en la red, no se tenga claro cómo proceder.



Figura 2.7. Caja de herramientas.

El uso de buscadores, como Google o Bing, es muy recomendable, pero en su generalidad está, muchas veces, su principal inconveniente: cuando hay que recurrir a fuentes más especializadas, que no siempre sabemos cuáles son.

Una buena forma de resolver esta situación es preguntar. Hemos visto sitios de preguntas como Quora, y también podemos utilizar las redes sociales (evidentemente podemos preguntar a un amigo tomando un café, pero estamos hablando de conseguir información en la red) y una vez obtenida la respuesta podremos hacer una búsqueda mejor.

Vemos un ejemplo: Isabel va a empezar sus estudios universitarios, quiere hacer una ingeniería, pero no tiene claro cuál ni dónde.

Decide buscar información en la red, va a Google y busca «grados en ingeniería» y el primer resultado es *educaweb*, según se muestra en la Figura 2.8.

No parece mal resultado, hemos dado con un metabuscador que permite búsquedas avanzadas, según se indica en el cuadro de diálogo que aparece a la derecha.

Pero no es una página oficial y son los previstos para el curso 22/23. Si picamos en uno de ellos nos manda a la universidad correspondiente a pedir información, pero lo primero que quiere saber Isabel es si los estudios indicados tienen el reconocimiento oficial.

No parece que en Google o en otro buscador pueda hacer mucho más, por lo que Isabel lanza la pregunta en Twitter y le sugieren que vaya a la página de la ANECA y en ella encuentra lo que quiere: buscador de grados y másteres evaluados favorablemente. Para las personas que estén interesadas, la ANECA es la Agencia Nacional de Evaluación de la Calidad y Acreditación del sistema universitario español.

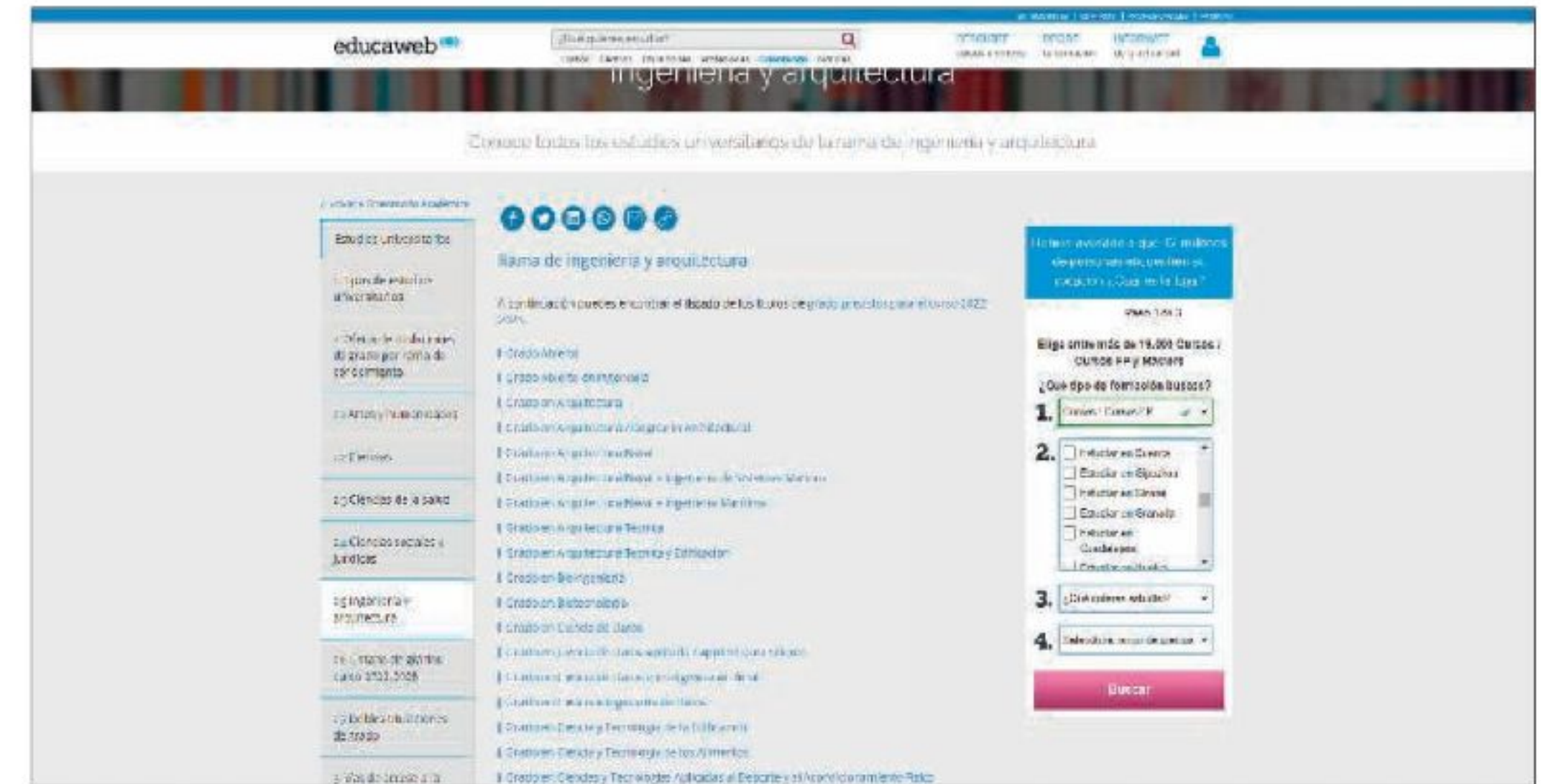


Figura 2.8. Resultado de búsqueda.

En este caso, la primera herramienta ha funcionado razonablemente, aunque no cumplía todas las expectativas, pero, tras preguntar, Isabel ha obtenido el resultado deseado en una fuente distinta del típico buscador.

Saquemos nuestras propias conclusiones sobre la forma de hacer búsquedas específicas, pues saber dónde están las cosas facilita el trabajo.

► ACTIVIDAD PROPUESTA 2.1

Búsqueda avanzada

Para practicar las búsquedas avanzadas le invitamos a plantearse realizar una búsqueda sobre un determinado tema:

- Búsqueda inicial en Google.
- Búsqueda avanzada en Google con el cuadro de diálogo que se muestra en la Figura 2.3.
- Búsqueda avanzada en Google con operadores.
- Siga el mismo esquema en Bing.

► ACTIVIDAD PROPUESTA 2.2

Otras fuentes de información

Como hemos visto, a veces hay que preguntar para saber dónde buscar.

- Trabaje con Quora. ¿Qué le parece?



2.2. Curación de contenidos

En primer lugar, conviene hacer un comentario sobre la traducción de la expresión inglesa «content curation», que se traduce por «curación de contenidos». Aunque suene algo extraño, responde a una de las acepciones de curar, que recoge la Real Academia, que es tener cuidado de algo; por tanto, la curación de contenidos es el «cuidado» de estos, como se verá a continuación.

Ahora, vamos a definir el término curación de contenidos y aprender cuál es su función. Veamos lo que dice la fuente elegida, teniendo en cuenta que en esta fuente como en otras muchas se hace un planteamiento dirigido a cierto tipo de profesionales por lo que el texto siguiente se ha adaptado para hacerlo lo más general posible:

La curación de contenidos (o content curation) consiste en seleccionar información relevante que ya está publicada en internet, filtrarla, organizarla, añadir un valor adicional y difundirla a nuestra comunidad.

Quiero llamarte la atención a una parte muy importante de esta definición: añadir valor.

¿Por qué? Porque el content curator (la persona que realiza la esta actividad digital) tiene la tarea de adaptar ese contenido a su comunidad.

Debe, por tanto, enriquecerlo cuando vaya a compartirlo, bien dando su opinión o aportando información adicional.

Es decir, un retweet no es curación de contenidos. Tampoco lo es copiar el título de un post, añadir el enlace original y difundirlo en tus perfiles sociales. Sin embargo, sí lo es si al contenido de tu difusión le añades un «plus» que no aparece en la información original.

Para realizar una correcta curación de contenidos se recomienda seguir estos 6 pasos:

1. Selecciona información relevante.

La palabra clave en este paso es «relevante».

¿Qué quiero decir con ello? Obviamente, no vas a seleccionar cualquier información sobre una temática, sino solo la que sea de interés y utilidad para tu comunidad.

Por ejemplo, si vas a hacer un artículo sobre «cómo pasar unas bonitas navidades en Laponia», no es relevante que selecciones información genérica sobre los viajes en los países nórdicos, debes saber qué necesidades vas a cubrir y debes también conocer a los usuarios a los que te diriges.

2. Filtra esta información.

No te servirá toda la información que cae en tus manos a diario. Ni tampoco toda la que vas a salir a buscar para ese tema concreto que quieres abordar, vas a tener que hacer una selección de aquella que te encaja con las respuestas que quieres dar a tus usuarios.



Con el ejemplo de Laponia, es posible que no te interese la información que encuentres sobre las navidades en otros lugares de Finlandia.

3. Organiza todos los datos filtrados.

Ordena lo que has encontrado, para que te resulte más fácil elaborar el artículo nuevo que estás preparando.

Para este mismo caso de Laponia, los posibles grupos de información podrían ser, preparativos, fechas más adecuadas de salida, compañías aéreas que vuelan a Laponia, hoteles, tradiciones, etcétera.

4. Añadir información de valor.

Todo ese contenido que has recopilado lo debes poner en una coctelera, añades tus ingredientes secretos, agitas y ¡listo! Ya tienes tu bonito artículo sobre las navidades en Laponia.

Añade experiencias personales, define un título atractivo, haz un buen índice, completa la información con datos que conoces por otras vías, etcétera.

5. Difunde el nuevo contenido.

Si no das a conocerla información, es como si tuvieras una tienda en un callejón oscuro a las afueras de la ciudad: nadie te va a leer.

Así que compártelo en las redes sociales en las que estás presente, súbelo a los agregadores de noticias, publícalo en tu blog, etcétera.

6. Mide los resultados obtenidos.

El último paso que debemos dar es saber si nuestra publicación ha tenido éxito.

¿Cuáles son los beneficios de la curación de contenidos digitales?

- Recopilas una amplia cantidad de información, que te ayuda a crear tus propios artículos, ya sean los de tu web o blog.
- Aprendes, porque lees cosas nuevas, que seguramente hablan de temas que tú desconoces o que mejorarán tus conocimientos.
- Son el soporte para hacerte visible en las redes sociales, ya que aprovechas esos contenidos de calidad para difundirlos en tu comunidad y que te conozcan.
- Te ayuda a mejorar tu reputación digital, ya que puedes posicionarte como un especialista en la materia.
- Facilita los contactos, porque al colaborar con la difusión de los contenidos de otros, si lo haces bien, ellos seguramente te lo van a agradecer.
- Aumentas el número de seguidores, como consecuencia de los puntos anteriores⁸.

⁸ <https://www.webempresa.com/blog/curacion-de-contenidos.html>



Como se desprende del texto anterior la curación de contenidos se hace tomando como referencia a un grupo o comunidad de personas que puedan estar interesadas en un tema determinado, por lo que hemos de contemplarla como destinatarios de la información o como elaboradores de esta.

La primera fase de la curación de contenidos es la recopilación de información, veamos las recomendaciones de la fuente citada.

Manejar un alto volumen de información puede hacer que nos saturemos de ella, nos bloqueemos y seamos incapaces de seguir con la tarea que estábamos realizando.

Por suerte, existen herramientas que te ayudan a superarla y que te dan soporte en las fases que hemos descrito. Vamos con las 10 que, desde mi punto de vista, te ayudarán a horrar más tiempo, realmente, en tu trabajo.

1. Feedly

Si eres un recién llegado a este mundillo y no conoces Feedly, te recomiendo que vayas a abrirte un perfil en ella inmediatamente, además de ser muy popular es gratuita (en su mayor parte) y muy intuitiva.

Es un lector de RSS que te permite seguir los blogs que te interesan y organizarlos en diferentes categorías.

También puedes crear alertas, equipos de trabajo con los que compartir los contenidos que filtras y detectar aquellos blogs inactivos o desaparecidos.

2. Pocket

Otra herramienta gratuita excelente.

Una vez la vinculas a tu navegador instalando el pequeño botón de Pocket, puedes guardar en ella todas las URLs que te parezcan interesantes.

Yo guardo incluso las URLs de los emails que sé que necesitaré consultar en unos meses. Por ejemplo, las suscripciones que tengo a los blogs de algunos colegas.

Las opciones son las de clasificarlas en categorías que tú decides, leer más tarde, vídeos, etcétera.

3. Content Gems

Esta es una herramienta de curación de contenidos que te ofrece los artículos ya publicados en internet a partir de la búsqueda que defines. Se diseñó pesando exclusivamente en ayudar a profesionales del marketing digital.

Igual que ocurre con las anteriores, puedes definir categorías o nichos de mercado que te interesan y la herramienta te avisa, vía email, de las nuevas publicaciones que aparecen en él.



4. Buffer

Para la fase de difusión de contenidos ya curados te recomiendo Buffer, por la rapidez en programar. Tan solo tienes que vincular tus redes sociales: Twitter, LinkedIn, Facebook, Google+, Instagram y Pinterest y listo.

En la versión gratuita puedes conectar un perfil por red social y programar un máximo de 10 publicaciones en cada una.

5. Alertas de Google

Otra utilidad de Google, que podemos también utilizarla como herramienta para la curación de contenidos.

Mi recomendación es que utilices un email solo para ello, si no quieres agobiarte cuando veas la bandeja de entrada de tu correo electrónico principal.

6. Agregadores de contenidos

Son espacios digitales en los que los autores subimos nuestros artículos, con la intención de darles difusión, los posts son votados por otros usuarios y solo unos pocos llegan a ser portada.

El beneficio que tú puedes obtener de ellos para la curación de contenidos es que, gracias a esos votos, sabes cuáles son los que más han gustado.

Te menciono 5 de los más utilizados por la comunidad de bloggers:

- MarketerTop.
- Mktfan («Marketing Fan»).
- Bloggers.net.
- Menéame.

7. Paper.li

Paper.li es un periódico digital que construyes tú mismo. Me parece una herramienta muy divertida para la curación de contenidos.

- La de recopilar artículos que te vayan a ser útiles para tus nuevos artículos.
- La de aprovechar esos posts que te resultan interesantes, organizar tu periódico y difundirlo.

Es decir, además de obtener información, la reorganizas para darte visibilidad.

8. Scoop.it

Scoop.it te permite realizar una selección de tus artículos de interés, publicados en diferentes redes sociales, y llevarlos a una misma plataforma. En ella, muestras los contenidos como si fuera una pizarra.



9. Storify

Esta es otra herramienta que me resulta interesante de utilizar. Storify te ofrece la posibilidad de crear historias, a través de una presentación de transparencias.

Puedes utilizarla con información recabada de diferentes redes sociales. Por ejemplo, para hacer un resumen de un «Twitter Chat», para diseñar manuales, para dar consejos sobre tareas, etcétera.

10. Flipboard

Flipboard es otra herramienta muy interesante y divertida.

¡Qué bien te lo puedes pasar haciendo curación de contenidos!

Si antes hablábamos del periódico digital, ahora vamos con la revista. Aquí, eliges los temas que te interesan, sigues las revistas de otros usuarios o construyes la tuya propia⁹.

Es, realmente, mucha información, hay que leerla con calma y trabajar con ella, para lo que proponemos las correspondientes actividades.

Aunque nos hemos resistido hasta ahora a utilizar la palabra **infoxicación**, no hay más remedio que hablar de ella (por cierto, no aparece en el diccionario de la RAE).

La infoxicación es el exceso o sobrecarga de información, que te impide profundizar en los temas que abordes¹⁰. En esta fuente hay información muy interesante sobre el tema, pero nosotros la vamos a utilizar para presentar el siguiente apartado, la veracidad de la información, pues en muchas ocasiones la desconfianza en las fuentes hace que se repitan las búsquedas y que lleguemos a tener tal cantidad de información que no sepamos qué hacer con ella.

2.2.1. Técnicas de detección de veracidad de la información

Al hablar de este tema conviene hacer una reflexión inicial: en internet hay muchas fuentes de información que se nutren de las aportaciones de las personas, de cualquier persona, y que no requieren de ningún filtro previo para publicar la información, más allá de unas mínimas normas de corrección como es el caso de algunas redes sociales.

Cualquiera puede aportar información; en algunos casos basta registrarse y subir material para poder descargar lo que hay en ellas, y en otros ni siquiera es necesario ese requisito. Nos referimos a sitios como Wikipedia, El Rincón del Vago (el nombre lo dice todo) o Gestipolis, cuyo problema no es que no haya buena información, sino que no son fiables al no estar contrastada la información. Hace falta ser experto para saber si una determinada información es buena y, por lo tanto, utilizarlos para aprender algo es muy arriesgado.

⁹ <https://www.webempresa.com/blog/curacion-de-contenidos.html>

¹⁰ <https://www.webempresa.com/blog/que-es-infoxicacion.html>



Los ejemplos citados muestran la necesidad de disponer de fuentes fiables y de mecanismos para comprobar la veracidad de la información, pues no siempre es cuestión de fraude o mala voluntad, a veces es simple ignorancia.

Veamos de qué se dispone para comprobar, o asegurar, la veracidad de la información; en primer lugar, un enfoque es el que se muestra a continuación, donde se dan una serie de consejos:

Usar fuentes oficiales

De esta manera, para ir más allá de la mera apariencia y verosimilitud —recuerda que en la red tiene la posibilidad de escribir cualquiera— existen una clase de recursos, herramientas y trucos que deberías poner en marcha. Para empezar, decántate siempre por las fuentes originales.

Por ejemplo, si en una noticia se incluye un dato sobre un informe completo, pero no se incorpora el enlace correspondiente, deberías sospechar. En primer lugar, desconocemos la vigencia de este supuesto «reciente» o «nuevo» estudio y, en segundo, la fuente puede ser interpretada de múltiples modos. Así que búscala. Ocurre lo mismo con las referencias a determinados medios internacionales, estadísticas y similares.

Buscadores académicos

Como comentábamos y a pesar de que es posible encontrar cantidades ingentes de información de todo tipo, existen determinadas ocasiones en que no podemos permitirnos, bajo ningún concepto, que nuestras fuentes se cuestionen. Es el caso de los trabajos de investigación, en los que comprobar cada dato resulta básico.

Expertos en la materia

Aunque, a priori, puede parecer complicado contactar con un experto en la materia que quiera y pueda explicarnos el asunto que tratamos con conocimiento de causa, LinkedIn y otras plataformas similares nos han puesto las cosas más fáciles. Sí, porque estas herramientas nos permiten dirigirnos a distintos profesionales.

Asimismo, que contactes con ellos no deja de ser algo halagador, pues se les está reconociendo su condición y méritos. Sé amable, paciente, identifícate siempre y pregunta con educación sobre el tema que estás investigando. Merece la pena y te llevarás una grata sorpresa.

Reportaro (que actúa en España y América Latina) también te servirá, pues se trata de una aplicación que pone en contacto a periodistas y blogueros con expertos y fuentes personales de manera gratuita. Eso sí, dispone de varias versiones Premium que, si bien amplían la información, no resultan especialmente baratas.



Revistas y medios especializados

Para encontrarlos, acude a páginas y servicios como Google Académico, Microsoft Academic Search, RefSeek, ERIC, y otros. Acuérdate —siempre que tengas la opción— de seleccionar el tipo de documento que quieres encontrar, sé concreto y sítete de símbolos como ~ para incluir sinónimos en tus búsquedas, así como de herramientas como la RAE y su Diccionario Panhispánico de Dudas para las definiciones. Otra página que pueden serte de ayuda es Wordreference, que te permitirá encontrar sinónimos más exactos que se ajusten a tus objetivos.

Tampoco dejes de lado Google News que, si bien ha quedado ciertamente limitado en nuestro país, te servirá para dar con artículos actuales sobre el tema que vas a tratar, organizarlos según su fecha de publicación, y demás. Además, estos escritos te serán de utilidad a la hora de formarte una idea de lo que opina la comunidad internacional. Y si no sabes idiomas, siempre puedes servirte del traductor para hacerte una idea general.

Reputadas multinacionales

Para que te hagas una idea, si lees acerca de que una multinacional o gran empresa ha logrado determinados resultados en la bolsa, ha presentado ciertas novedades, etcétera; lo más apropiado será que acudas a su página. La mayoría de ellas, de hecho, cuentan con kits de prensa, un blog específico en el que recaban sus últimas noticias e iniciativas, y similares.

Legislación

En caso de dudas y a pesar de que consultes con un abogado, es recomendable que verifiques lo que dice a través de los diferentes códigos civiles y penales del correspondiente país, reglamentos, normas y demás con el objetivo de cerciorarte de que los datos que te han brindado son ciertos. Para lograrlo bastará con que acudas a las webs estatales que se correspondan con el asunto que aboradas.

Además, en ellas se suelen incluir estadísticas, gráficos y otros recursos. Indaga en la estructura de las administraciones, ayuntamientos, órganos gubernamentales y otras instituciones relacionadas con el tema de interés. En ocasiones estos sitios no resultan intuitivos. Ten paciencia y sigue indagando hasta dar la respuesta adecuada a tus dudas. Y ahí va un truco sencillo: ponte en contacto con ellos mediante el teléfono de atención, en muchas ocasiones es la opción más ágil.

Bibliotecas online

Las referencias bibliográficas de calidad tampoco resultan fáciles de lograr. Por fortuna, nos topamos con una serie de bibliotecas online que te permitirán agilizar esta ardua tarea. Entre ellas nos quedamos con The Free Library, Gallica y Questia, aunque su variedad es amplia.

Para que te hagas una idea, esta primera consiste en un catálogo de recursos online; un sitio que contempla varios ámbitos técnicos —como la salud, el derecho, la comunicación, los negocios, etcétera— y que contempla desde boletines recientes hasta noticias vigentes publicadas en revistas y periódicos especializados.

Respecto a Gallica, nos brinda la oportunidad de revisar libros enteros y reúne más de 1 millón de referencias organizadas por categorías (libros, mapas, prensa, distribuidores, etcétera). Questia, por su parte, se trata de una biblioteca multilingüe con más de 77 mil libros completos de hasta 300 editoriales distintas, artículos de revistas especializadas y demás. Cuenta con un acceso privilegiado a fuentes originales y dispone de filtros de búsqueda con diversos campos que te serán de utilidad.

Redes sociales y comunidades específicas

Las redes sociales y determinadas comunidades resultan de utilidad en casos muy concretos. Y no nos estamos refiriendo a foros en los que cualquier mindundi insulte, vilipendie o tergiverse los datos, sino a entidades de la talla de Reddit y similares. En cuanto a los foros y blogs, constituyen un excelente punto de partida, pero no olvides contrastar lo que se dice.

Asimismo, Twitter también resulta de gran ayuda a la hora de determinar determinadas tendencias, y averiguar la opinión real acerca de un acontecimiento o polémica actual. Tal es así que, ya en 2011 se afirmaba que casi la mitad de los periodistas usaba la plataforma de microblogging para mantenerse informado. Además, los comentarios y seguimientos durante presentaciones y directos son muy útiles.

Trucos

Al margen de lo comentado, no podemos dejar de lado algunos consejos a la hora de encontrar información como un auténtico profesional. Por ejemplo, sítete de las búsquedas avanzadas.

Asimismo, puedes tener en cuenta otra serie de rasgos para identificar la veracidad de la información online como, por ejemplo, comprobar siempre la vigencia del artículo o legislación consultados, ponerse en contacto con un conocido que entienda de la materia (trabaje en el sector o similares, no hace falta que acudas a LinkedIn si un familiar o amigo es especialista, ¿no crees?), buscar más datos sobre el autor (consultar su trayectoria, autoridad y credenciales), e investigar sobre el método con el que se ha conseguido la información que se cita.

Otras cuestiones que no deberías perder de vista son si la información se ha actualizado, si resulta objetiva o se trata de una mera opinión sesgada, así como el nivel de profundidad del contenido (incluso su presentación), el propósito con el que ha sido escrito, su concreción y precisión, y su relevancia respecto de nuestro «objetivo»¹¹.

¹¹ <https://www.genbeta.com/a-fondo/9-herramientas-y-otros-trucos-para-identificar-la-informacion-mas-fiable-en-internet>



En los párrafos anteriores se plantea dónde, y en algunos casos cómo, buscar para encontrar información fiable. Se puede resumir diciendo que hay que utilizar fuentes originales y rigurosas y utilizar búsquedas avanzadas lo más concretas posible.

Un aspecto muy importante, que se cita de pasada, es la actualidad de la información; por ejemplo, al preparar el apartado de curación de contenidos el autor encontró varias informaciones sobre Delicious, sitio que se cerró hace años, por lo que esa información es inútil para conocer los sitios que están en funcionamiento al redactar este apartado. Hay que comprobar la vigencia de los datos y de la información obtenida.

Muchos internautas leen la prensa en la red. Es interesante tener unas pautas para tratar de detectar las noticias falsas, veamos los consejos de la BBC:

Cinco consejos...

- *Tómate un minuto y piensa. No te creas la noticia ni compartas el texto de inmediato.*
- *¿Te causó una reacción emocional muy grande? Desconfía. Las noticias inventadas se hacen para causar grandes sorpresas o rechazo.*
- *¿Confirma alguna convicción que ya tenías? También es una técnica habitual de las noticias inventadas. Desarrolla el hábito de desconfiar e investigar.*
- *¿La noticia está «pidiendo» que creas en ella o «muestra» por qué desconfiar? Cuando una noticia es cierta, es más probable que cite fuentes, que incluya enlaces y que cite documentos oficiales (en decir, que sea transparente).*
- *Producir un reportaje tan pronto como acontecen los eventos toma tiempo y exige profesionales cualificados. Desconfía de las noticias «bomba» en el calor del debate.*

...y nueve pasos

1. *Lee la noticia entera, no solo el titular.*
2. *Averigua la fuente.*
 - *¿Es una cadena de WhatsApp sin autoría o sin enlace? Desconfía y, preferentemente, no la compartas.*
 - *¿Tiene autoría? ¿Es una fuente legítima en la que hayas confiado en el pasado? Investiga el nombre del medio o del autor en Google para ver qué más hizo esa persona y para qué medios trabaja. Presta atención a si el sitio que reprodujo la noticia publica cosas solo de un lado político con algún sesgo ideológico.*
 - *¿Hace referencia a un medio de comunicación? Entra a la página web de ese medio para comprobar si la noticia está ahí.*
3. *Busca el titular en Google. Si es verdadera, es probable que otros medios confiables la hayan reproducido; si es falsa, puede que algunos sitios de verificación de datos hayan averiguado que es un rumor falso.*



4. *Busca los datos que se citan. ¿Se apropia de acontecimientos verificables? Si afirma que alguna autoridad dice algo, ¿hubo otros medios que reprodujeran lo que dijo?*
5. *Verifica el contexto, como la fecha de publicación. Sacar una noticia de contexto y divulgarla en una fecha diferente también es una forma de desinformación.*
6. *Pregúntale a quien te mandó la noticia de quién la recibió, si confía en esa persona y si logró verificar alguna información.*
7. *¿Recibiste una imagen que cuenta una historia? Puedes hacer una búsqueda «inversa» de imágenes y comprobar si otros sitios la reprodujeron. Guarda la foto en la computadora y súbela en <https://images.google.com/> o en <https://reverse.photos>.*
8. *¿Recibiste un audio o un video con informaciones? Trata de resumirlas y búscalas en internet introduciendo las palabras clave y WhatsApp.*
9. *Piensa en números: ¿la noticia cita cifras de investigaciones o de otros datos? Búscalos para ver si tiene sentido¹².*

Una vez más, sentido común y prudencia.

Para terminar, conviene conocer otro aspecto de la información que es importante en ciertos ámbitos, como el académico. Nos referimos a la autoría u originalidad de la información.

Al redactar documentos o trabajos es habitual buscar información en la red y utilizarla. En esta obra se hace con frecuencia para poner a disposición del lector la opinión de expertos y proporcionarle fuentes a las que acudir para ampliar sus conocimientos; por eso se cambia el tipo de letra y se indican las citadas fuentes, para poner de manifiesto que no es material original del autor.

También hay herramientas para detectar el plagio, o la copia, que no siempre se hace con mala intención. Una de las más conocidas es Turnitin que, entre otras cosas, ofrece un inmenso repositorio de documentación con la que comparar. Para más información es posible visitar su web.

2.2.2. Fuentes de contenidos digitales abiertos

¿Qué son los contenidos digitales abiertos?

Los contenidos digitales abiertos se caracterizan por la integración de conjuntos de información multimodal, por una organización y sentido propio, por su publicación en la red mediante aplicaciones sociales que permiten a los usuarios, modificar, reutilizar, combinar, hacer comentarios, recomendaciones, seleccionar, registrar, y cualquier otra operación de reconstrucción o remezcla por adición, supresión, yuxtaposición y combinación.

¹² <https://www.bbc.com/mundo/noticias-45561204>

Este tipo de uso de los contenidos es posible por la apertura y flexibilidad de sistemas de licenciamiento de derechos de propiedad intelectual como Creative Commons y otros. Son sistemas derivados de la alternativa al Copyright, es decir, del CopyLeft, cuya existencia y proliferación está estrechamente relacionada con las capacidades socio técnicas de la Web Social y especialmente por las posibilidades crecientes de la computación distribuida en la nube¹³.

Un ejemplo muy conocido de contenido digital abierto es Wikipedia.

Veamos el significado de ciertos términos.

ARGOT TÉCNICO

- **Copyright:** derechos de autor. El copyright representa los derechos de autor que se le conceden a los creadores de una obra literaria, tema musical o artículo científico, entre otras¹⁴.
- **Copyleft:** el copyleft es un método general para liberar un programa u otro tipo de trabajo (en el sentido de libertad, no de gratuidad), que requiere que todas las versiones modificadas y extendidas sean también libres¹⁵.
- **Creative Commons:** las licencias de derechos de autor Creative Commons y sus herramientas, forman un equilibrio dentro de la premisa tradicional de «todos los derechos reservados» que las leyes de propiedad intelectual establecen. Nuestras herramientas proporcionan a todo el mundo, desde el creador individual a grandes compañías, así como a las instituciones, una forma simple y estandarizada de otorgar permisos legales a sus obras creativas. La combinación de nuestras herramientas y nuestros usuarios conforma un vasto y creciente patrimonio digital, un conjunto de contenido que puede ser copiado, distribuido, editado, remezclado y desarrollado, todo ello dentro de los límites de la ley de propiedad intelectual¹⁶.

Como vemos, se trata de formalizar los contenidos libres, de modo que puedan ser utilizados por cualquier usuario, dentro de los límites impuestos por la legislación de propiedad intelectual, sin estar sometidos al rigor de los derechos de autor; pero no olvidemos que es el autor el que puede permitir el uso libre de sus obras.

Para ver un ejemplo de licencia Creative Commons recurrimos a Wikipedia. En las Figuras 2.9 y 2.10 mostramos dos capturas de pantalla de la página de Wikipedia. En la Figura 2.9 podemos ver que está bajo licencia Creative Commons y en la Figura 2.10 informa sobre los términos de la licencia.

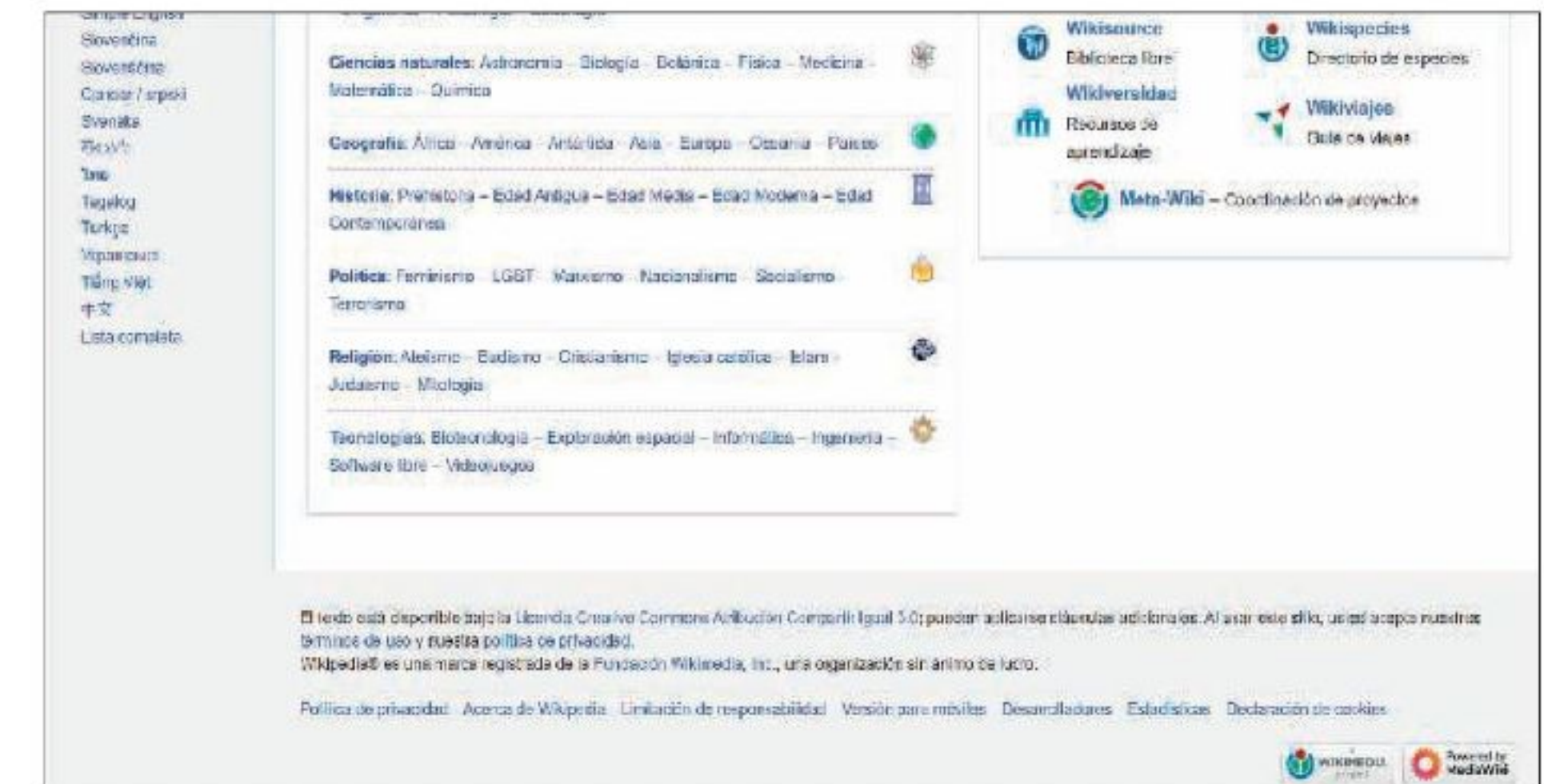


Figura 2.9. Wikipedia y Creative Commons.



Figura 2.10. Wikipedia y Creative Commons.

No parece haber una clasificación clara de los contenidos digitales abiertos (CDA), que en opinión de algunos autores¹⁷ incluyen conceptos tales como los sistemas de publicación de CDA, habituales en la elaboración y difusión de material educativo; las wikis (el término «WikiWiki» es de origen hawaiano y significa rápido; de forma abreviada se utiliza Wiki, que es un software para la creación de contenido de forma colaborativa); los entornos multijugador; y los sistemas sociales de calificación, utilizados, por ejemplo, por las empresas para obtener todo tipo de datos, entre otros.

¹³ <http://www.redalyc.org/articulo.oa?id=82319126006>

¹⁴ <https://economipedia.com/definiciones/copyright.html>

¹⁵ <https://www.gnu.org/licenses/copyleft.es.html>

¹⁶ https://creativecommons.org/licenses/?lang=es_ES

¹⁷ <https://burjcdigital.urjc.es/bitstream/handle/10115/7242/36991-39288-1-PB.pdf?sequence=1&isAllowed=y>



La principal ventaja de los CDA es que favorecen la comunicación y la colaboración entre personas, siendo esa su principal vulnerabilidad: el depender de los conocimientos y buena voluntad de los usuarios para generar contenidos de calidad.

Una vez más, hay que apelar a la corrección y a la prudencia, hay que ser consciente del tipo de licencia que ampara un determinado material y respetar sus condiciones de uso.

► ACTIVIDAD PROPUESTA 2.3

Curación de contenidos

Al hablar de curación de contenidos hemos listado una serie de herramientas. Para familiarizarse con ellas, le proponemos las siguientes actividades:

- Alertas de Google: abra dos o tres alertas y vea cómo funcionan, la información que recibe, etc. Piense en la posibilidad de abrir una nueva cuenta de correo para recibir esta información.
- Visite las páginas web del resto de sitios para ver lo que ofrecen y su utilidad para un usuario no profesional.

► ACTIVIDAD PROPUESTA 2.4

Wikis

Busque wikis e información sobre los wikis. Hay sitios muy curiosos.
Recomendación: utilice las técnicas de búsqueda avanzada.

► ACTIVIDAD PROPUESTA 2.5

Sistemas sociales de calificación

Busque información sobre este tema. Además de ser un ejemplo de CDA, puede tener importantes repercusiones en determinadas circunstancias de la vida.



2.3. Almacenamiento de contenido en la nube (Dropbox, Google Drive, OneDrive de Microsoft)

Comenzaremos este apartado recomendando trabajar en la nube, especialmente en lo que se refiere al almacenamiento y custodia de la información que, de este modo, dejamos en manos de profesionales.

Para poder trabajar así hay que disponer de conexión a la red y, dependiendo de la cantidad y tipo de información que manejemos, de una conexión de calidad.

Cuando necesitamos la información y no tenemos acceso a internet, conviene tenerla almacenada en alguno de los dispositivos que existen para ello, sea el propio disco duro del ordenador, un disco externo, una memoria USB, etc., pero ello no implica que, además, no esté en la nube, de donde lo podremos recuperar en caso de accidente.

En resumen, es muy conveniente que la información relevante está almacenada en la nube.

Hay muchos proveedores de este tipo de servicios en la nube, gratuitos y de pago, pero nos vamos a centrar en tres que, según algunas fuentes, son de los más utilizados (Dropbox, Google Drive y OneDrive de Microsoft) y cómo introducción veamos un resumen de los cinco más utilizados según la fuente citada.

Amazon Cloud Drive. El almacenamiento en línea que ofrece Amazon está entre los mejores. Una de sus ventajas es que, si eres miembro de plataformas alternas como Amazon Prime, automáticamente, te haces acreedor a 5 GB de almacenamiento gratuito para todo tipo de archivos.

Dropbox. Entre los servicios de almacenamiento más populares, encontramos a Dropbox. Su plan gratuito ofrece una capacidad limitada, pero se puede ampliar si invitas a otros usuarios para que se unan a la plataforma.

Google Drive. Definitivamente, uno de los más utilizados es el producto estrella de Google. Este viene instalado predeterminadamente en Android y Chrome, y su capacidad de almacenaje en la versión gratuita es bastante buena. Otro punto fuerte radica en la edición de documentos en línea entre varios usuarios, lo que facilita el trabajo en equipo y lo convierte en una opción ideal para empresas y usuarios.

OneDrive. El caballito de batalla de Microsoft es uno de los más completos y de los que ofrecen más beneficios; tan solo su versión gratuita te facilita varios gigabytes para almacenar documentos y diversos archivos. Al igual que Google Drive, OneDrive te permite editar archivos con Microsoft Office, por lo cual es la opción preferida por aquellas empresas que trabajan con el servicio de correos Outlook.

iCloud. Apple no se quedó atrás en este ámbito y con iCloud brinda el servicio de almacenamiento exclusivo para todos sus usuarios. Es bastante completo, ya que no se concentra solo en almacenar archivos, también te permite guardar otros elementos como calendarios o contactos, por mencionar algunos¹⁸.

¹⁸ <https://mediaimpact.pe/los-5-servicios-de-almacenamiento-en-la-nube-mas-utilizados>

2.3.1. Dropbox

Para ver lo que nos ofrece Dropbox, vamos a mostrar una secuencia de capturas de pantalla tomadas de su web. En ellas (Figuras 2.11, 2.12, 2.13, 2.14 y 2.15) está la información básica que necesitamos para empezar a trabajar con la versión gratuita.



Figura 2.11. Dropbox.



Figura 2.12. Dropbox.

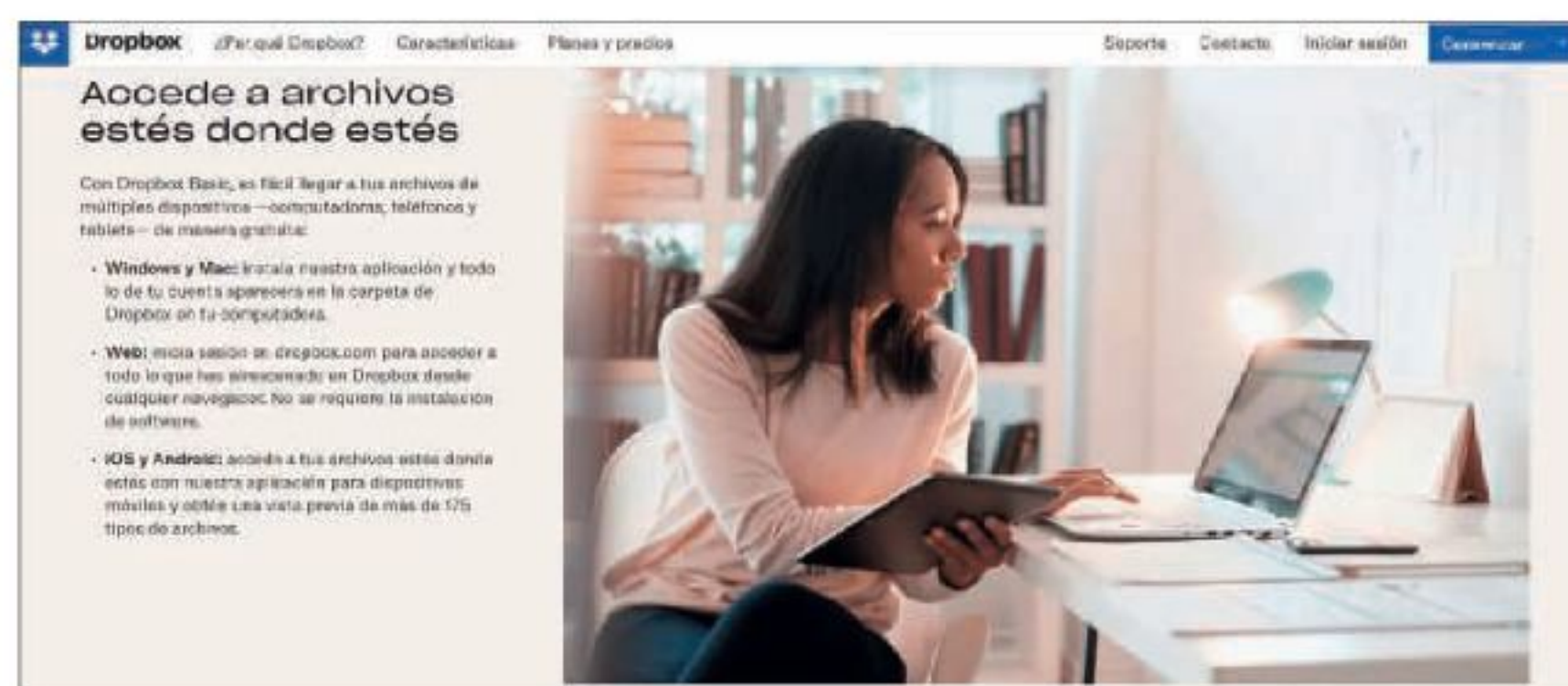


Figura 2.13. Dropbox.

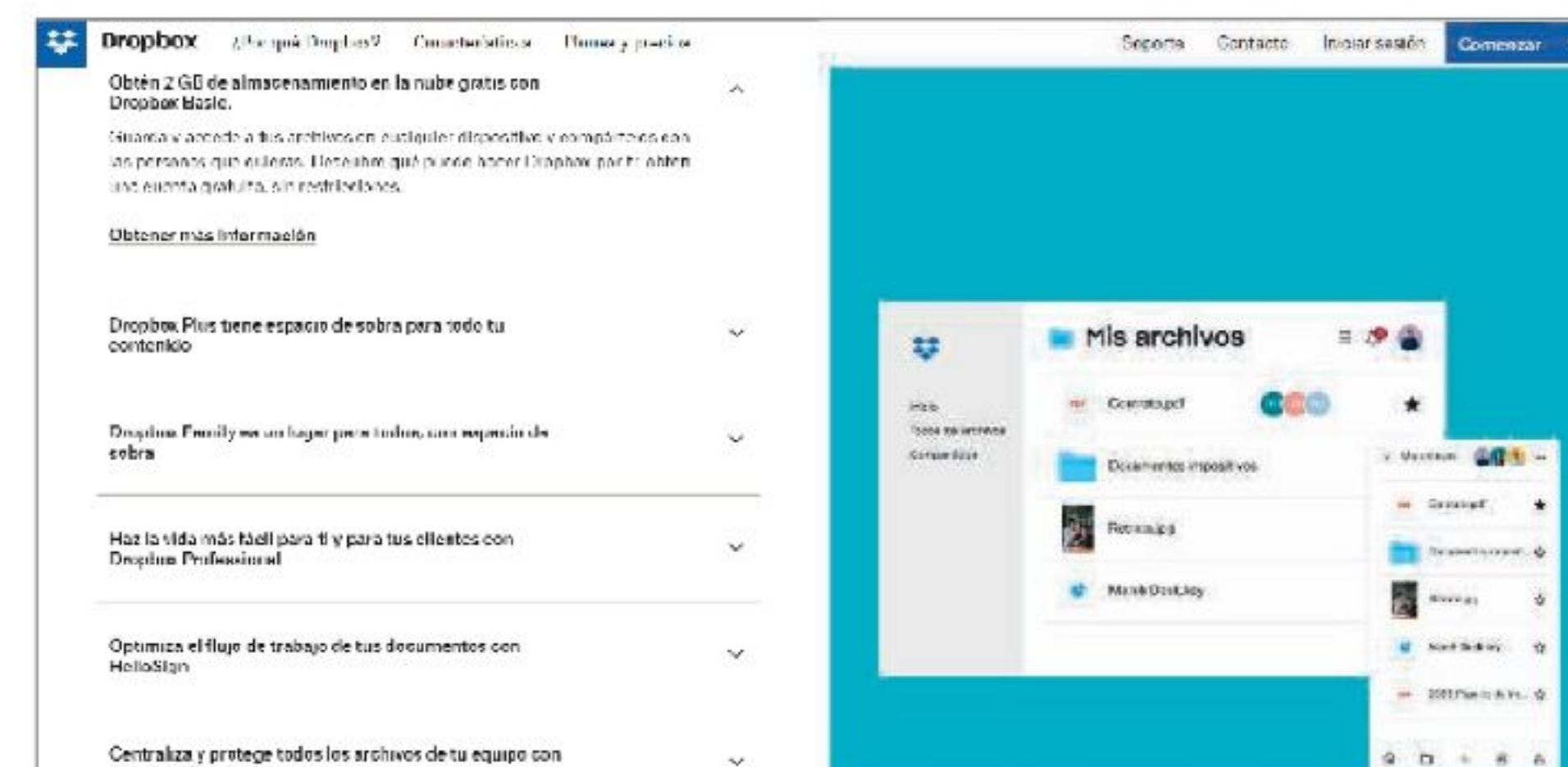


Figura 2.14. Dropbox.

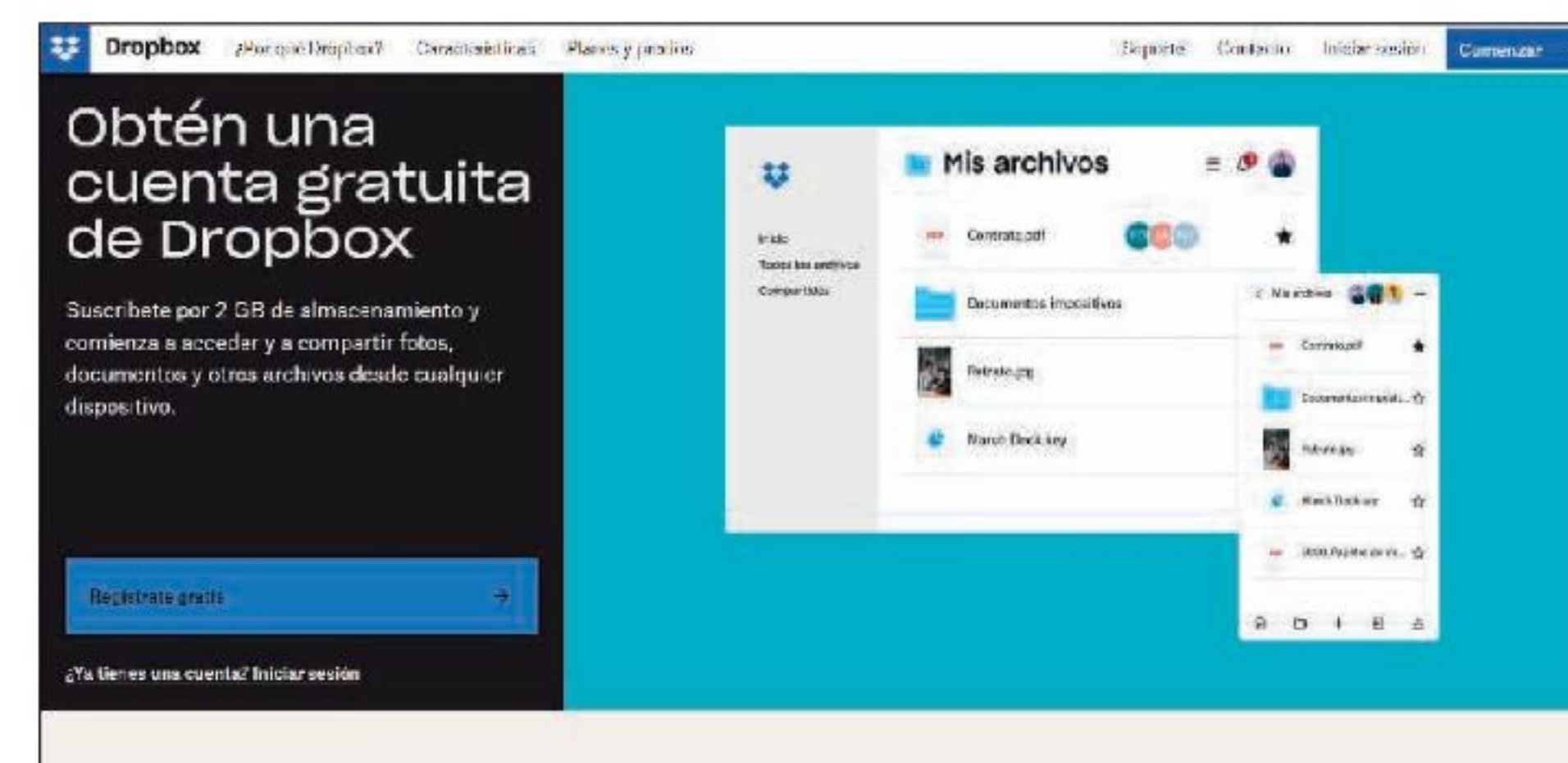


Figura 2.15. Dropbox.

En resumen, basta con instalarlo en nuestro ordenador y empezar a usarlo; como es habitual, la versión gratuita tiene una capacidad limitada, aunque hay distintas opciones de pago, que conviene conocer.

No está ligado a ningún otro servicio, aunque es compatible con otros muchos programas como se indica en su web.

Para más información sobre su uso, podemos recurrir a Xataka¹⁹.

¹⁹ <https://www.xataka.com/basics/dropbox-24-trucos-algun-extra-para-exprimirlo-al-maximo>

2.3.2. Google Drive

Es una aplicación de Google a la que podemos tener acceso con una cuenta de Google, disponible cuando tenemos Gmail. Para aprender a utilizarlo basta con seguir los pasos de la ayuda²⁰ que mostramos en la Figura 2.16.

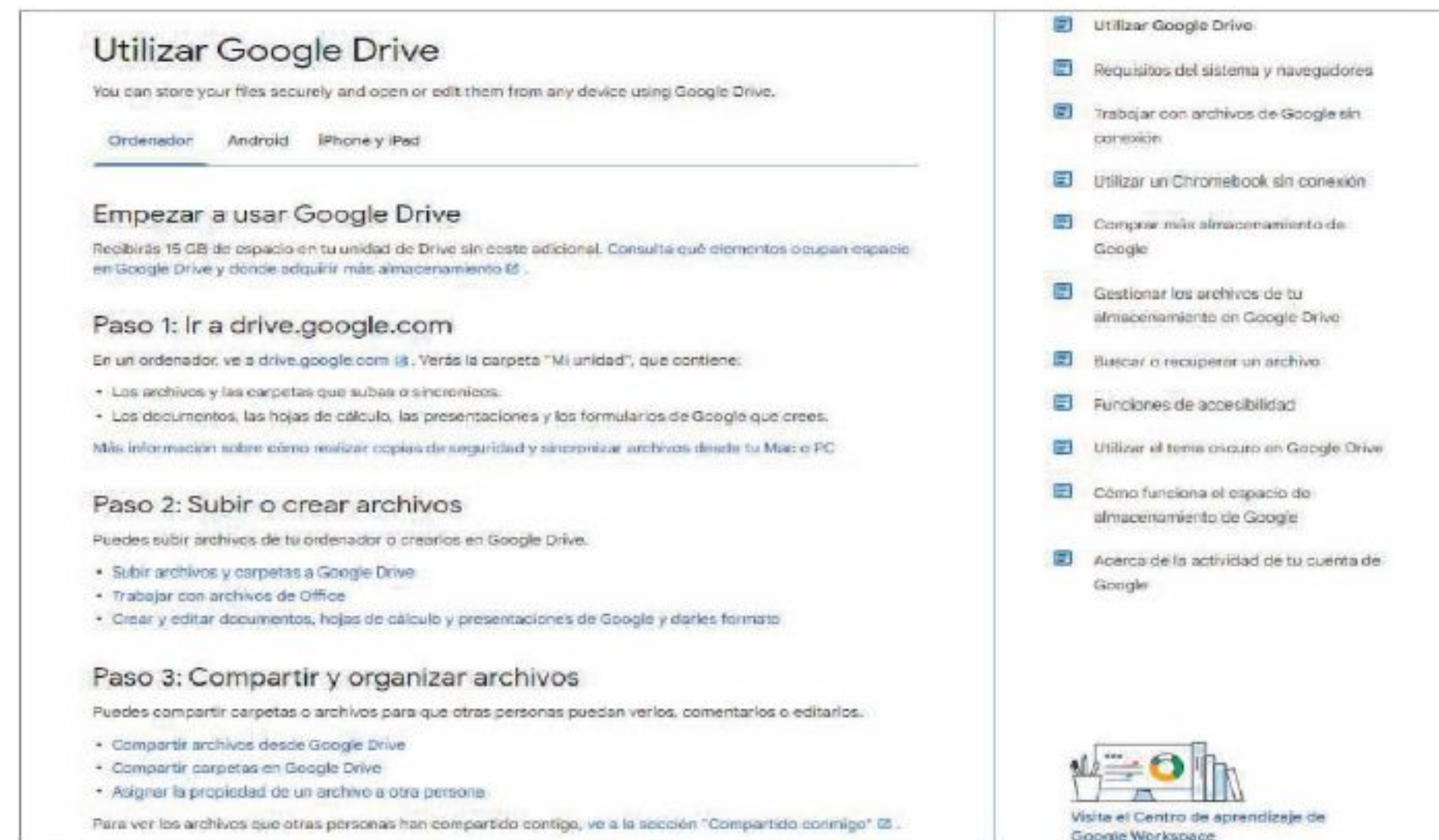


Figura 2.16. Google Drive.

Una vez que tenemos la cuenta, basta con picar en el icono que aparece en aplicaciones de Google y entramos en nuestro Google Drive.



Figura 2.17. Google Drive.

Ya podemos empezar a subir documentos, teniendo en cuenta que si optamos por la versión gratuita la capacidad es limitada. En caso de necesitar más, debemos informarnos en la página indicada y ver qué otras opciones hay.

²⁰ https://support.google.com/drive/answer/2424384?hl=es&ref_topic=14940

2.3.3. OneDrive

OneDrive es una aplicación de Microsoft ligada a sus otros programas como Windows, Office, etc. Para ver lo que ofrece y aprender a utilizarlo, lo mejor es usar el tutorial que mostramos en la Figura 2.18²¹ y también consultar Crehana²².

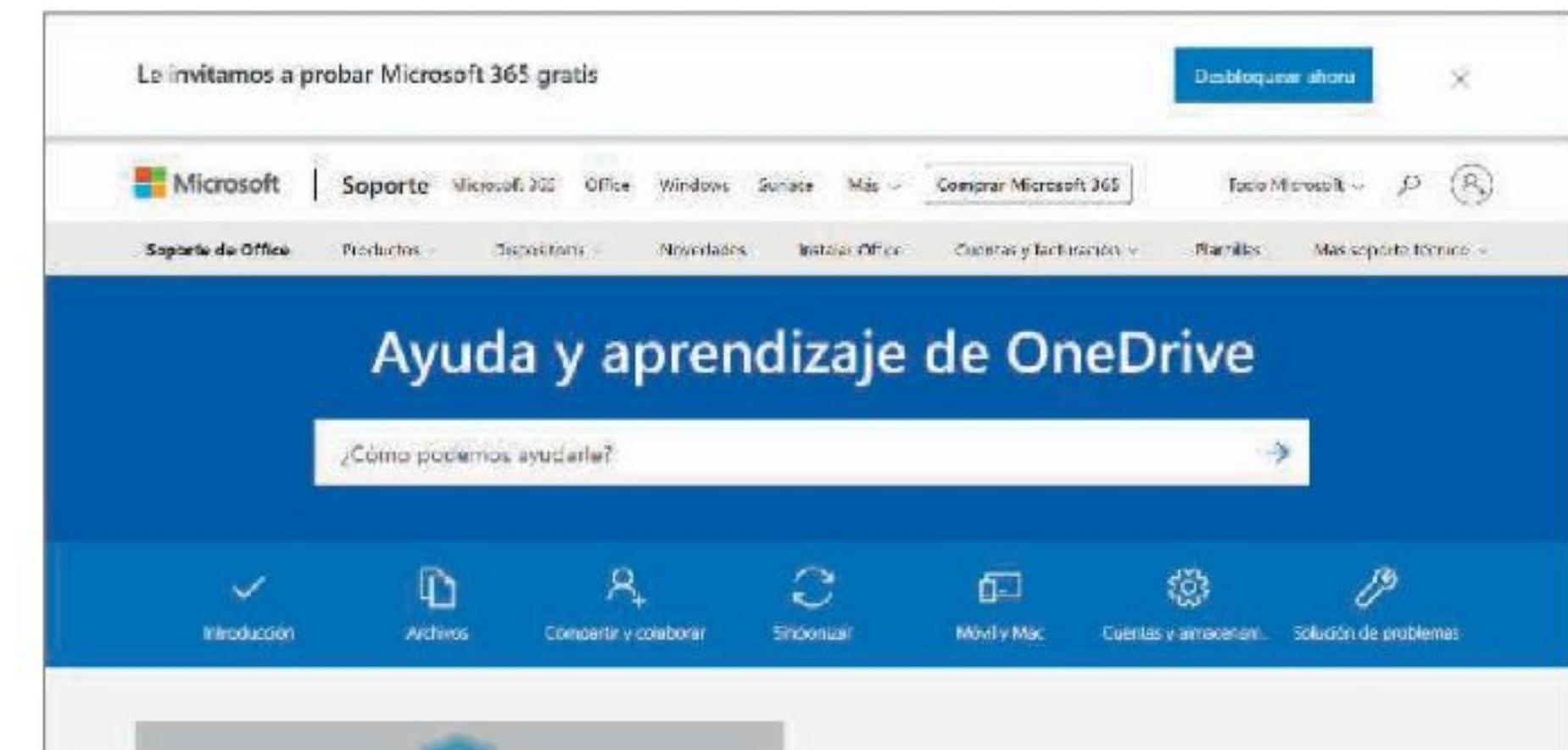


Figura 2.18. OneDrive.

Si trabajamos con Windows 10, OneDrive ya está instalado por defecto en nuestro ordenador y solo hay que empezar a utilizarlo.



Figura 2.19. Icono de OneDrive.

La forma de utilizar los tres sistemas de almacenamiento es similar. Como ejemplo, mostraremos la forma de guardar un documento de Word conforme vamos redactando.

²¹ <https://support.microsoft.com/es-es/onedrive?ui=es-es&rs=es-es&ad=es>

²² <https://www.crehana.com/blog/negocios/onedrive-para-que-sirve>

Al abrir un documento de Word, en la esquina superior izquierda de la pantalla, al lado del icono de Word, aparece la palabra *Autoguardado* y un interruptor. Cuando lo activamos (desplazando el punto hacia la derecha), aparece lo que mostramos en la Figura 2.20. Picamos en *OneDrive: Personal* y ya está hecho (debajo de *OneDrive: Personal* aparece la dirección de correo del usuario, que hemos ocultado).

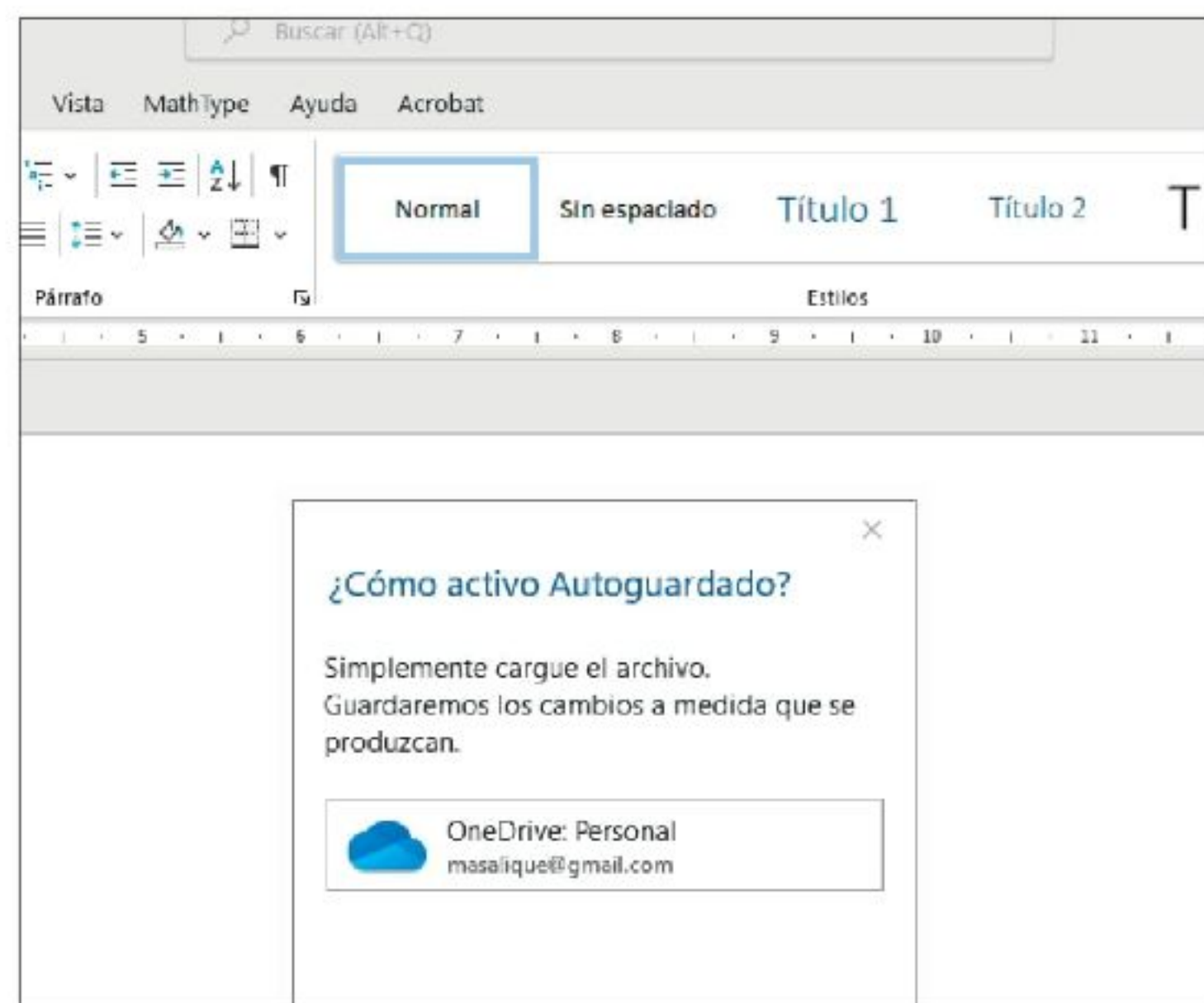


Figura 2.20. Autoguardado.

La mejor forma de elegir con cual de estos sistemas de almacenamiento trabajar es hacer un análisis comparativo. Lo proponemos como actividad.

► ACTIVIDAD PROPUESTA 2.6

Almacenamiento en la nube

Haga un análisis comparativo de Dropbox, Google Drive y OneDrive; no se olvide de que también funcionan con Android.

- ¿Cuál es el más adecuado para usted?
- ¿Por qué?

ACTIVIDADES FINALES

DE COMPROBACIÓN

2.1. Google Chrome y Microsoft Edge son buscadores:

- a. No, son sistemas operativos.
- b. No, son navegadores.
- c. Sí.
- d. Claro, no hay diferencia entre buscador y navegador.

2.2. Los operadores de búsqueda:

- a. Se utilizan en las actualizaciones.
- b. Los eliminan los antivirus.
- c. Son programas.
- d. Son símbolos y comandos que permiten afinar las búsquedas.

2.3. Seleccionar información relevante que ya está publicada en internet, filtrarla, organizarla, añadir un valor adicional y difundirla a nuestra comunidad:

- a. Es una pérdida de tiempo, la información ya está disponible.
- b. Se denomina curación de contenidos.
- c. Se realiza antes de ejecutar los programas.
- d. Se realiza principalmente por motivos de seguridad.

2.4. Exceso o sobrecarga de información, que impide profundizar en los temas que se abordan:

- a. Esto no sucede nunca.
- b. No es posible que ocurra, hay filtros.
- c. Solo les ocurre a los profesionales.
- d. Infoxicación.

2.5. Fuentes veraces y para comprobar la veracidad de la información:

- a. Expertos en la materia.
- b. Buscadores académicos.
- c. Legislación.
- d. Las tres respuestas anteriores son correctas.

2.6. Es fundamental comprobar la fecha de las informaciones:

- a. Sea cual sea la fecha, si la información es veraz, vale.
- b. No tiene importancia.
- c. Si no se hace, se puede obtener información inútil.
- d. No es posible hacerlo.

**2.7. ¿Le causó la noticia una reacción emocional muy grande?**

- a. Es falsa.
- b. Desconfíe. Las noticias inventadas se hacen para causar grandes sorpresas o rechazo.
- c. Siempre es verdad, a pesar de todo.
- d. Esto solo sucede con la prensa en papel.

2.8. Creative Commons:

- a. Programa de tratamiento de textos.
- b. Red de datos.
- c. Programa de creación de contenidos.
- d. Tipo de licencia para gestionar derechos de autor.

2.9. Es recomendable almacenar cierto tipo de información en la nube:

- a. Sí, la gestionan y cuidan profesionales.
- b. No, da acceso a terceros a nuestra información.
- c. No, es indiscreto.
- d. Carece de utilidad.

2.10. Los contenidos digitales abiertos:

- a. Se caracterizan por la integración de conjuntos de información multimodal, que pueden ser modificados y utilizados por los usuarios.
- b. Son los programas de la televisión en abierto.
- c. Todos los contenidos digitales son abiertos.
- d. Son los que publican los no profesionales.

2.11. El uso de fuentes oficiales:

- a. Es muy complicado.
- b. No es necesario nunca.
- c. No es recomendable.
- d. Es recomendable para tener información veraz.

2.12. Alertas de Google:

- a. Herramienta sencilla de curación de contenidos.
- b. Fuente RSS.
- c. Agregador de contenidos.
- d. Carpeta de archivos.

2.13. La red social de las preguntas:

- a. Asktwee.
- b. Rexpondex.
- c. PreguntaTodo.
- d. Quora.

2.14. Google dispone de:

- a. Menús de búsquedas avanzadas.
- b. Buscadores especializados.
- c. Algoritmos que entienden el uso de operadores de búsqueda.
- d. Las tres respuestas anteriores son correctas.

2.15. Una búsqueda avanzada es:

- a. Cualquier búsqueda, todas son avanzadas.
- b. La que nos permite combinar términos y operadores que nos dan resultados más próximos a lo que buscamos.
- c. Buscar en la nube.
- d. Una pérdida de tiempo.

DE APLICACIÓN

2.16. ¿Recuerda la palabra infoxicación? Busque el término en Google, después en Google Ngrams y luego en Google Académico, y compare los resultados obtenidos.

2.17. Haga una búsqueda en Google utilizando operadores; por ejemplo, empiece con ordenadores, siga con ordenadores* y con ordenadores and juegos. Plantee su propio ejemplo de búsqueda, para practicar.

2.18. Busque un foro sobre un tema que sea de su interés y vea que información ofrece. ¿Le resulta útil?

2.19. ¿Conoce LinkedIn? Vea qué información se comparte en esta red. ¿Es de su interés?

2.20. Twitter, Facebook, YouTube. ¿Hay información en ellas que le sea útil?

2.21. Trabaje con Talkwalker y vea la información que se comparte.

2.22. Trabaje con Feedly y vea si le resulta útil.

2.23. Trabaje con Content Gems y vea si le resulta útil.

2.24. Busque información sobre Menéame. ¿Qué le parece?

2.25. Trabaje con Storyfy. ¿Qué le parece?

2.26. ¿Conoce algún buscador académico? Busque información sobre Web of Science.

2.27. Vaya a la página de The Free Library. ¿Considera útiles sus contenidos?

2.28. ¿Ha visto últimamente alguna noticia que le resulte sospechosa? Siga las instrucciones de la BBC que se indican en el Apartado 2.2.1.

2.29. ¿Conoce Wikiloc? Si le gustan las excursiones, es un sitio curioso.

2.30. Haga, con un amigo, un ejercicio de trabajo colaborativo en red usando Google Drive.



Comunicación

La red es una maravillosa fuente de información y un gran medio para compartirla pero, para poder utilizarla, hay que saber dos cosas fundamentales: las herramientas de las que se dispone y la forma de usarlas, así como los riesgos en los que se incurre al hacerlo.

En esta unidad tratamos las herramientas, su uso y utilidad, y la finalidad que persiguen y, a continuación, comentamos unas normas de conducta que permitan esquivar los riesgos implícitos a la navegación por internet, haciendo especial mención a dos desagradables situaciones: el ciberacoso y la suplantación de identidad.

Contenido

- 3.1. Compartir información
- 3.2. Comunicación mediante tecnologías digitales
- 3.3. Normas de conducta y peligros

3.1. Compartir información

Todas las personas debemos ser conscientes de que es posible encontrar información en la red porque alguien, personas o instituciones, la ha elaborado y subido para hacerla pública, con las condiciones pertinentes en cada caso.



Figura 3.1. Subir información.

RECUERDA

- Subir información (o cargar), upload.
- Bajar información (o descargar), download.

Hay muchas formas de compartir información en internet: las entidades públicas o privadas suelen utilizar sus propios sitios web para poner a disposición del público información que consideran relevante para sus fines, sea publicidad o información acerca de las modificaciones del Código de la Circulación.

Realmente es compartir información, pero en una sola dirección, ya que el objetivo es informar a la persona que visita el sitio, aunque en algunos casos se pueden plantear preguntas o dudas mediante un chat. Estos contenidos no tienen por objeto ser comentados, solo informar.

Lo mismo sucede cuando es un particular el que abre su web al público: comparte información con el único objetivo de informar.

Pero si queremos compartir información para hacer partícipes a los demás y que puedan contribuir al enriquecimiento de esta, mediante sus aportaciones, hay otras formas de hacerlo. Sigamos leyendo.

3.1.1. Foros, wikis, etcétera

En este apartado vamos a comentar distintas maneras de compartir información: foros, blogs, wikis y comunidades virtuales, empezando por definir cada una de ellas.

Un **foro** es una aplicación web que permite a sus participantes mantener discusiones y aportar opiniones e información en un espacio virtual categorizado en temas de discusión o «hilos» que pueden abrir las propias personas usuarias, y a los que el resto de los usuarios pueden responder con sus opiniones y aportaciones¹.

Un **blog**, también conocido en español como bitácora digital, es un sitio web en el que uno o varios autores publican sus textos, que quedan ordenados en orden cronológico inverso, de tal forma que lo último que se ha publicado, lo más reciente, es lo que aparece en primer lugar en la pantalla².

Un **wiki** o una wiki (del hawaiano wiki, rápido) es un sitio web cuyas páginas pueden ser fácilmente editadas por múltiples personas a través de una interfaz web. Las personas usuarias pueden crear, borrar o modificar el texto de cada página, que es accesible a todos ellos³.

Una **comunidad virtual** es un grupo de gente con objetivos comunes que usan una misma forma de comunicación para interactuar entre ellos en un entorno online⁴.

Todas permiten compartir información, pero cada una tiene sus características.

Los **foros** permiten la participación de los usuarios, esa es su principal función, pero hay distintas modalidades, pues los hay de pago y gratis y en, general, hay que registrarse. Existen foros sobre casi todo y también hay foros sobre foros (no es un trabalenguas).

En las siguientes figuras se muestran distintos foros. Veámoslas antes de ir a los comentarios.



Figura 3.2. Foros.

¹ https://moodle2021-22.ua.es/moodle/pluginfile.php/10774/mod_resource/content/11/tema/index.html

² https://moodle2021-22.ua.es/moodle/pluginfile.php/10774/mod_resource/content/11/tema/index.html

³ https://moodle2021-22.ua.es/moodle/pluginfile.php/10774/mod_resource/content/11/tema/index.html

⁴ <https://www.questionpro.com/blog/es/comunidades-virtuales-de-investigacion>



Figura 3.3. Foros.



Figura 3.4. Foros.

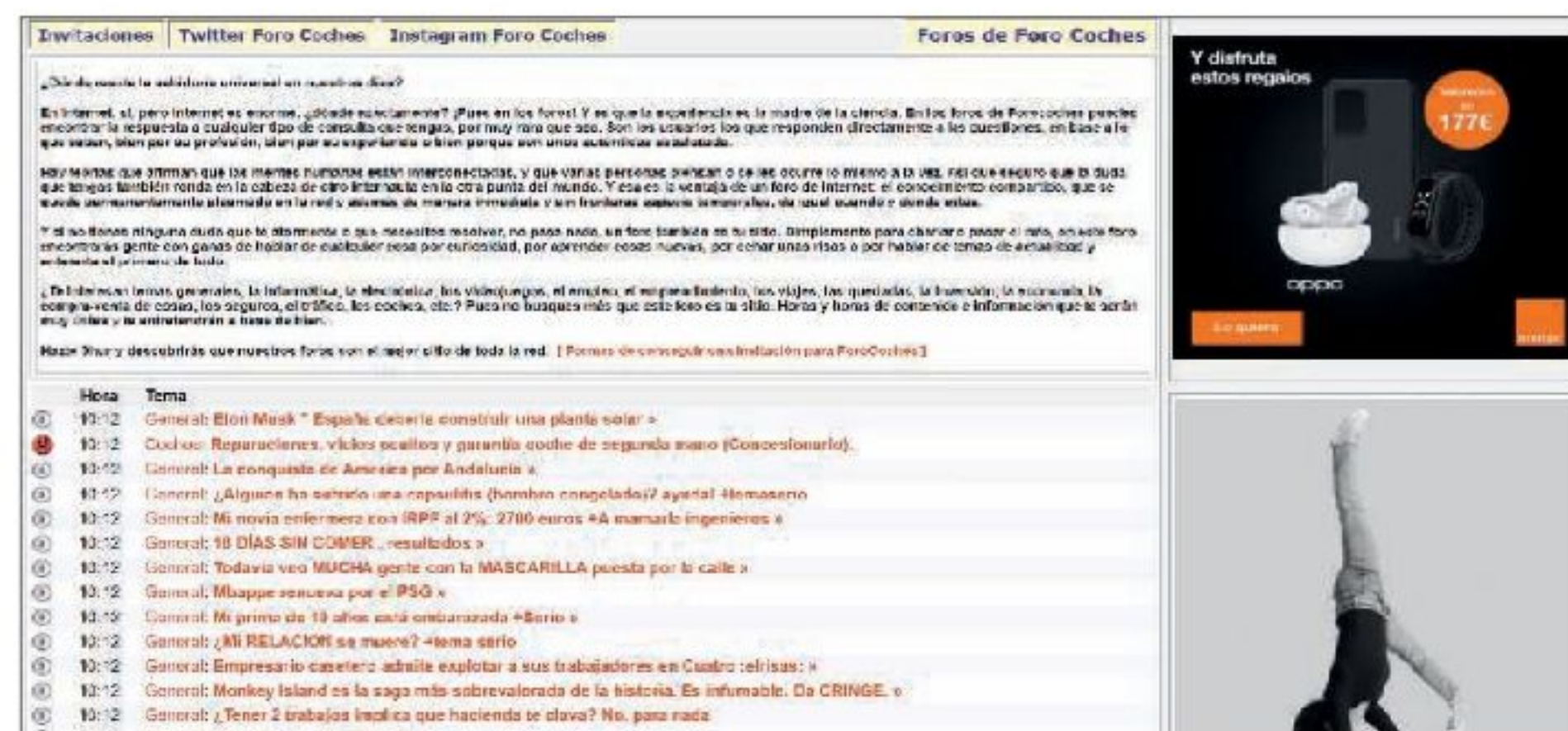


Figura 3.5. Foros.

En la Figura 3.2 mostramos un foro de foros cuyo objetivo es, entre otros, el encuentro intergeneracional. En la Figura 3.3 mostramos un buscador de foros (en realidad es un metabuscador) desde el que es posible ir a distintos foros sobre materias de lo más variado. En la Figura 3.4 se indican unas normas básicas sobre el uso de foros y la forma de montar un foro, y en la 3.5 mostramos la página de entrada a Forocoches, en el que, para entrar, hay que conseguir una invitación.

Lo anterior es solo una muestra de la inmensa cantidad de foros que hay en la red y sirve de guía al lector interesado; basta con buscar un tema y seguro que hay foros sobre él.

En algunos foros hay un moderador, pues es sorprendente la forma en la que determinadas personas se expresan, mostrando auténtica inquina, por no decir odio, hacia los participantes que no estén de acuerdo con sus opiniones; de ahí la necesidad del moderador.

Un foro debe ser un sitio donde compartir opiniones y discutirlos, si procede, pero nunca debe servir para descargar la ira recurriendo al insulto y a la descalificación personal; entre otras razones, porque todo ordenador es identificable mediante su dirección IP y porque existe, y es punible, el delito de odio.

Es evidente que dentro de los foros puede haber comunidades, y de hecho las hay, cuando se constituye un grupo con un interés común que utiliza el foro para tratar el tema en cuestión; por ejemplo, dentro de Forocoches podría haber una comunidad cuyo tema de interés sean los vehículos históricos.

Aprovechar las ventajas de la red para relacionarse con personas que tienen intereses comunes puede ser muy provechoso; aprovechar un (ficticio) anonimato para dar salida a otros sentimientos, tiene un nombre muy feo.

Hablemos ahora de **blogs**. La finalidad del blog es compartir información entre el autor, o autores, y el público al que, en algunos casos, se le permite participar mediante preguntas. Es menos abierto que el foro y su finalidad es distinta.

Basta hacer una búsqueda sencilla con la palabra «blog» para encontrar una gran cantidad de ejemplos. También hay blogs sobre casi todo. Veamos las figuras siguientes.



Figura 3.6. Blogs.



Figura 3.7. Blogs.

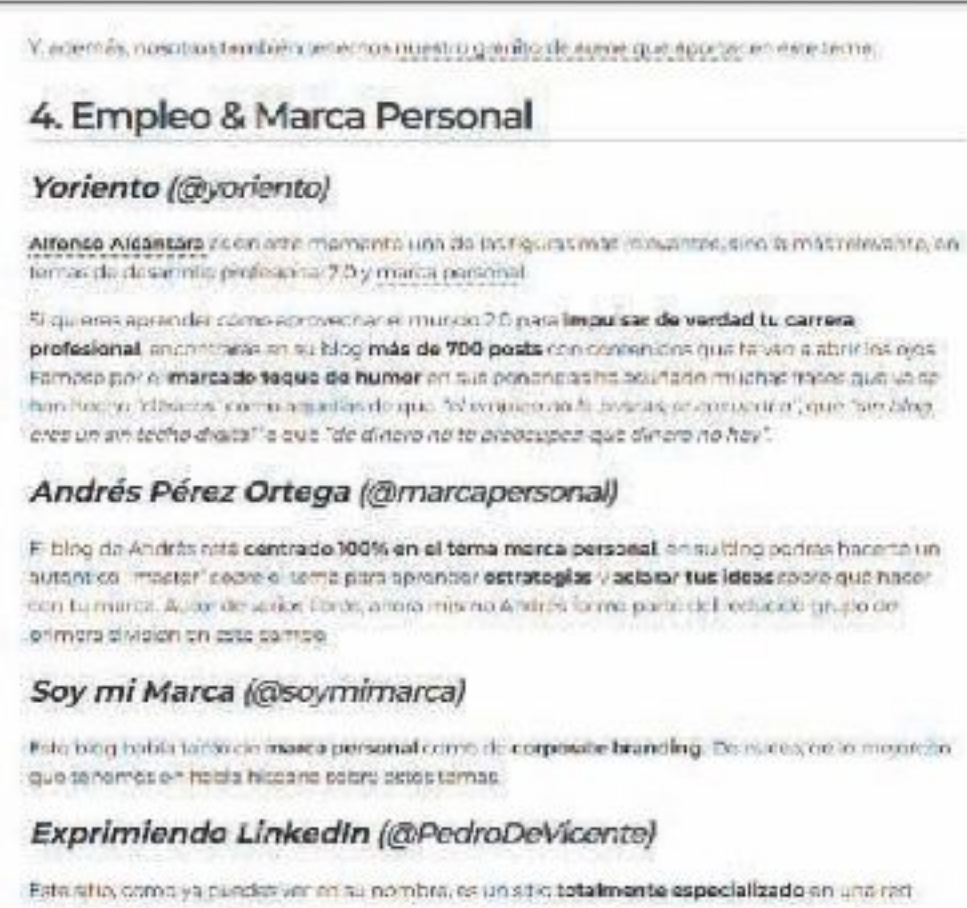


Figura 3.8. Blogs.

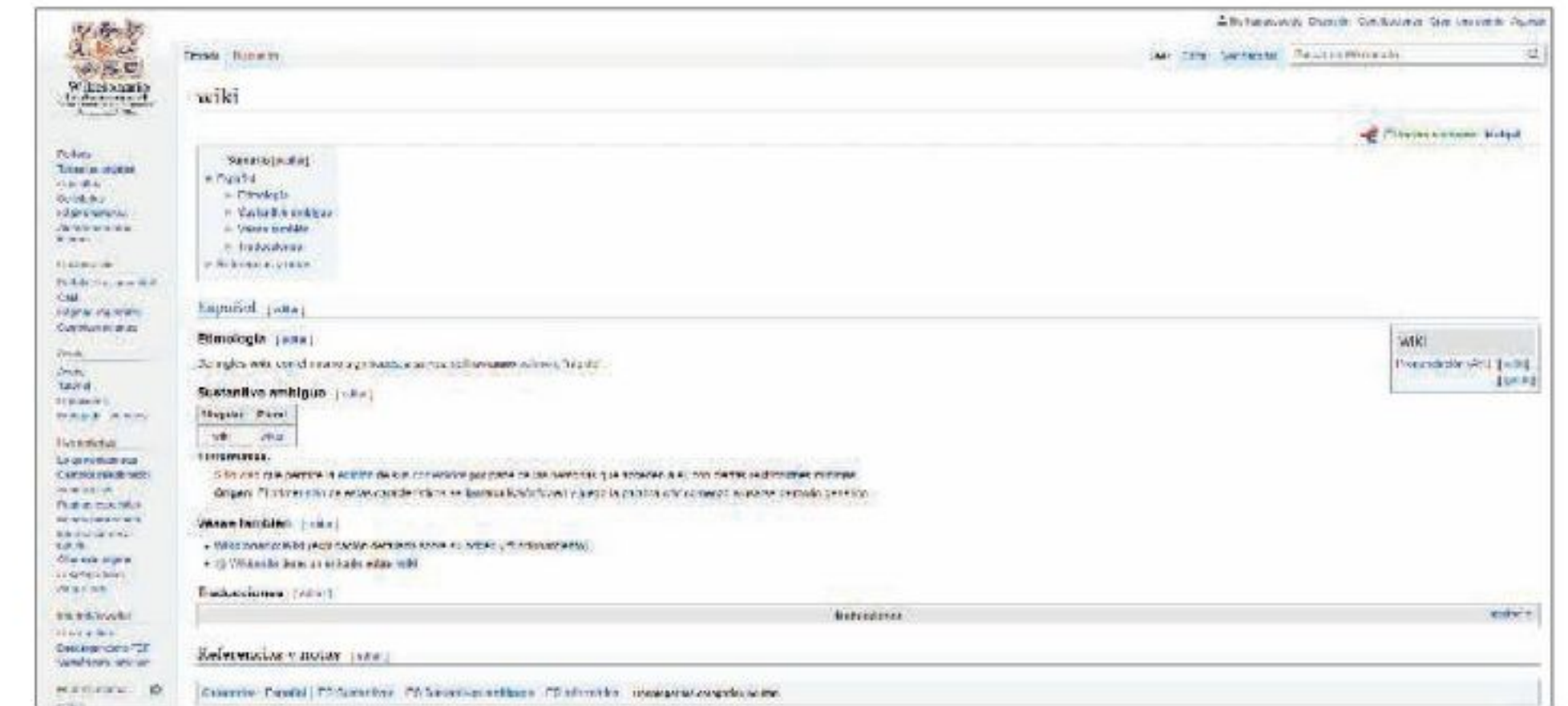


Figura 3.9. Wikis.



Figura 3.10. Wikis.

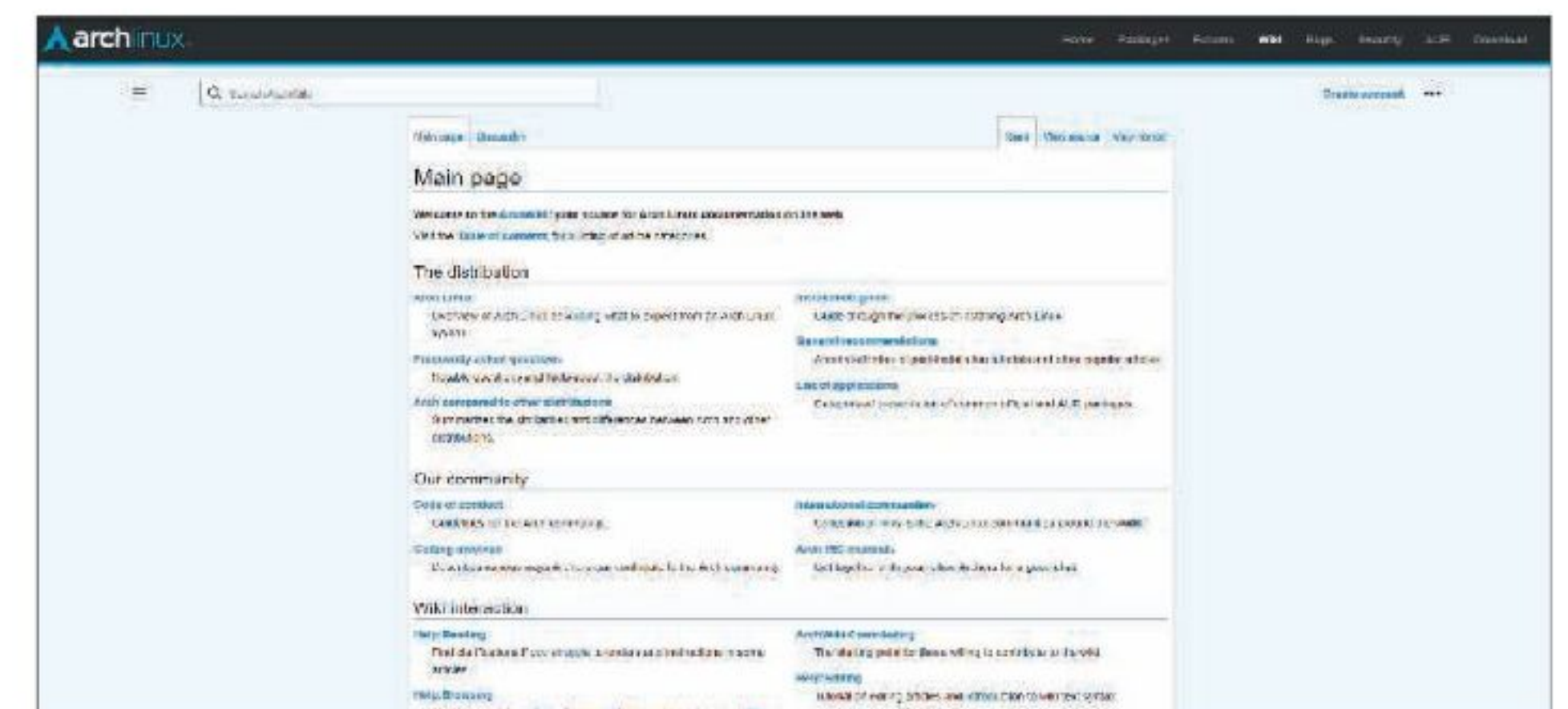


Figura 3.11. Wikis.

En la Figura 3.6 mostramos la página de entrada a un blog y en las Figuras 3.7 y 3.8 vemos distintos blogs recomendados en la página citada; como podemos ver, hay para todos los gustos. Recomendamos visitar el sitio y entrar en aquellos blogs cuyo tema consideremos más interesante. Es una buena manera de familiarizarnos con esta forma de compartir información.

Ahora les toca el turno a los **wikis**. Recordemos lo dicho en la Unidad 2, Apartado 2.2.2, respecto de Wikipedia, probablemente el wiki más conocido, pero hay muchos más.

Al igual que en los casos anteriores hay wikis sobre casi todo, algunos tristemente famosos como WikiLeaks. Al igual que con los foros y los blogs, hemos hecho una búsqueda en la red y en las figuras siguientes mostramos un wiki diccionario, un wiki sobre la Guerra de las Galaxias y un wiki sobre Linux; hay de todo.

También dentro de los wikis puede haber comunidades: en el de la Guerra de la Galaxias pueden agruparse los fans de Mandalorian y los de Boba Fett.

Al utilizar los foros, los blogs y los wikis como fuentes de información hay que tener en cuenta que cualquiera puede montarlos, lo que pone al alcance del internauta una gran cantidad de información, pero no toda la información está contrastada y, tristemente, no todo el que habla de algo domina el tema. Hay que ser muy prudente y buscar la misma información en fuentes distintas, pero una vez encontrada, a una fuente fiable le podemos sacar un gran partido.

Para participar en cualquiera de estas modalidades de compartir información hemos de seguir las instrucciones del sitio y recordemos que la corrección, la prudencia y el respeto a los demás deben ser la norma.

¿Queremos montar un blog, un foro o un wiki? Veamos cómo hacerlo.

Para crear un wiki podemos seguir las instrucciones de Microsoft⁵; las instrucciones para crear un blog se pueden encontrar en unavidaonline.com⁶; y respecto a los foros, se pueden encontrar las instrucciones para hacerlo en foroactivo.com⁷.

Un último comentario sobre las comunidades: estas pueden existir dentro de los foros, los blogs, las redes sociales, los wikis, etc., pero también se pueden crear con una finalidad concreta, por ejemplo, un estudio de marca; el lector interesado puede ampliar la información sobre comunidades virtuales en la referencia indicada en la definición.

3.1.2. Uso básico de redes sociales como medio de comunicación

Constantemente estamos oyendo hablar de las redes sociales, lo que demuestra que es un tema de indudable interés en nuestro mundo y probablemente muchos de los lectores son usuarios habituales de ellas, pero para conocer un tema conviene empezar por definirlo.

¿Qué es una red social?

Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo⁸.

⁵ <https://support.microsoft.com/es-es/office/crear-y-editar-un-wiki-dc64f9c2-d1a2-44b5-ac59-b9d535551a32>

⁶ <https://unavidaonline.com/como-crear-un-blog>

⁷ <https://www.foroactivo.com>

⁸ <https://dpej.rae.es/lema/red-social>

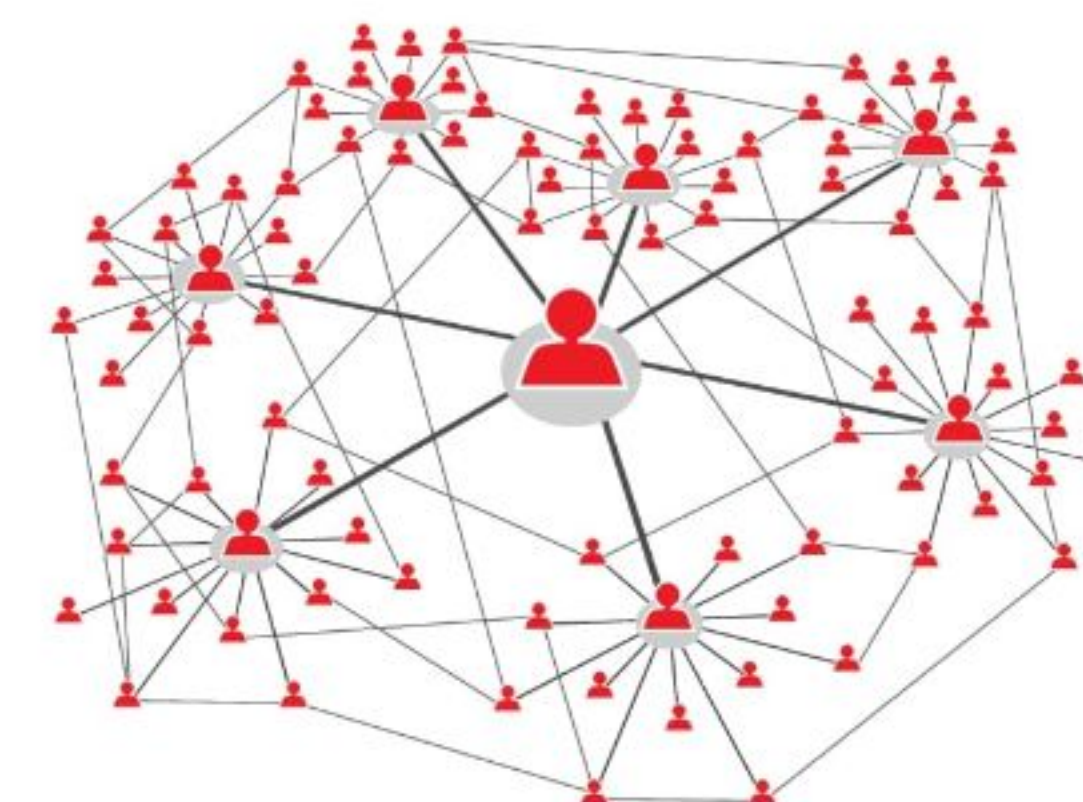


Figura 3.12. Red social.

Como vemos, es una definición general que plantea los aspectos más importantes de las redes sociales, definiendo su finalidad fundamental: la comunicación entre usuarios.

Antes de dar unos consejos básicos (y en muchos casos elementales) sobre el uso de las redes, hagamos un repaso de las más conocidas.

En la Figura 3.13 mostramos un gráfico con las más usadas según la fuente elegida⁹, que recomendamos al lector si quiere profundizar en el conocimiento de las citadas redes.

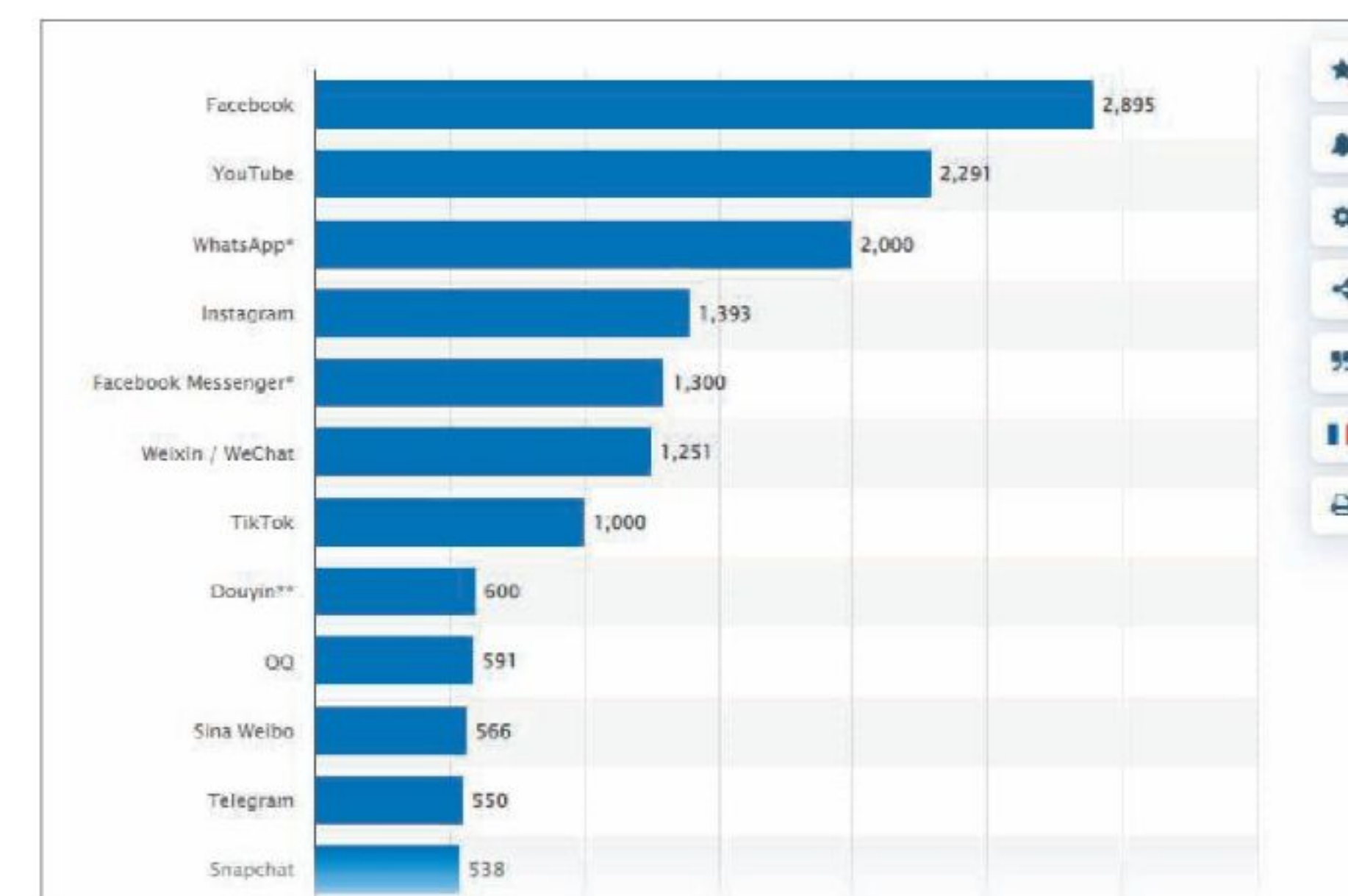


Figura 3.13. Redes sociales.

⁹ <https://netbulbsocialmedia.com/noticias/redes-sociales-mas-importantes-2022>



Como no todas las fuentes coinciden, podemos ver que Twitter no figura en los primeros lugares, lo que sí sucede en otras clasificaciones; en cualquier caso, lo importante es que el numerito a la derecha de la barra indica el número de usuarios: casi 3000 millones de personas utilizan Facebook.

Con estos números, y teniendo en cuenta el uso que podemos hacer de la información compartida, es importante saber comportarse en las redes, sea cual sea el uso que hagamos de ellas.

Algunas normas de comportamiento en las redes sociales son:

- *Pide permiso antes de subir una foto o un vídeo. Pregunta a las personas aludidas qué información puedes publicar de ellas y asegúrate de que no les importa.*
- *Solicita autorización antes de etiquetar las fotos subidas por otras personas. Puede ocurrir que haya alguien que no quiera estar etiquetado en una foto, aunque se haya publicado.*
- *Piénsatelo bien antes de publicar algo. No subas aquello que pueda perjudicarte a ti o a otras personas. Podrás eliminarlo posteriormente, pero las copias que ya circulen por la red resultarán imposibles de borrar.*
- *Usa etiquetas positivas. No utilices etiquetas que resulten ofensivas para otras personas.*
- *Ayuda a crear un ambiente agradable. En tus intervenciones sé amable, educado y respetuoso con los demás.*
- *Valora cuando utilizar mensajes privados o públicos. Al enviar mensajes a los demás hazlo con respeto sobre todo cuando terceras personas pueden leerlos. Si necesitas aclarar algo con una persona puede resultar más apropiado utilizar los mensajes privados.*
- *Escribe usando mayúsculas y minúsculas. En la red cuando alguien escribe en mayúsculas se interpreta como si hablase a gritos y eso puede molestar a algunas personas.*
- *Usa los emoticones. A veces resulta interesante usarlos para expresarnos mejor y evitar malentendidos :-)*
- *Críticas y comentarios. Modera tus críticas hacia otras personas. Recuerda que si te excedes con otros usuarios/as puedes llegar a vulnerar sus derechos y ser penado por la Ley. Tu libertad de expresión termina donde comienzan los derechos de los demás. Si atentas contra el honor o intimidad de una persona puedes cometer un delito.*
- *Respetar la privacidad de otras personas. No difundas en público o en otros grupos aquella información que un usuario comparte contigo o con un grupo en concreto. Cuida la privacidad de las personas como quisieras que cuidasen la tuya.*



- *No participes en aquello que no te interese o no lo veas claro. No hay problema con ignorar solicitudes de amistad de personas que no conoces. Tampoco con declinar invitaciones a ciertos eventos o grupos. No reacciones de forma violenta cuando alguien no te acepta como amigo/a.*
- *Conserva una actitud pacífica. Si algo o alguien te molesta en la red social no actúes de forma agresiva. Es posible que busquen la provocación o el engaño y si reaccionas mal habrán conseguido su propósito. A veces puede tratarse de errores o acciones no intencionadas.*
- *Utiliza los sistemas de denuncia si fuera necesario. Las redes sociales disponen de formularios para denunciar el comportamiento inadecuado de un usuario. No utilices estos sistemas a la ligera o de manera injustificada para no generar desconfianza o enfado.*
- *Comprueba tu identidad digital. Presta atención a cómo te presentas a los demás en la red social y a cómo te perciben el resto de los usuarios.*
- *Comunica tus criterios de privacidad a tus amistades si fuese necesario. En algunas ocasiones conviene recordar esos criterios de forma educada a algunos de tus contactos. Por ejemplo, en relación con la reutilización de fotos de tus álbumes privados, cuando te etiqueten sin tu permiso o publiquen tus datos personales en páginas vistas por otras personas que no conoces.*
- *Sé responsable. Recuerda que las redes sociales no son un juego. Eres responsable de todo lo que haces en ellas.*
- *Consulta tus dudas o problemas. Si tienes temores, problemas o dudas en relación con tu experiencia con las redes sociales, dirígete a tus padres, profesores o adultos de confianza para tratar de solucionarlos. Ellos podrán ayudarte.*

La mayoría de estas normas se han extraído del espacio Netiquetate¹⁰.

Como podemos apreciar, las instrucciones anteriores van dirigidas a jóvenes, pero son de aplicación general y sirven para que los adultos seamos conscientes de los peligros de las redes sociales para la juventud.

El uso de las redes sociales como fuente de información y medio de comunicación admite muchas posibilidades, desde compartir noticias a mantener el contacto con amigos que está lejos de donde vivimos, pero en todos los casos hay que respetar los principios básicos que hemos comentado repetidamente: corrección, respeto, prudencia y veracidad.

¹⁰ https://www3.gobiernodecanarias.org/medusa/contenidosdigitales/FormacionTIC/cdtic2014/04cd/33_netiqueta_de_las_redes_sociales.html

**► ACTIVIDAD PROPUESTA 3.1****Foros, blogs, wikis y comunidades**

Elija un tema cualquiera que sea de su interés:

- Realice una búsqueda en un foro sobre él.
- Realice una búsqueda en un blog sobre él.
- Realice una búsqueda en un wiki sobre él.
- Realice una búsqueda en una comunidad sobre él.

¿Qué le parece el tratamiento del tema elegido que hacen en cada sitio?

► ACTIVIDAD PROPUESTA 3.2**Redes sociales**

Para conocer un poco mejor el mundillo de las redes, le proponemos dos actividades:

- Busque información sobre las redes que no conoce. ¿Algo interesante?
- Hable con usuarios de redes ¿Qué uso hacen? ¿Cómo se comportan?

3.2. Comunicación mediante tecnologías digitales

En el apartado anterior, titulado Compartir información, hemos comentado distintas maneras de poner información a disposición de los demás, pero, aunque es posible la comunicación entre personas o grupos en el seno de un blog o de un foro, por ejemplo, no es el mejor método para ello.

Hay otras formas de mantener una reunión o de comunicarnos con nuestra hija pequeña que está en China.

Hace tiempo, todas las reuniones eran presenciales o, como mucho, por teléfono, pero, cuando lo normal era la presencialidad, la conversación telefónica resultaba muy fría.

A continuación, aparecieron aquellos complicados, y caros, equipos de videoconferencia: podíamos ver a la persona con la que estábamos hablando, al mismo tiempo que evitábamos pérdidas de tiempo y de dinero, ya que ya no había que hacer costosos y largos viajes. El autor trabajaba por aquel entonces en una empresa multinacional en la que eran habituales las reuniones con personas que estaban en dos o tres países distintos, y nos enamoramos de la videoconferencia.

Pero el avance de las tecnologías de la información, tanto en los ordenadores como en los móviles, y la mayor facilidad de uso de equipos y dispositivos han dado lugar

a que, hoy en día, tengamos a nuestra disposición una serie de medios de comunicación con una muy buena relación calidad precio que nos permiten comunicarnos de forma fiable y ágil.

Nos hemos acostumbrado al chat, a la llamada telefónica, a la videollamada o a la videoconferencia hasta el punto de que cada vez más trabajamos con personas a las que no conocemos personalmente.

No es que haya desaparecido la presencialidad, pero la agilidad que da el uso de las TIC ha hecho que la presencialidad se haya disminuido en aras de la facilidad de comunicación, de la rapidez y del ahorro en costes.

Para eso son las formas de comunicación que vamos a ver en este apartado.

3.2.1. Comunicación textual: chats, sistemas de mensajería, etcétera

La comunicación textual es la que se hace mediante letras, mediante distintos sistemas de escritura. Baste con esta definición por ahora, aunque al final del apartado haremos una reflexión sobre el lenguaje utilizado en estos medios de comunicación.

La RAE define chat como:

- *Intercambio de mensajes electrónicos a través de internet que permite establecer una conversación entre dos o más personas.*
- *Servicio que permite mantener conversaciones mediante chats¹¹.*

Como vemos, se refiere tanto al acto de charlar (que es lo que deberíamos decir en español) como al programa o aplicación que nos permite charlar.

Según algunas fuentes¹², los programas de chat más usados son los que figuran en la lista siguiente:

- Telegram.
- Hispachat.
- Casual Dating.
- Badoo.
- Tinder.
- Meetic.
- WhatsApp.

¹¹ <https://dle.rae.es/chat?m=form>

¹² <https://tecnologia10.top/mejores-aplicaciones-para-chatear-gratis/#comparativa>



Figura 3.14. Red social.

Como curiosidad, Casual Dating, Badoo, Tinder y Meetic tienen como finalidad conocer a otras personas, lo cual da una idea del uso creciente de las TIC en el terreno de las relaciones personales.

La mensajería más usada es WhatsApp, por eso la han puesto la última (cada uno tiene sus criterios), por ser la más conocida, aunque Telegram va ganando terreno.

Un comentario aparte merece Franz que, como podemos ver en la Figura 3.15, es una aplicación que integra diversos servicios de mensajería.

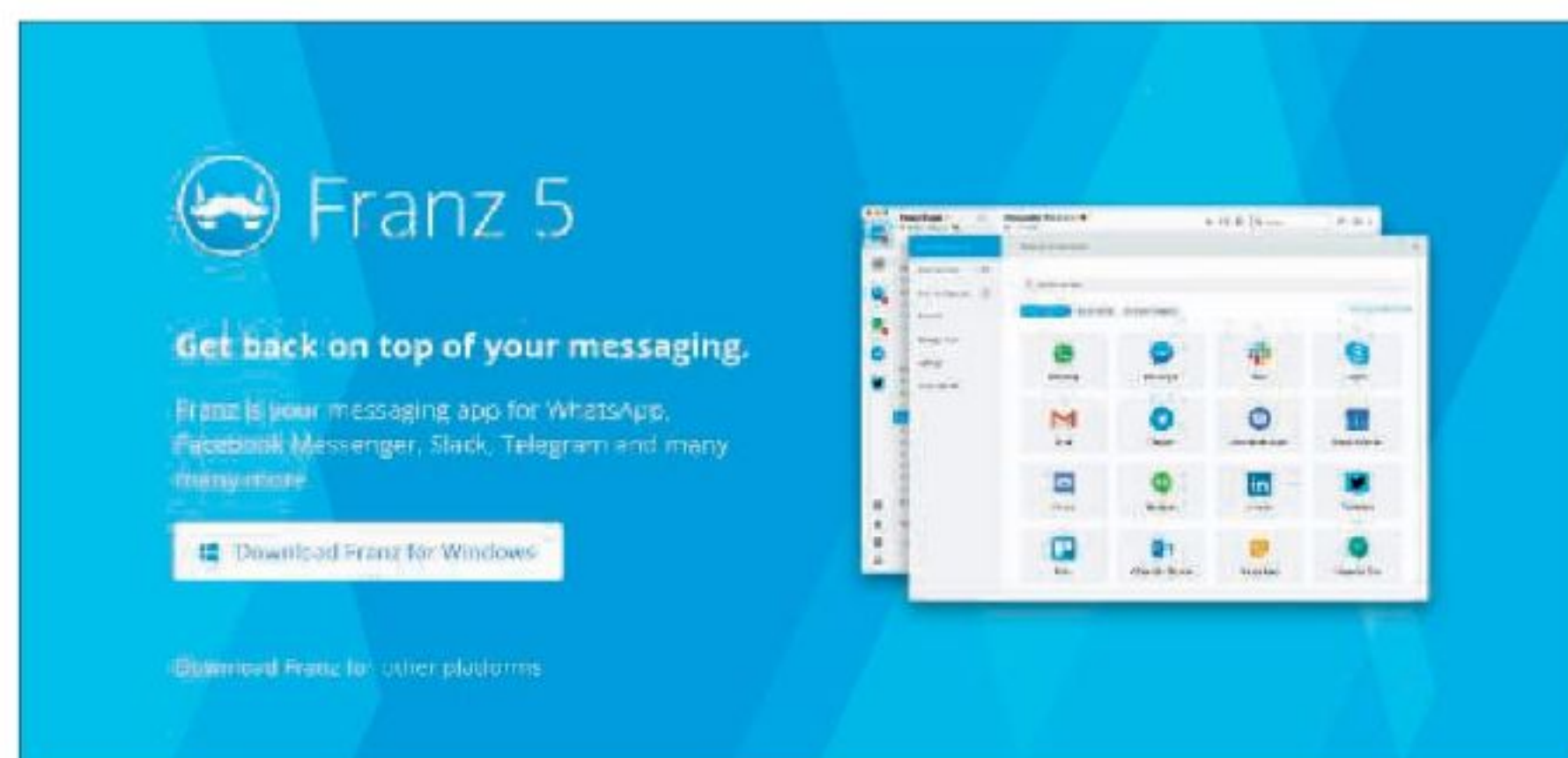


Figura 3.15. Franz.

Pero no solo hay aplicaciones específicas para chatear. Google incluye un chat entre sus servicios, como veremos, y además es habitual que los sitios web de muchas empresas y organizaciones tengan su propio chat para plantear preguntas y resolver dudas.

El chat es una herramienta instantánea de comunicación que se utiliza en ámbitos muy distintos.

Para entender un mejor el uso del chat, veamos lo que nos ofrece Google.

Google ofrece Google Chat, que se puede utilizar desde el correo (aparece en el menú de Gmail) o como aplicación independiente, y Messages; si nos centramos en el chat,

vemos que, al ofrecerlo en el menú de su programa de correo, todo parece indicar que se considera un medio más rápido e informal que el propio correo, y eso es realmente un chat.

¿Qué es Google Messages? Es una aplicación de mensajería.

Las aplicaciones de mensajería más utilizadas son las que figuran en la lista siguiente¹³. Como podemos ver, hay aplicaciones de mensajería como tal y alguna otra que suele ser más utilizada para videollamadas o videochat, como Skype, pero es que la mensajería puede ser por voz, escrita y con imagen; de hecho, una aplicación como WhatsApp incluye todos estos servicios y la RAE define mensajería como *sistema de emisión y recepción de mensajes a través de dispositivos electrónicos y digitales o de correo tradicional*¹⁴.

- WhatsApp.
- Telegram.
- Viber.
- Messenger.
- Snapchat.
- Hangouts.
- Line.
- Wire.
- Skype.

Como no queremos abrumar al lector con más iconos, dejaremos que sea él quien los busque e identifique.

Al hablar de mensajería hay que tener en cuenta que se hace un uso habitual de ella desde dispositivos móviles, como el teléfono o la tableta, lo que debemos considerar a la hora de elegir una aplicación u otra.

Sea cual sea el medio de comunicación utilizado y el tipo de mensaje, hablado o escrito, hay que hacerlo de forma correcta; respetar la ortografía y la sintaxis no está reñido con la rapidez y la concisión, y lo contrario es destrozar el idioma y empobrecer nuestra forma de expresarnos.

Se ha definido la comunicación textual como la que se hace mediante el lenguaje escrito, por lo que, además de los chats y la mensajería, hay que incluir en este grupo el correo electrónico y los medios antes citados, como blogs, foros, etc., sin olvidar las redes sociales, cada vez más utilizadas, incluso por algunos gobernantes, para

¹³ <https://oficina10.top/mejores-aplicaciones-de-mensajeria-instantanea>

¹⁴ <https://dle.rae.es/mensajer%C3%ADa?m=form>



comunicar noticias y opiniones de interés general; aunque el mundo de la comunicación digital está en continua evolución, hay que utilizar las herramientas de forma adecuada y correcta en el ambiente en el que nos movemos.

Como ejemplo de lo que no se debe hacer, veamos la siguiente noticia, publicada a finales de 2021: *Convoca a 900 empleados a la misma reunión por Zoom y los despide a todos: en apenas un minuto, el CEO de esta empresa echó al 15 % de su plantilla*¹⁵. Dejando aparte los aspectos legales, no parece la forma más adecuada de proceder.

3.2.2. Comunicación audiovisual: videoconferencia (Skype, Google Hangouts, etcétera)

Algunas de las aplicaciones de mensajería antes citadas incluyen servicios de videoconferencia o videochat. Pero antes de seguir comentando este modo de comunicación veamos cuáles son las más utilizadas¹⁶. Son datos de mayo de 2021, pero valen para nuestros fines:

- Skype.
- Hangouts.
- WhatsApp.
- FaceTime.
- Google Duo.
- Discord.
- Zoom.
- Jitsi Meet.
- Gruveo.
- Instagram.
- Snapchat.
- Facebook Messenger.

Recordemos algo evidente: para usar estas aplicaciones hay que disponer de video y audio; si el equipo o dispositivo no los tiene incorporados, hay que utilizar los periféricos correspondientes. Respecto al uso con Windows, hay que tener en cuenta que FaceTime es una aplicación de Apple que a principios de 2022 se abrió a dispositivos con Windows o Android, pero que debe iniciarse desde un dispositivo de Apple. Las demás aplicaciones se pueden utilizar en Windows, en Android o en ambos, pero dependiendo de si han sido diseñadas para un sistema operativo u otro pueden tener funcionalidades distintas. Conviene revisar su funcionamiento para elegir cuál vamos a utilizar.

¹⁵ <https://www.xataka.com/empresas-y-economia/convoca-a-900-empleados-a-reunion-zoom-despide-a-todos-apenas-minuto-ceo-esta-empresa-echo-al-15-su-plantilla>

¹⁶ <https://www.xataka.com/basics/aplicaciones-gratis-para-hacer-videollamadas-grupales>



Todas las aplicaciones citadas son gratuitas y, para un uso normal, sea personal o profesional, suelen ser suficientes.

En casi todas ellas hay que registrarse. El proceso es muy sencillo y puede ir asociado a otras cuentas, como en el caso de Hangouts, que es de Google.

Aunque todas tienen funcionalidades similares, hay diferencias en cuanto a la posibilidad de grabar o no las conferencias, el número de asistentes que pueden estar presentes simultáneamente, etc., por lo que conviene definir nuestras necesidades y buscar la que más se adecue a ellas.

Una vez que hemos comprobado que disponemos de los medios necesarios para su utilización, hay que instalar la aplicación y seguir las instrucciones para su uso. Como ya hemos dicho no todas requieren que el usuario se registre, otro factor a tener en cuenta.

Como siempre, seamos prudentes: aunque no se esté grabando la videoconferencia, nada impide que algún asistente la grabe, por ejemplo, con su móvil; no debemos decir nada que no queremos decir, aquello de que las palabras se las lleva el viento era antes de que fuera tan fácil grabarlas.

3.2.3. Herramientas colaborativas

Las herramientas colaborativas son programas para trabajar en equipo que incluyen funciones para gestionar proyectos y tienen como objetivo mejorar el proceso de trabajo. Para ello, contienen funciones específicas para planificar, organizar y analizar tareas¹⁷.

Con la inveterada manía de utilizar el inglés, si oímos hablar de groupware, ya sabemos que son herramientas (informáticas) para el trabajo en equipo.

Hablamos, una vez más, de compartir información, pero su finalidad es compartir tareas y facilitar el trabajo en equipo, aunque sus miembros estén en distintas ubicaciones. Es un objetivo distinto al de otras aplicaciones o herramientas que hemos visto, que también son válidas para el trabajo en equipo.

En la Tabla 3.1 mostramos el mejor software para trabajo en equipo (a criterio de la fuente elegida¹⁸). Leámosla con atención: en ella se indica el nombre del software, el fabricante, su fecha de publicación, donde están los centros de datos, con qué sistemas operativos trabajan y cuál es su peculiaridad más interesante, siempre a criterio de la fuente seleccionada.

¹⁷ <https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/comparativa-de-herramientas-de-gestion-de-proyectos>

¹⁸ <https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/comparativa-de-herramientas-de-gestion-de-proyectos>

Tabla 3.1. Groupware

Nombre	Fabricante	Año de publicación	Centro de datos	App	Peculiaridad
Asana	Asana	2011	EE. UU.	iOS, Android	Sistema de etiquetas para filtrar tareas.
Basecamp	Basecamp	2004	EE. UU.	Windows, macOS, iOS, Android	Consulta de estado automática.
Google Workspace	Google	2006	EE. UU.	iOS, Android	Suite ofimática.
Lifsize Cloud	Lifsize	2014	Para funciones basadas en la nube, en todo el mundo; si no, se usan las capacidades inhouse.	Windows, macOS, iOS, Android	Función de livestreaming.
Nextcloud	Nextcloud GmbH	2016	Alemania	Linux, macOS, Windows, Android, iOS	Dos versiones para escenarios diferentes.
Microsoft 365	Microsoft	2001	EE. UU.	Windows, macOS, iOS, Android	Suite ofimática.
Slack	Slack	2014	EE. UU.	Windows, iOS, Android, Windows Phone	Se pueden compartir fragmentos de código.
Spike	Chatflow Ltd.	2018	—	Windows, macOS, iOS, Android	Correos electrónicos en formato de chat.
Trello	Atlassian	2011	EE. UU.	iOS, Android	Presentación visual personalizable.
Wrike	Wrike	2007	EE. UU.	Windows, macOS, iOS, Android	Hilo de actividades y control de versiones.

Estas herramientas son, en general, para uso profesional, por lo que a aquella persona que no esté familiarizada con la gestión de equipos o de proyectos o que no haya participado en este tipo de tareas puede resultarle algo extraño; no debemos preocuparnos, vamos a comentar dos de ellas y veremos que no es nada raro, es algo muy evidente para trabajar en equipo, sobre todo en remoto.

Veamos las herramientas que ofrecen Google y Microsoft. Están entre las mejores y las más conocidas Google Workspace y Microsoft 365.

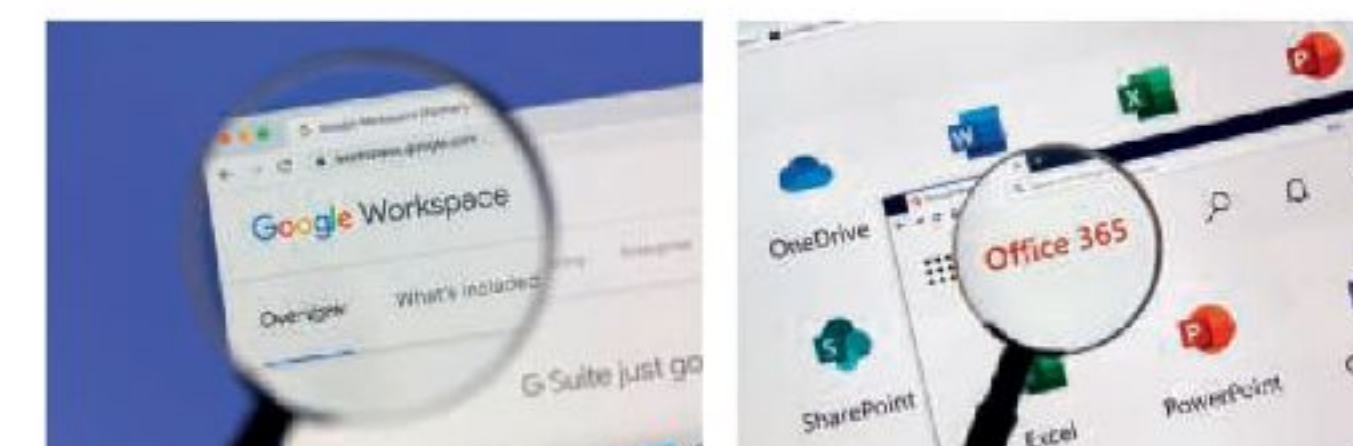


Figura 3.16. Herramientas colaborativas.

Primero, veremos lo que nos dice nuestra fuente:

Microsoft 365

Junto a Windows, Microsoft es sobre todo conocido por sus aplicaciones ofimáticas. Con Microsoft 365, la compañía llevó estos programas a la nube como aplicaciones web, allanando así el camino para convertir a Word y cía. en un groupware. Ya no hace falta comprar las licencias para utilizar la suite de oficina. Mediante una suscripción a Microsoft 365, pueden utilizarse todos sus programas en el navegador web.

Con Microsoft 365 (anteriormente conocido como Office 365) todas las aplicaciones ofimáticas de Microsoft pueden utilizarse en la nube. Las versiones más actuales de tus aplicaciones favoritas de Office como Word, Excel, PowerPoint y más desde cualquier dispositivo.

Como Microsoft 365 está constituido por varios programas diferentes, permite una gran variedad de formas de colaboración: gracias a Outlook (y Exchange) pueden compartirse los calendarios privados; Word, Excel y PowerPoint no solo permiten trabajar en los archivos a un usuario, sino a varios al mismo tiempo, lo que evita tener que enviar los archivos varias veces, y Teams es un software de colaboración que sobre todo facilita la comunicación entre los empleados.

Estas son las aplicaciones de colaboración que componen Microsoft 365:

- Word: procesador de textos en grupo.
- Excel: hojas de cálculo con varios usuarios.
- PowerPoint: preparar presentaciones en equipo.

- Outlook: compartir citas, calendario y tareas con otros miembros del equipo.
- Teams: comunicarse con los compañeros y colegas.
- Access: crear bases de datos junto con otros empleados.
- OneNote: compartir notas.
- OneDrive: almacenamiento en la nube de uso común.

Google Workspace

Si bien Google es sobre todo conocido por su buscador web, son millones los usuarios en todo el mundo que utilizan las otras ofertas de la empresa, algunas de las cuales se encuentran reunidas en Google Workspace. Se trata aquí de un paquete de aplicaciones para la oficina y varias herramientas de colaboración ya conocidas por la mayoría de los usuarios: Gmail, el servicio de correo gratuito de Google; Google Docs, para la creación de documentos, y Google Drive, el almacén en la nube del proveedor. Gran parte de estas aplicaciones ya está disponible de forma gratuita para los usuarios particulares, pero las empresas tienen a su disposición una versión ampliada con otros servicios: correo electrónico profesional, más espacio de almacenamiento y atención al cliente en todo momento.

Pensadas como software como servicio, las aplicaciones de groupware no se ejecutan en el equipo del usuario, sino que se proveen a través de una interfaz web. Al encontrarse todos los datos en la nube, los usuarios pueden acceder a ellos con total facilidad, compartir los calendarios, trabajar en los documentos en grupo y llevar a cabo reuniones online.

La colaboración en Google Workspace se lleva a cabo así:

- Comunicación: gracias al servicio de correo Gmail, a Google Chat (la aplicación para chatrooms) y Google Meet (la aplicación de videoconferencia), los miembros de los equipos pueden hablar entre ellos.
- Reparto de tareas: las tareas y las citas se gestionan con el calendario y las aplicaciones de notas.
- Creación: además de las conocidas aplicaciones para crear documentos (Docs, Hojas de cálculo, Formularios y Presentaciones), también puede trabajarse en páginas web y aplicaciones propias.
- Almacenamiento: además de Drive, Google ofrece con Vault un archivo para clientes Business.
- Administración: para otorgar a las empresas pleno control sobre Google Workspace, en la app de administración pueden gestionarse los usuarios y los derechos¹⁹.

¹⁹ <https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/comparativa-de-herramientas-de-gestion-de-proyectos>

Lo primero: ambas son de pago. Las suscripciones no son caras, pero hay que pagarlas.

La buena noticia es que algunas de las funciones de Google Workspace, como hemos indicado, están disponibles con una cuenta de Google que permite, entre otras cosas, compartir documentos.

Veámoslo: en las Figuras 3.17 y 3.18 mostramos la página de inicio de Google. A la derecha de las imágenes podemos ver algunos de los programas y aplicaciones que ofrece Google: Gmail, Meet, Chat, Drive, Documentos, Hangouts, etc.; para ver las demás, basta con deslizar la barra a la derecha del desplegable que se abre picando en los cuadritos que se ven arriba a la derecha. Todas estas herramientas son colaborativas.

El trabajo en equipo es aplicable a un grupo de estudiantes haciendo una tarea conjunta, a la ayuda que nos pueda prestar una amiga para redactar un escrito o a la gestión de proyectos complejos en una empresa; en muchos casos, las herramientas gratuitas serán suficientes, pero conforme aumenta la complejidad del proyecto puede ser recomendable recurrir a servicios profesionales, de pago.

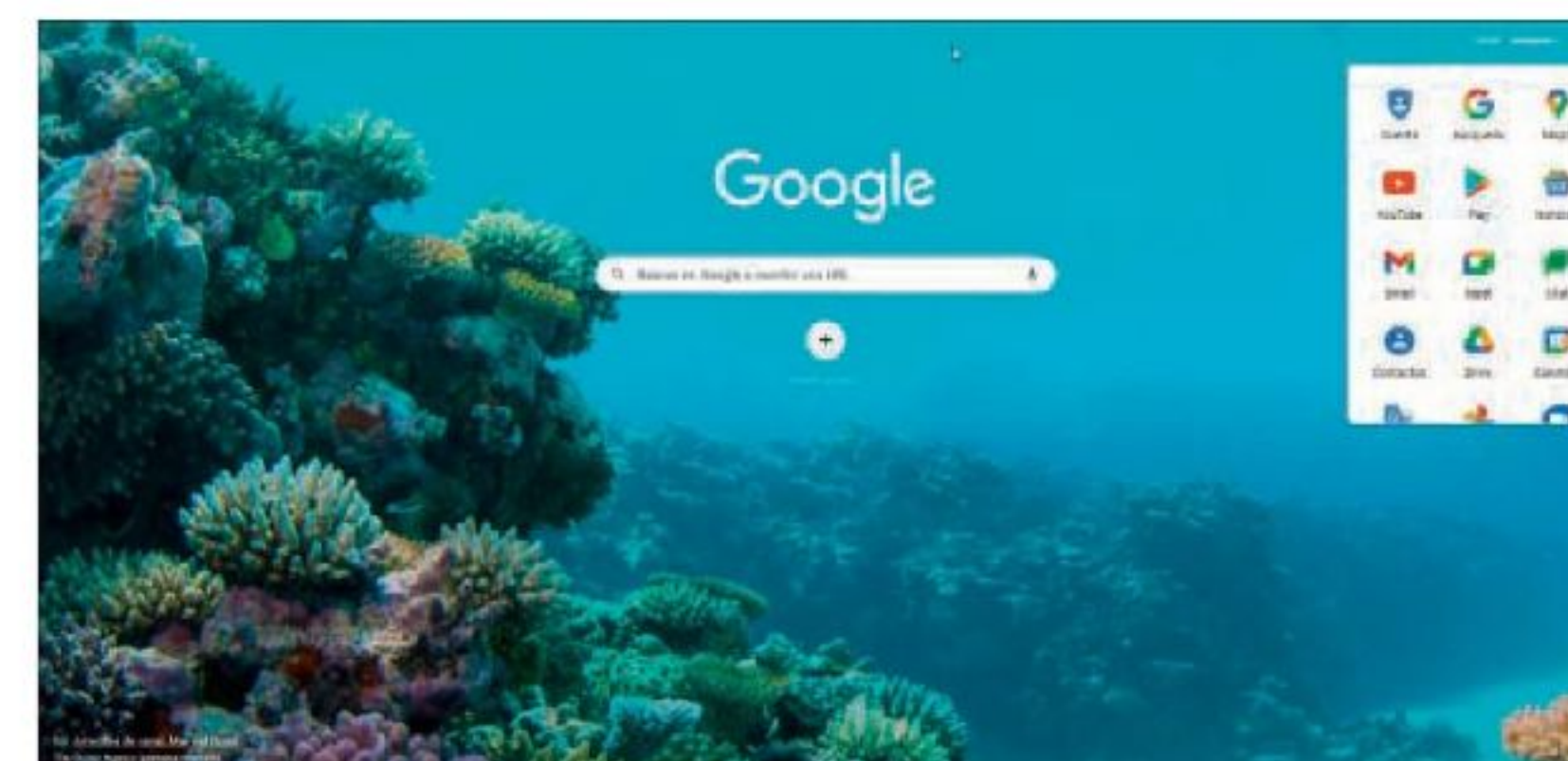


Figura 3.17. Herramientas colaborativas de Google.

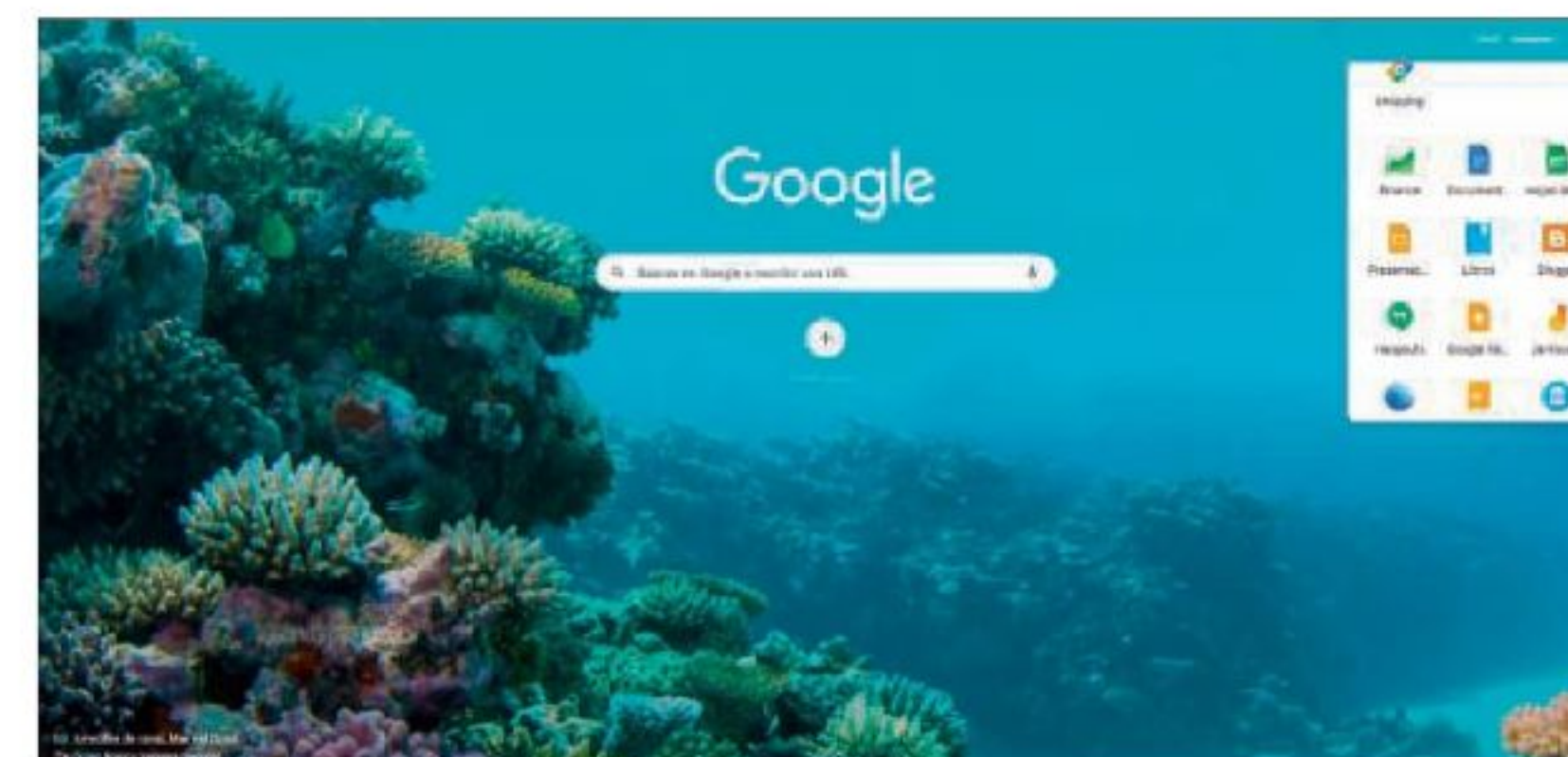


Figura 3.18. Herramientas colaborativas de Google.

Ya sabemos utilizar el correo, los chats y las videoconferencias y también sabemos usar Drive, pero nos puede surgir la duda sobre cómo compartir documentos. Veamos las Figuras 3.19 y 3.20. En el desplegable de la Figura 3.18 picamos en documentos y, después de identificarnos con nuestra cuenta de Google (Gmail), aparece lo que se muestra en la Figura 3.19. Abrimos un documento en blanco y arriba a la derecha hay un recuadro azul que indica *Compartir*. Si picamos en él, nos pide que pongamos un nombre al documento, podemos hacerlo o no, y después aparece el cuadro de diálogo de la Figura 3.20, en el que configuramos la forma de compartir. Lo mismo vale para las hojas de cálculo y demás aplicaciones de ofimática.

Podemos hacer muchas cosas con las herramientas de nuestra cuenta (gratuita) de Google.

Microsoft 365 es de pago y ofrece las aplicaciones indicadas en párrafos anteriores que se muestran en su web (Figura 3.21), donde se indican las diversas opciones del servicio.

La forma de compartir documentos es similar a la descrita para Google (debemos buscar el recuadro azul *Compartir*).

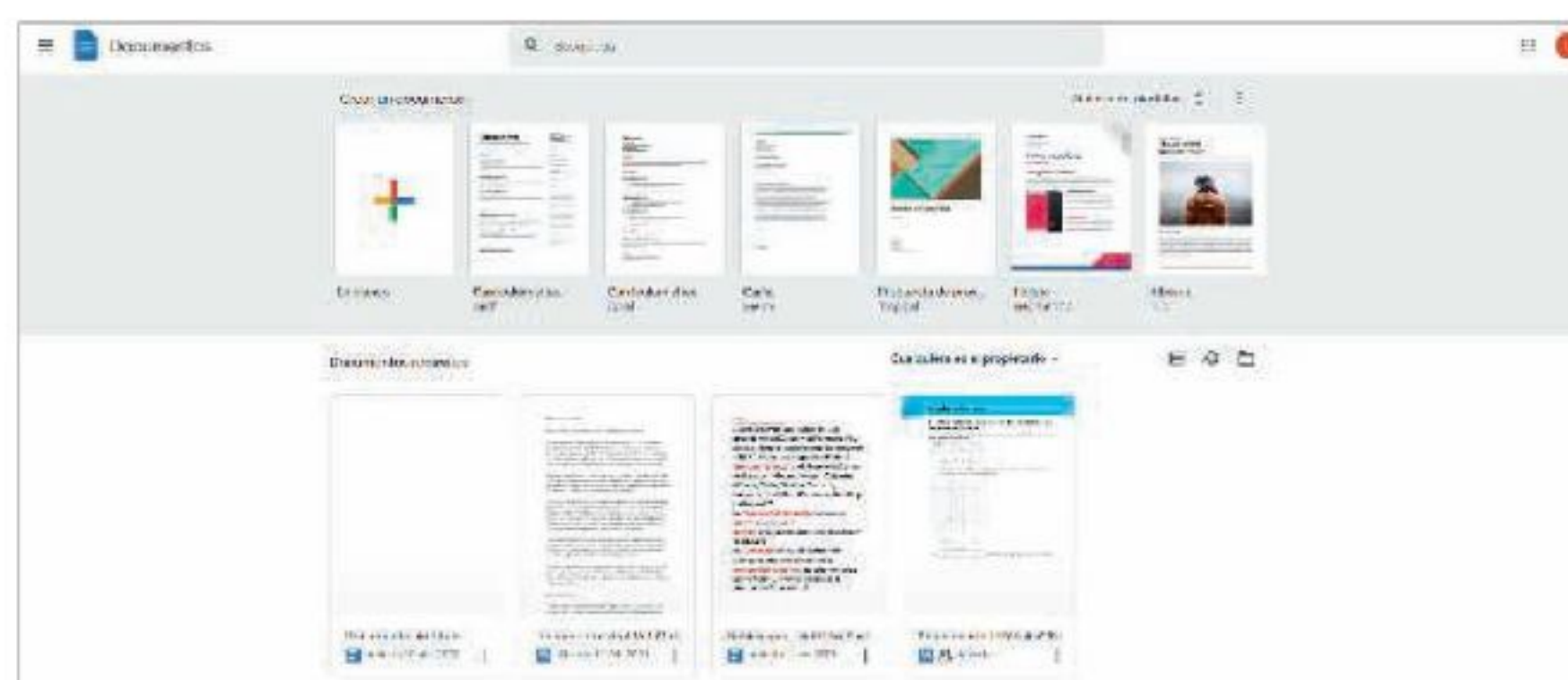


Figura 3.19. Documentos de Google.

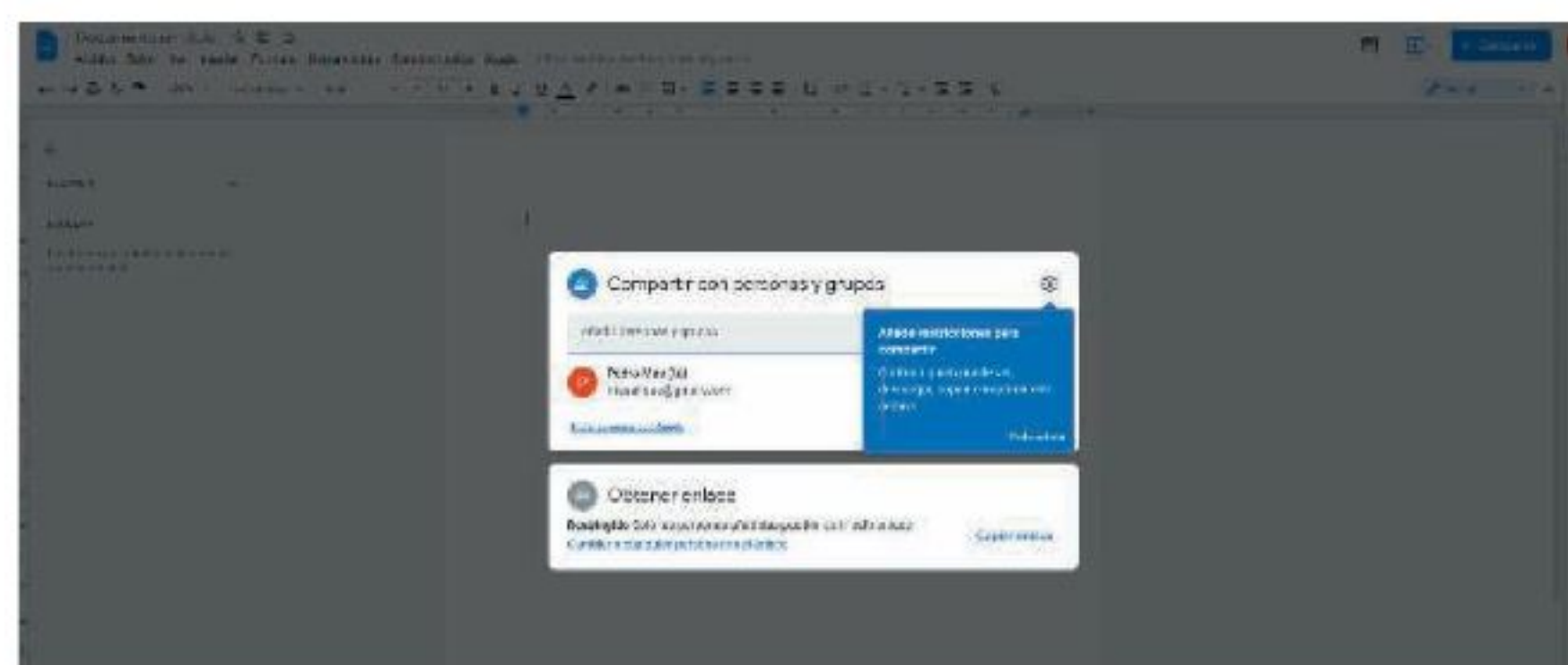


Figura 3.20. Documentos de Google.



Figura 3.21. Microsoft 365.

Ahora hay que practicar con estas y otras herramientas, haciendo las actividades propuestas.

► ACTIVIDAD PROPUESTA 3.3

Chat y mensajería

¿Qué características son importantes para usted en una aplicación de chat o mensajería?

- Conteste a la pregunta anterior y estudie lo que ofrece cada una de las aplicaciones citadas, sobre todo las que no conozca.
- ¿Ha encontrado lo que busca? Si no es así, puede que tenga que buscar otras aplicaciones, no son las únicas.

► ACTIVIDAD PROPUESTA 3.4

Videoconferencia

¿Qué características son importantes para usted en una aplicación de videoconferencia?

- Conteste a la pregunta anterior y estudie lo que ofrece cada una de las aplicaciones citadas, sobre todo las que no conozca.
- ¿Ha encontrado lo que busca? Si no es así, puede que tenga que buscar otras aplicaciones, no son las únicas.

**► ACTIVIDAD PROPUESTA 3.5****Herramientas colaborativas**

¿Ha trabajado con este tipo de herramientas?

Si la respuesta es afirmativa, compare la que haya utilizado con las aplicaciones citadas.

Si la respuesta es negativa, haga tres cosas:

1. Practique con las herramientas gratuitas de Google.
2. Descargue la versión de prueba de Microsoft 365 y trabaje con ella.
3. Compare con las demás que se citan.

Nota: el objeto es que se familiarice con esta forma de trabajar; si puede recurrir a otras personas para que colaboren con usted en estas tareas, mucho mejor.

3.3. Normas de conducta y peligros

Hemos comentado diversas formas de compartir información, pero al hacerlo hay que ser conscientes de que compartimos aquello que hacemos público, lo que realmente queremos compartir y de que, en muchos casos, publicamos datos personales como direcciones de correo electrónico y otros.

Pero no solo compartimos eso: vamos dejando una huella digital que va conformando la identidad digital²⁰, que da mucha información de cada internauta.

Hasta ahora hemos insistido en las normas básicas al compartir información: prudencia, corrección, respeto, etc., pero hay que extremar las precauciones al navegar por la red, pues hay amenazas constantes. Si se quieren evitar, hay que adoptar unas pautas básicas de comportamiento.

Antes de comentar dos de los peligros más frecuentes, el ciberacoso y la suplantación de identidad, veamos unas normas básicas de conducta en la red y unas reglas elementales de seguridad.

Normas de conducta en la red:

Existen numerosas recopilaciones en la red sobre las normas de conducta que se han de seguir para los distintos canales: foros, chats, correo electrónico, redes sociales, etc., pero es el libro NETiquette de Virginia Shea, el que se toma como base y en el que se establecen las normas elementales. Las reglas que define son las siguientes:

²⁰ Mas Alique, P. (2022): *Competencias digitales básicas*. Madrid: Ediciones Paraninfo

- No olvidar nunca que quien lee el mensaje es una persona y tiene sentimientos que podemos ofender.
- Seguir los mismos patrones de conducta en internet que en los demás contextos comunicativos.
- Comprobar el entorno para conocer los usos del sitio web.
- Respetar el tiempo y ancho de banda de las otras personas.
- Mostrar lo mejor de nosotros mismos mientras estemos en internet.
- Compartir nuestro conocimiento con la comunidad.
- Ayudar a mantener los debates en un ambiente sano e instructivo.
- Respetar la privacidad de terceras personas.
- No abusar del poder.
- Perdonar los errores ajenos.

En la comunicación empresarial también se han de cuidar las normas de conducta, no solo de los interlocutores corporativos o encargados de la comunicación, sino también de las aportaciones en internet de cada uno de sus empleados. Actualmente la reputación en línea de la empresa convive junto a la del individuo, cualquiera puede convertirse en portavoz solo con especificar su lugar de trabajo en su perfil personal. Una opinión personal puede dañar la imagen de la empresa, por ello es importante que los empleados conozcan la cultura corporativa y las normas de la compañía en internet, en el caso de que las tenga.

Existen numerosas empresas que crean un manual de estilo o guía de uso para los nuevos medios, de esta manera se invita a los empleados a seguir las recomendaciones específicas que han de guiar sus actos. Estas pueden ir desde cómo escribir los correos electrónicos según sea el destinatario, hasta la manera en que se hace referencia a la empresa en un tuit.

La etiqueta en la red es más extensa de lo que se ha explicado aquí, y sigue en permanente construcción, según van apareciendo nuevos servicios. Las reglas básicas que hay que recordar son, de una parte, que al otro lado del monitor siempre hay personas que tienen sentimientos igual que nosotros, a las que debemos tratar tal y como nos gusta que nos traten a nosotros; y, de otra parte, que los recursos de la red son limitados y debemos cuidarlos entre todos²¹.

Hemos reproducido el texto completo para que podamos entenderlo tanto desde el punto de vista personal como de la empresa, pero realmente es un tratado de buenas maneras que se recomienda seguir, pues contribuye a hacer de la red un medio más amable.

²¹ <https://www.fundeu.es/escribireninternet/normas-basicas-de-conducta-en-la-red>



No solo hay que ser correctos, también hay que ser prudentes. Veamos los consejos de Kaspersky, empresa que fabrica uno de los antivirus más conocidos:

Las 10 reglas principales de seguridad en internet y qué no hacer online

Un joven de 19 años, candidato para un cargo público en Nuevo Hampshire, descubrió de la manera más dura la importancia que tiene seguir las reglas de seguridad en internet. Tal como indica Seacoastonline, sus oponentes encontraron imágenes en publicaciones de las redes sociales que eran muy sugerentes sexualmente y hacían referencia al uso de drogas en el pasado. Así como así, su fulminante carrera política se estrelló y ardió en llamas justo al despegar. Pero, desafortunadamente, no es el único al que ha sucedido algo parecido, ya que los descuidados hábitos en internet han dejado a muchas otras personas expuestas a estafas, robo de identidad y daños físicos a manos de personas que conocieron online. Cada vez más usuarios acceden a internet a través de dispositivos móviles, por lo que estos riesgos cambian y crecen rápidamente.

Aunque las aplicaciones han adquirido mayor relevancia en la mayoría de las interacciones online diarias de las personas en comparación con los sitios web tradicionales, esto no significa que las reglas de seguridad básicas en internet hayan cambiado. Los hackers siguen buscando información personal que puedan utilizar para acceder a tu tarjeta de crédito e información bancaria.

La navegación no segura puede llevar también a otras amenazas, desde imágenes o comentarios personales embarazosos que, una vez online, son casi imposibles de borrar, hasta mezclarte con personas con las que preferirías no haber tenido nada que ver jamás.

A continuación, se incluyen las 10 reglas principales de seguridad en internet que debes seguir para evitar tener problemas online (y sin conexión).

1. *Publica información personal de forma limitada y profesional.* Los posibles empleadores o clientes no necesitan saber el estado de tu relación personal o la dirección de tu casa. Lo que necesitan saber es información sobre tu experiencia laboral y tus conocimientos profesionales, y cómo ponerse en contacto contigo. No proporcionarías información puramente personal a extraños individualmente, por lo tanto, no la proporcionas a millones de personas online.
2. *Mantén la configuración de privacidad activada.* A los responsables de marketing les encanta saber todo acerca de ti, al igual que los hackers. Ambos pueden aprender mucho de tus hábitos de navegación y el uso que haces de las redes sociales. Pero puedes tomar el control de tu información. Como señala Lifehacker, tanto los navegadores web como los sistemas operativos móviles disponen de ajustes para proteger tu privacidad online. Los principales sitios web, como Facebook, también tienen ajustes de mejora de la privacidad disponibles. Estos ajustes son a veces (deliberadamente) difíciles de encontrar, porque las empresas quieren tu información personal por su valor de marketing. Asegúrate de que has activado estas garantías de privacidad y de mantenerlas activadas.

3. *Practica la navegación segura.* No elegirías caminar por un vecindario peligroso, por lo tanto, no visites barrios peligrosos online. Los cibercriminales utilizan contenido morboso como cebo. Ellos saben que las personas a veces se sienten tentadas ante el contenido dudoso, y pueden bajar la guardia cuando lo buscan. El «demi monde» de internet está plagado de problemas ocultos, donde un clic descuidado podría exponer datos personales o infectar tu dispositivo con malware. Al resistirte al impulso, los hackers ni siquiera tendrán la mínima oportunidad.
4. *Asegúrate de que tu conexión a internet es segura.* Cuando te conectas online en un lugar público, por ejemplo, mediante el uso de una conexión wifi pública, PCMag señala que no tienes control directo sobre tu seguridad. Los expertos en ciberseguridad corporativa muestran preocupación por los «endpoints», es decir, los lugares en los que una red privada se conecta con el mundo exterior. Tu «endpoint vulnerable» es tu conexión a internet local. Asegúrate de que el dispositivo es seguro y, en caso de duda, espera a conectarte en un momento mejor (es decir, hasta que seas capaz de conectarte a una red wifi segura) antes de proporcionar información como el número de tu cuenta bancaria.
5. *Ten cuidado con lo que descargas.* Uno de los principales objetivos de los cibercriminales es engañarte para que descargues malware, es decir, programas o aplicaciones que incluyen malware o tratan de robar información. Este malware puede disfrazarse como una aplicación: desde un juego popular a una aplicación que comprueba el tráfico o el clima. Como aconseja PCWorld, no descargues aplicaciones que parezcan sospechosas o procedan de un sitio en el que no confías.
6. *Elige contraseñas seguras.* Las contraseñas son uno de los mayores puntos débiles de toda la estructura de seguridad en internet, pero actualmente no hay manera de omitirlas. Y el problema de las contraseñas es que las personas tienden a elegir aquellas que son fáciles de recordar (como «contraseña» y «123456»), y que también son fáciles de adivinar para los ciberladrones. Selecciona contraseñas seguras que sean más difíciles de descubrir para los cibercriminales. El software Password Manager puede ayudarte a administrar varias contraseñas para que no las olvides. Una contraseña segura es aquella que es única y compleja, de al menos 15 caracteres y que incluya letras, números y caracteres especiales.
7. *Realiza compras online en sitios seguros.* Cada vez que realices una compra online, necesitas proporcionar información sobre la tarjeta de crédito o la cuenta bancaria, justo lo que los cibercriminales más desean tener en sus manos. Suministra esta información solo a aquellos sitios que te ofrecen conexiones seguras y cifradas. Tal como indica la Universidad de Boston, puedes identificar los sitios seguros mediante la búsqueda de una dirección que comience por https: (la S proviene de seguro) en lugar de comenzar simplemente por http:. También pueden incluir el icono de un candado situado junto a la barra de direcciones.



8. Ten cuidado con lo que publicas. Internet no tiene una tecla Suprimir, como descubrió el joven candidato de Nuevo Hampshire. Cualquier comentario o imagen que publicas online puede permanecer online para siempre, porque eliminar el original (por ejemplo, de Twitter) no elimina las copias que otras personas puedan tener. No hay ninguna manera de «borrar» un comentario que desearías no haber compartido, o deshacerte de ese vergonzoso selfie que te hiciste en una fiesta. No publiques online nada que no quieras que vea tu madre o un empleador.
9. Ten cuidado con quien conoces online. Las personas que conoces online no siempre son quienes dicen ser. De hecho, incluso pueden no ser reales. Como indica InfoWorld, los perfiles de redes sociales falsos son una forma popular entre los hackers de atraer a los usuarios incautos de internet y robarles la cartera online. Se aconseja que seas tan prudente y sensato en tu vida social online como lo eres en tu vida social en persona.
10. Mantén actualizado el programa antivirus. El software de seguridad en internet no puede protegerte contra toda amenaza, pero detectará y eliminará la mayor parte del malware, aunque debes asegurarte de que esté actualizado. Asegúrate de estar al día con las actualizaciones del sistema operativo y las actualizaciones de las aplicaciones que utilizas. Proporcionan un nivel de seguridad vital.

Mantén estas 10 reglas básicas de seguridad en internet en mente y podrás evitar muchas de las sorpresas desagradables que acechan online a los descuidados.

Poco más se puede decir, como siempre recomendar prudencia, veamos algunas de las desagradables consecuencias de la ignorancia y de la imprudencia²².

3.3.1. Ciberacoso

El ciberacoso es el acoso ejercicio mediante internet. Para conocer mejor este fenómeno, vamos a recurrir a UNICEF:

Reunimos a especialistas de UNICEF y a expertos internacionales en acoso cibernético y protección de la infancia, y colaboramos con Facebook, Instagram, Tik Tok y Twitter para responder algunas de las preguntas más frecuentes sobre el acoso en línea y ofrecer consejos sobre la manera de hacerle frente.

¿Qué es ciberacoso?

Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas. Por ejemplo:

²² <https://www.kaspersky.es/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online>

- Difundir mentiras o publicar fotografías o videos vergonzosos de alguien en las redes sociales.
- Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería.
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

El acoso cara a cara y el ciberacoso ocurren juntos a menudo. Pero el ciberacoso deja una huella digital; es decir, un registro que puede servir de prueba para ayudar a detener el abuso²³.

El documento continúa respondiendo a una serie de preguntas sobre el tema. Recomendamos su lectura pues, aunque se refiere a los jóvenes, que son una población especialmente vulnerable, los consejos son de interés general.

Para ampliar información, recomendamos al lector que visite el sitio de Avast Academy²⁴ (otro fabricante de antivirus) y el de Sanitas²⁵, compañía de servicios médicos donde se indican las consecuencias del ciberacoso.

El ciberacoso es, por desgracia, un problema actual y muy real cuyas víctimas son en un alto porcentaje menores; de ahí la importancia de que padres, educadores y la sociedad en general estemos atentos a este tipo de conductas para proteger al débil y poner a los malos en manos de las autoridades para que se les aplique todo el peso de la ley. Todos hemos de contribuir a erradicar esta lacra.

3.3.2. Suplantación de identidad

La suplantación de identidad es lo que su propio nombre indica: hacerse pasar por otra persona.

Veamos lo que nos dice el Banco de Santander:

¿Qué es la suplantación de identidad?

Según diversos estudios realizados se estima que millones de personas cada año sufren robos o suplantaciones de identidad en todo el mundo. Saber cómo se realiza puede ayudarnos a protegernos de un posible robo de identidad.

¿Qué es?

La suplantación o robo de identidad en internet consiste en hacerse pasar por otra para cometer actividades delictivas, tales como fraude o estafas, obtener datos o información sensible o confidencial, cyberbulling (acoso a personas a través de internet), grooming (abuso sexual de menores), etcétera.

²³ <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>

²⁴ <https://www.avast.com/es-es/c-cyberbullying>

²⁵ <https://www.sanitas.es/sanitas/seguros/es/particulares/biblioteca-de-salud/psicologia-psiquiatria/acoso-psicologico/ciberacoso.html>



¿Cómo se realiza la suplantación de identidad en internet?

Para suplantar o robar la identidad de otras personas es necesario que el atacante obtenga ciertos datos personales utilizando para ello las vulnerabilidades conocidas en los sistemas de seguridad informáticos. Los ciberdelincuentes pueden utilizar diferentes técnicas para acceder a esa información personal: el robo de equipos que contienen información personal y la interceptación de la propia información personal enviada por los individuos a través de redes poco confiables mediante técnicas *man in the middle*.

La suplantación de identidad es un delito y puede ser castigado con penas de prisión. Según la OSI, existen varias formas para robar la identidad de alguien:

- Accediendo a la cuenta del usuario mediante técnicas de phishing y malware.
- A través de un perfil falso, por ejemplo, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

¿Cómo podemos protegernos?

Algunas recomendaciones para intentar mitigar la fuga de datos personales que pueden ocasionar las suplantaciones de identidad son:

- Disponer de procedimientos de clasificación y tratamiento de la información que contemple los datos personales.
- Formación y concienciación del personal en las buenas prácticas de seguridad de la información y en la protección de datos personales, uso aceptable de las TIC, así como en los procedimientos de clasificación y tratamiento de la información.
- Actualización y parcheo de seguridad de los equipos, sistemas y aplicaciones.
- Escaneo, análisis y remediación de vulnerabilidades en los sistemas y aplicaciones.
- Realización de pruebas de intrusión (pentesting) para la detección y corrección de debilidades o vulnerabilidades.
- Implementación de sistemas de prevención de fugas de información.
- Cifrado de la información en almacenamiento y en tránsito.
 - Cifrar los discos duros de los dispositivos portátiles para evitar el acceso a la información en caso de pérdida o robo de estos.
 - Evitar la utilización de soportes extraíbles como memorias USB, utilizando medios alternativos como repositorios cloud seguros o correo electrónico cifrado y en caso de ser imprescindible almacenar información de carácter personal en ellos, cifrarlos.
 - Al enviar datos personales a través de internet se deberían enviar por canales seguros como correo electrónico cifrado, VPN, túneles SSH o formularios web con implantación de HTTPS.

Mediante la suplantación o robo de identidad se puede cometer fraude y estafas u obtener información sensible o confidencial que puede ocasionar graves daños o perjuicios a las personas u organizaciones²⁶.

Antes de terminar, hay que aclarar un concepto del que no se ha hablado hasta ahora: ataque «*man in the middle*», es decir, ataque mediante un intermediario, el cibercriminal o un software malicioso que se incrusta entre la víctima y la fuente de datos con el objetivo de interceptar, leer o manipular de forma efectiva la comunicación entre la víctima y sus datos sin que nadie se dé cuenta de que hay un extraño en el proceso.

Mantenerse al día en temas de ciberseguridad es necesario y resulta muy interesante. No hace falta ser un experto para ello y hay varios sitios recomendables, por ejemplo, INCIBE, donde hay mucha información asequible para cualquier internauta.

► ACTIVIDAD PROPUESTA 3.6

Seguridad

Lea, de nuevo y detenidamente, las *Normas de conducta en la red* y *Las 10 reglas principales de seguridad en internet* y qué no hacer online.

- ¿Actúa de acuerdo con ellas?
- ¿Qué tendría que mejorar?

► ACTIVIDAD PROPUESTA 3.7

Ciberacoso

Busque información sobre ciberacoso, a ser posible, casos reales. En la página de INCIBE puede encontrarlo, pero busque en más sitios. El tema es lo suficientemente grave como para documentarse y ver lo que les ha sucedido a las víctimas. Le ayudará a tomar conciencia de la importancia de conocerlo y saber cómo actuar.

► ACTIVIDAD PROPUESTA 3.8

Suplantación de identidad

Busque información sobre suplantación de identidad, a ser posible, casos reales. En la página de INCIBE puede encontrarlo, pero busque en más sitios. El tema es lo suficientemente grave como para documentarse y ver lo que les ha sucedido a las víctimas. Le ayudará a tomar conciencia de la importancia de conocerlo y saber cómo actuar.

²⁶ <https://www.bancosantander.es/glosario/suplantacion-identidad-internet>



DE COMPROBACIÓN

3.1. Subir información a la red:

- a. Download.
- b. No se puede subir información a la red.
- c. Cibergeneración virtual.
- d. Upload.

3.2. El uso de las redes sociales debe ser:

- a. Correcto y veraz.
- b. Respetuoso.
- c. Prudente.
- d. Las tres respuestas anteriores son correctas.

3.3. El chat es una herramienta instantánea de comunicación que se utiliza en ámbitos muy distintos:

- a. Muchas páginas web los incluyen.
- b. Hay aplicaciones específicas de chat.
- c. Algunos están disponibles en los servicios de correo electrónico.
- d. Las tres respuestas anteriores son correctas.

3.4. La prudencia debe ser la norma en la comunicación vía internet, sea cual sea el medio utilizado:

- a. No se puede asegurar la no reproducción o archivo del mensaje.
- b. Es muy frecuente el mal uso de los mensajes, por error o con mala intención.
- c. Nunca se sabe dónde puede acabar un mensaje enviado, sea escrito, hablado, videos, fotos, etcétera.
- d. Las tres respuestas anteriores son correctas.

3.5. Ciberacoso:

- a. Propaganda emitida por la red.
- b. Acoso ejercido mediante internet.
- c. Anuncios que aparecen en determinadas aplicaciones.
- d. Las tres respuestas anteriores son correctas.

3.6. Intercambio de mensajes electrónicos a través de internet que permite establecer una conversación entre dos o más personas:

- a. Email.
- b. Chat.
- c. Blog.
- d. Solo se pueden comunicar dos personas, no más.

**3.7. Sistema de emisión y recepción de mensajes, de diversos tipos, a través de dispositivos electrónicos y digitales:**

- a. Videoconferencia.
- b. Cibercomunicación en la nube.
- c. Mensajería.
- d. Correo electrónico.

3.8. El acoso cara a cara y el ciberacoso ocurren juntos a menudo, pero el ciberacoso deja una huella digital: un registro que puede servir de prueba para ayudar a detener el abuso:

- a. No es cierto, no es el mismo perfil el del ciberacosador que el del acosador presencial.
- b. El ciberacoso no tiene importancia.
- c. Lo que permite, en muchos casos, identificar y detener al acosador, que es lo que hay que hacer.
- d. Solo si se tiene un móvil.

3.9. Sitio web en el que los autores publican sus textos, ordenados por orden cronológico inverso:

- a. Comunidad.
- b. Blog.
- c. Wiki.
- d. Foro.

3.10. Preste atención a cómo se presenta a los demás en la red social y a cómo le perciben el resto de usuarios:

- a. Porque las redes aportan información sobre usted, que puede ser utilizada para muchos fines.
- b. Porque su huella digital va configurando su identidad digital.
- c. Porque es la imagen que personas y entidades perciben de usted.
- d. Las tres respuestas anteriores son correctas.

3.11. Hacerse pasar por otra persona en la red para cometer actividades delictivas, tales como fraude o estafas, obtener datos o información sensible o confidencial, acoso, etcétera:

- a. No es posible hacerlo.
- b. Ciberpersonaje virtual.
- c. Avatar.
- d. Suplantación de identidad.

**3.12. Man in the middle:**

- a. Ataque mediante un intermediario.
- b. Persona o programa que se mete entre el usuario y su fuente de información, con fines delictivos.
- c. Ciberataque para manipular, con fines delictivos la información de una persona.
- d. Las tres respuestas anteriores son correctas.

3.13. Programas para trabajar en equipo que tienen como objetivo mejorar el proceso de trabajo:

- a. Blogs.
- b. Herramientas colaborativas.
- c. Foros.
- d. Comunidades.

3.14. Las redes sociales disponen de formularios para denunciar el comportamiento inadecuado de un usuario:

- a. Que solo sirven para ejercer una censura encubierta.
- b. Que solo pueden utilizar los gestores de la red.
- c. Que deben utilizarse para denunciar este tipo de comportamientos.
- d. Las tres respuestas anteriores son correctas.

3.15. Aplicación web que permite mantener discusiones y aportar opiniones e información en un espacio virtual categorizado en temas de discusión o hilos que pueden abrir las propias personas usuarias, y a los que el resto pueden responder:

- a. Blog.
- b. Wiki.
- c. Foro.
- d. Una pérdida de tiempo.

3.18. ¿Le gusta hacer punto de cruz? ¿Prefiere la cocina? Busque información sobre estos temas, por ejemplo en Google, y compare lo obtenido con lo que se encuentra en los foros visitados anteriormente. ¿Qué información considera que es mejor? ¿Son complementarias?

3.19. ¿Le interesan los motores rotativos? ¿Las maquetas? Busque blogs sobre estos temas u otros de su interés y analice tanto los contenidos como la forma de expresarse de los participantes. ¿Qué mejoraría?

3.20. ¿Va a comprarse un patinete eléctrico? ¿Un triciclo mejor? Busque wikis sobre estos temas u otros de su interés y analice tanto los contenidos como la forma de expresarse de los participantes. ¿Qué mejoraría?

3.21. Motores rotativos, maquetas, patinetes, etc. Busque información sobre estos temas, por ejemplo en Google, y compare lo obtenido con lo que se encuentra en los wikis o blogs visitados anteriormente. ¿Qué información considera que es mejor? ¿Son complementarias?

3.22. Cocina, punto de cruz, maquetas, etc. Busque comunidades sobre temas diversos. ¿Utilidad? ¿Interés? ¿Encuentra información en alguna red social?

3.23. Trabaje con Franz y vea si le resulta útil.

3.24. Trabaje con las distintas herramientas de Google para comunicación y trabajo en equipo y vea si le resultan útiles (conviene hacerlo con más personas).

3.25. Trabaje con las distintas herramientas de Microsoft para comunicación y trabajo en equipo y vea si le resultan útiles (conviene hacerlo con más personas).

3.26. Busque información sobre NETiquette. ¿Cree que es una forma de hacer de la red un medio más amable y seguro?

3.27. Como también hay vida fuera de Google y de Microsoft, analice otros programas y aplicaciones de comunicación y trabajo en equipo; cada persona u organización tiene sus costumbres y hay que ser flexible.

3.28. Busque noticias de prensa sobre ciberacoso, casos reales y situación general.

3.29. Busque noticias de prensa sobre suplantación de identidad, casos reales y situación general.

3.30. Reflexione sobre la manera de prevenir conductas delictivas en la red, sobre todo las que tienen como víctimas a menores.

DE APLICACIÓN

3.16. Para empezar a familiarizarse con la información que comparten empresas y entidades de distinto tipo, visite páginas web de administraciones públicas, de empresas privadas, de fundaciones, etc. Vea si tienen chat, qué tipo de información publican y si, en su opinión, consiguen hacerla fácilmente accesible al destinatario.

3.17. ¿Le gusta hacer punto de cruz? ¿Prefiere la cocina? Busque foros sobre estos temas u otros de su interés y analice tanto los contenidos como la forma de expresarse de los participantes. ¿Qué mejoraría?



Creación del contenido

Mucha de la información que compartimos en la red es textual, pero también hay fotografías, imágenes, tablas y gráficos que sirven para ilustrar y explicar los contenidos.

En esta unidad estudiamos hojas de cálculo y bases de datos, cuya utilidad es procesar y almacenar la información para su tratamiento matemático, estadístico y gráfico, sin olvidar el retoque de imágenes, necesario en determinadas actividades.

Finalizamos con el estudio de los derechos de autor y de las licencias de uso de la información, pues no todo lo que hay en la red es de uso libre y gratuito.

Contenido

- 4.1. Herramientas ofimáticas (hoja de cálculo y base de datos)
- 4.2. Retoque básico de imágenes
- 4.3. Derechos de autor y licencias

4.1. Herramientas ofimáticas (hoja de cálculo y base de datos)

Recordemos la definición de ofimática: *automatización, mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas*¹.

La Real Academia de la Lengua no siempre está al día en los temas técnicos y lo que en su momento respondía a la realidad, cuando los ordenadores y los programas eran mucho más caros y mucho menos abundantes, hoy en día no solo es aplicable a las oficinas sino también a nuestra vida cotidiana. Pero la definición sigue siendo válida y responde a la forma de realizar determinadas tareas mediante medios electrónicos.

¿Qué son una hoja de cálculo y una base de datos?

Hoja de cálculo: *programa que opera con tablas formadas por filas y columnas de celdas que contienen información numérica y fórmulas o texto, y las presenta en una pantalla*².

Base de datos: *conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información*³.

Recordemos lo visto sobre paquetes ofimáticos o suites de ofimática⁴, comentando los más usados y algunos más. Hay que tener en cuenta que hay paquetes gratuitos y de pago, y que no todos tienen los mismos programas.

A la hora de pensar en adquirir un paquete de ofimática hay que tener en cuenta sus componentes: que no todos tienen base de datos, el que sus documentos puedan abrirse con otros programas y el dispositivo en el que se van a usar. No despreciemos el software libre, si es adecuado a nuestras necesidades, puede representar un ahorro importante.

Las distintas fuentes consultadas coinciden en que los paquetes más utilizados son (no necesariamente por el orden expuesto):

- Microsoft 365.
- Google Docs.
- Apache OpenOffice.
- LibreOffice.

Dependiendo del dispositivo y del uso que se haga de los distintos programas, no hay que olvidar iWork de Apple y Polaris Office para los móviles Samsung.

¹ <https://dle.rae.es/ofimática?m=form>

² <https://dle.rae.es/hoja?m=form>

³ <https://dle.rae.es/base?m=form>

⁴ Mas Alique, P. (2022): *Competencias digitales básicas*. Madrid: Ediciones Paraninfo

Vamos a comentar los cuatro paquetes citados, recurriendo a sus respectivas webs.

Microsoft 365

Paquete de Microsoft, de pago, como ya se ha visto en la Unidad 3 al hablar de herramientas colaborativas. Lo que ahora nos interesa es que incluye un programa de hoja de cálculo, Excel, y uno de base de datos, Access, disponibles para Windows; el paquete para Apple no dispone de Access, aunque existen alternativas como FileMaker Pro, Destreza o Base de datos de Ninnox.

Es el paquete de ofimática más utilizado y, como ya vimos, puede incluir distintos programas y aplicaciones tanto para PC, como para Mac y también se puede usar en Android.

A la hora de explicar las hojas de cálculo y las bases de datos lo haremos con Excel y Access, por ser las más completas.

Google Docs

En la Figura 4.1 mostramos la web de Google Docs, que para las empresas envía a Workspace, ya comentado en la unidad anterior. Como podemos ver, incluye procesador de textos, Documentos, Hojas de cálculo y Presentaciones, pero no dispone de base de datos.

Si queremos ir a la hoja de cálculo, debemos picar en la pestaña correspondiente y, tras identificarnos con la cuenta de Google, aparece lo que mostramos en la Figura 4.2, en la que podemos ver una serie de pestañas y de iconos que permiten trabajar con la hoja de cálculo.

Es importante saber que podemos abrir archivos de Excel con esta aplicación.



Figura 4.1. Google Docs.

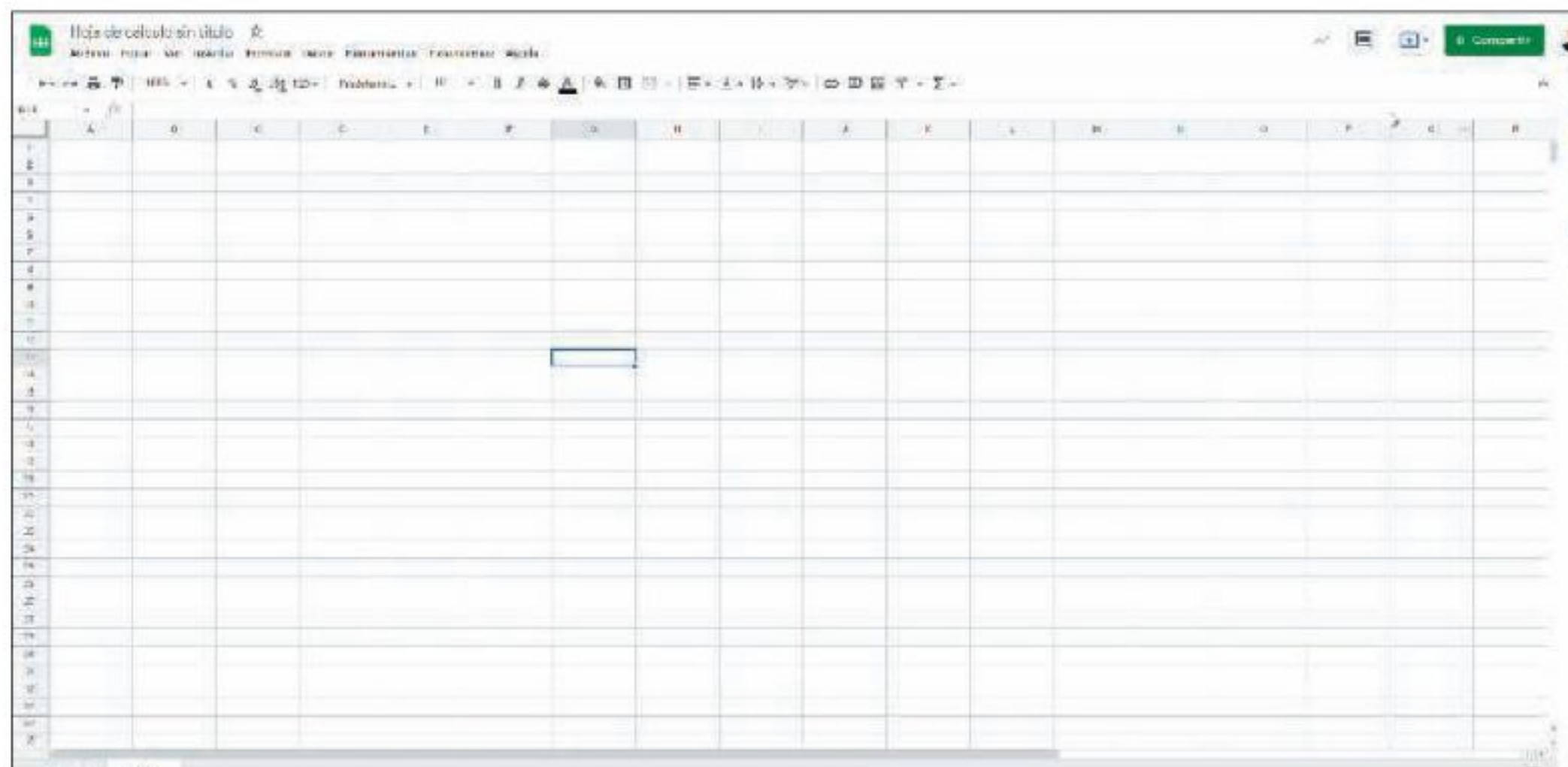


Figura 4.2. Hoja de cálculo. Google Docs.

Apache OpenOffice

En la Figura 4.3 (captura de pantalla de la web de Apache OpenOffice) mostramos los componentes del paquete: hoja de cálculo, base de datos, entre otros.



Figura 4.3. Apache OpenOffice.

Para obtenerlo, basta descargarlo desde su web y, como ya hemos indicado, es gratuito. En las Figuras 4.4 y 4.5 mostramos la hoja de cálculo, que se entiende bien con Excel, y la base de datos.

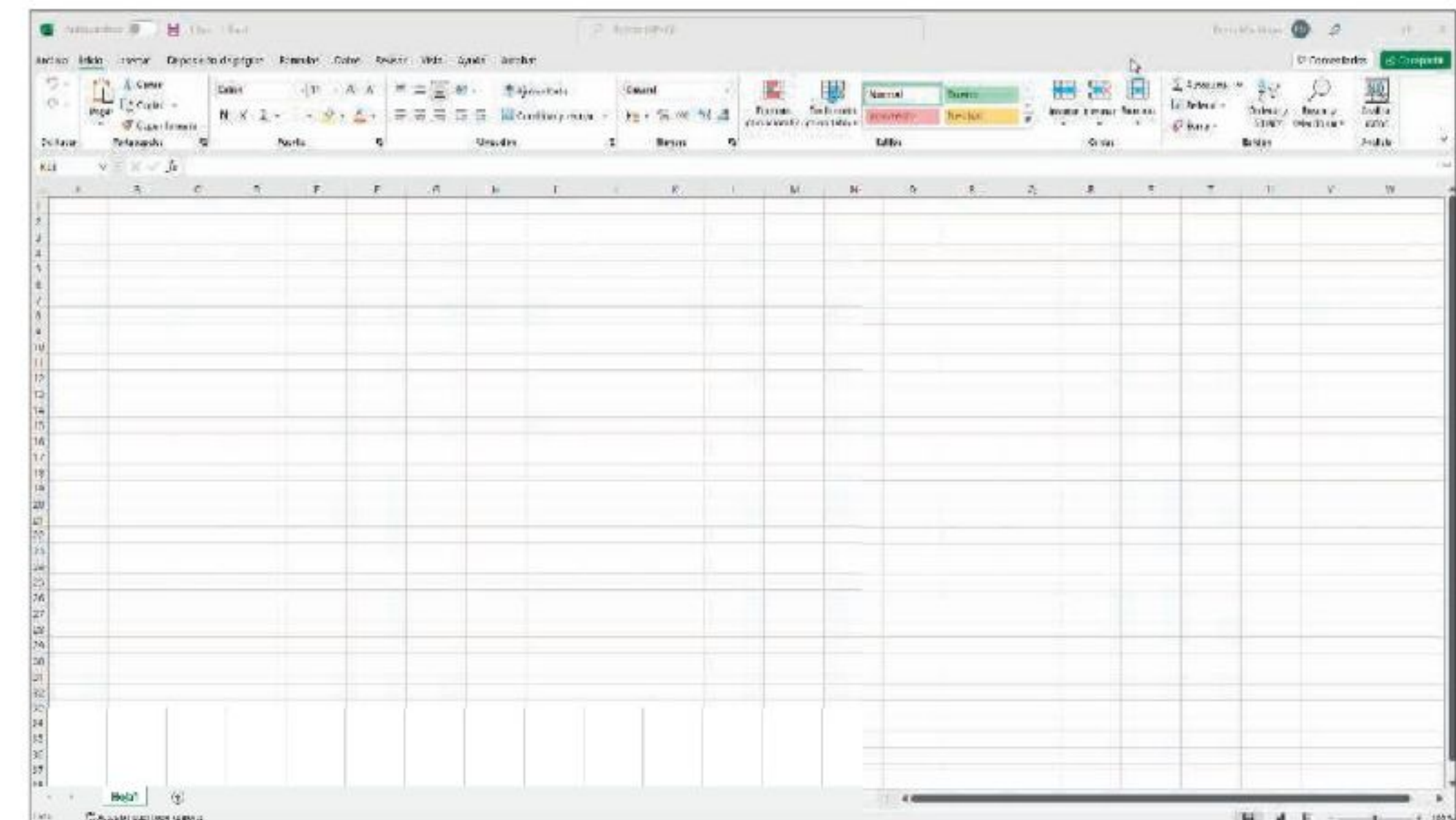


Figura 4.4. Calc. Apache OpenOffice.

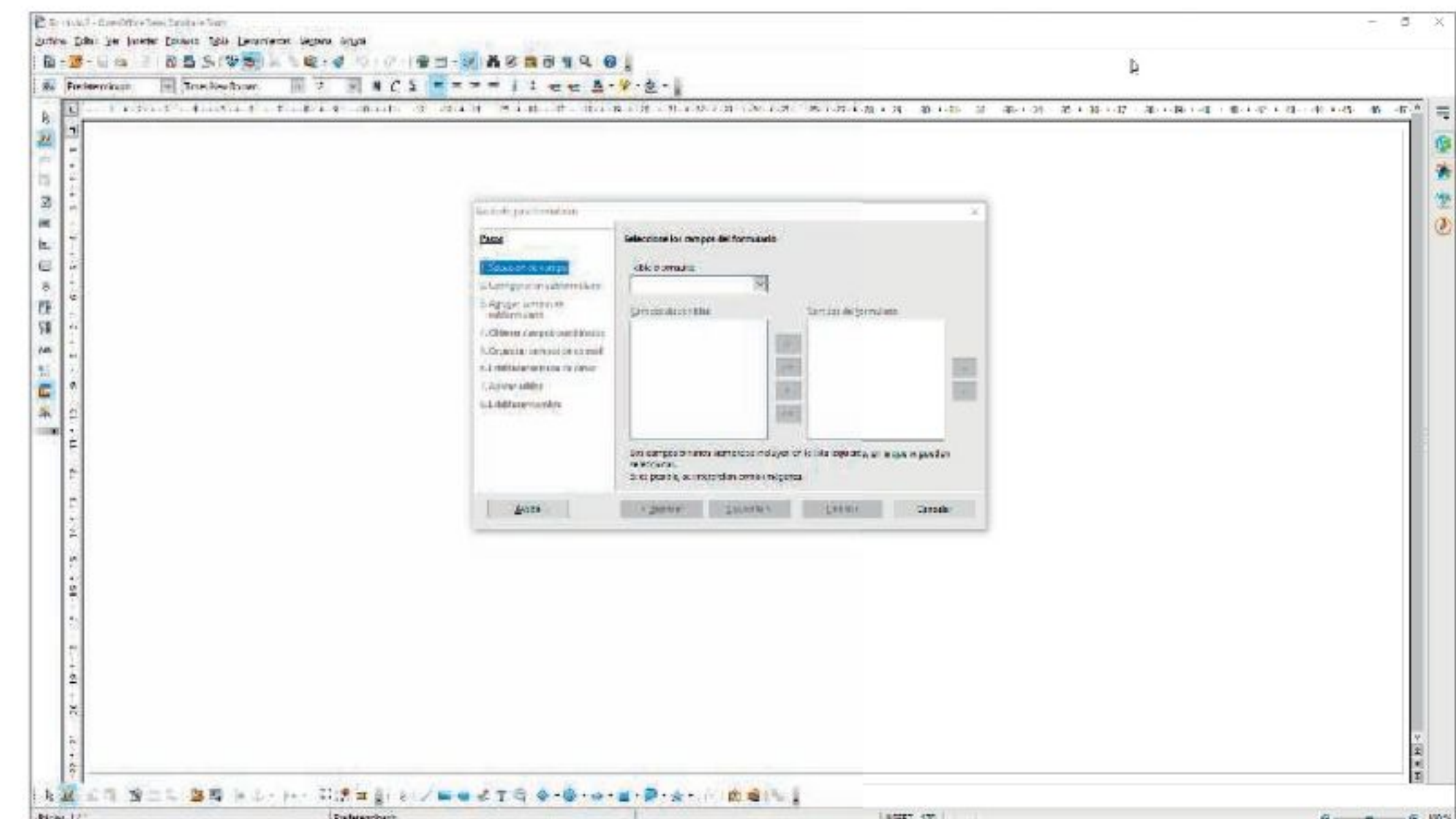


Figura 4.5. Base. Apache OpenOffice.

Para crear una base de datos podemos completar una tabla, una vez definidos los campos necesarios, o rellenar un formulario, que es la forma más adecuada de hacerlo. Por eso en la Figura 4.5 mostramos el asistente para crear un formulario. Podemos llegar hasta esa pantalla siguiendo las indicaciones una vez abierto Base.

LibreOffice

En la Figura 4.6 mostramos el contenido de LibreOffice, también con hoja de cálculo, Calc, y base de datos, Base.



Figura 4.6. LibreOffice.

El manejo de la hoja de cálculo es similar a la que hemos mostrado de Apache, y lo mismo cabe decir de la base de datos, si bien en este caso la hoja de cálculo tiene más funcionalidades. De cualquier forma, la mejor manera de aprender a manejar los programas es trabajando con ellos y siguiendo los tutoriales y consejos que ofrecen en sus webs.

Una vez conocidos los principales paquetes de ofimática y sus componentes, veamos cómo manejar la hoja de cálculo y la base de datos; como ya hemos comentado, las explicaremos mediante Microsoft Excel y Access por ser las más utilizadas y las más completas, lo que facilita el uso de las de otros fabricantes.

Si no disponemos de una licencia del paquete, podemos probar gratis durante un mes, según se indica en la web de Microsoft 365.

4.1.1. Hoja de cálculo

Para aprender a manejar Excel, la hoja de cálculo de Microsoft, lo mejor es utilizar los recursos de aprendizaje que ofrece el fabricante.

En la Figura 4.7 mostramos la página de entrada al sitio de Microsoft 365. Picando en *Recursos* y en *Aprendizaje* aparece la pantalla que mostramos en la Figura 4.8. Picando en Excel vamos a los distintos tutoriales que se ofrecen y picando en cada uno de

ellos vamos aprendiendo a manejar el programa. No hay atajos, hay que seguir las instrucciones y practicar.

Para empezar a practicar hay que abrir Excel. Al abrirlo, aparecen distintas opciones y debemos ir a la de *Libro en blanco* para empezar a trabajar siguiendo los tutoriales; así veremos lo que mostramos en la Figura 4.10. También se ofrecen distintas plantillas, pero para utilizarlas primero hay que conocer el manejo del programa.

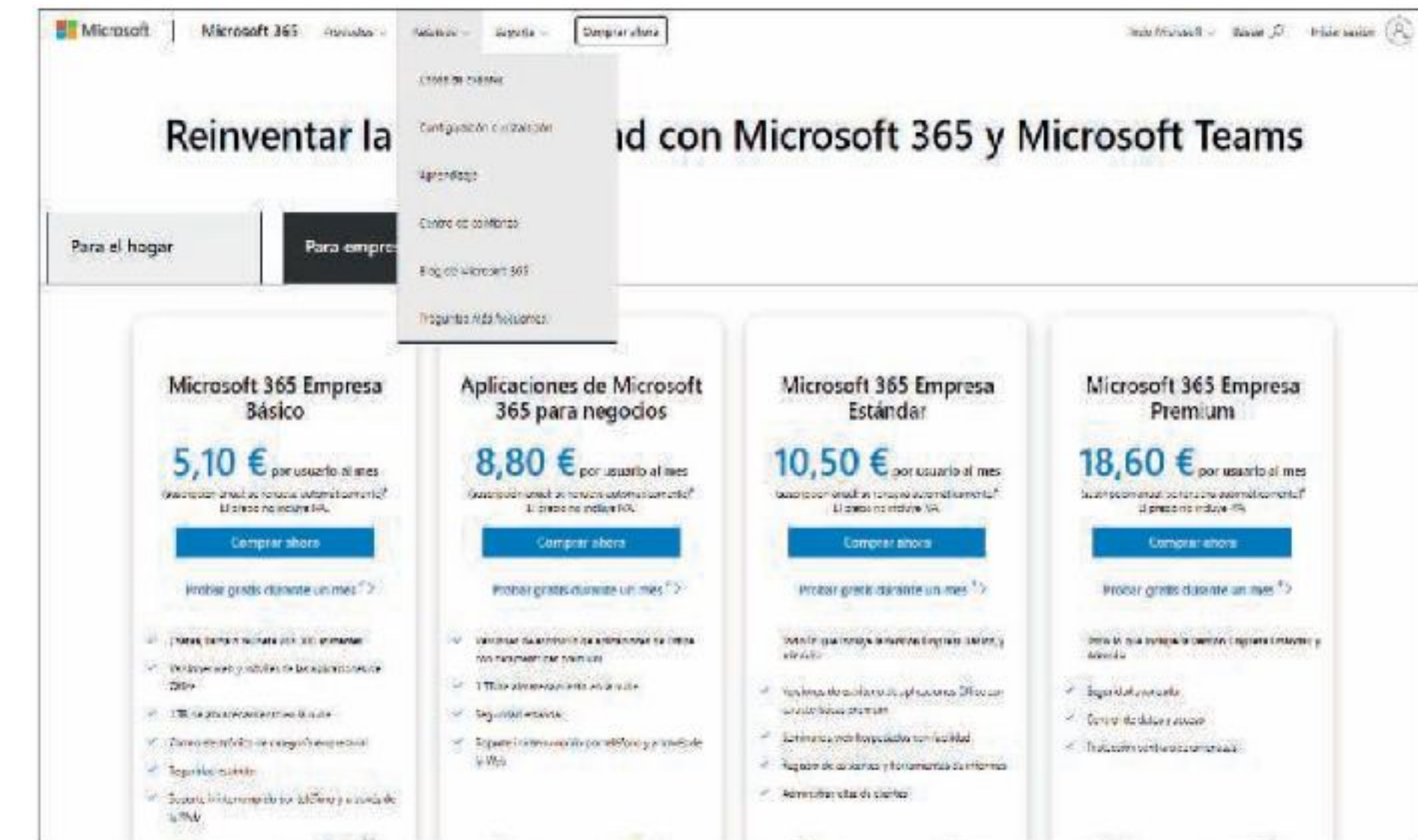


Figura 4.7. Microsoft 365.



Figura 4.8. Microsoft 365.

Excel es una hoja de cálculo muy potente, permite hacer muchas cosas, pero sirve, principalmente, para hacer cálculos y para sacarle todo el partido hay que tener ciertos conocimientos de matemáticas, de estadística y de programación matemática. No debemos asustarnos, solo queremos indicar que sirve para mucho más de lo que se podría pensar cuando se hace un uso sencillo de ella.

Aunque no seamos usuarios avanzados con Excel podemos hacer muchas cosas, como analizar información, construir tablas, hacer gráficos, crear bases de datos, etc., pero, recordemos, hay que practicar.



Figura 4.9. Excel.

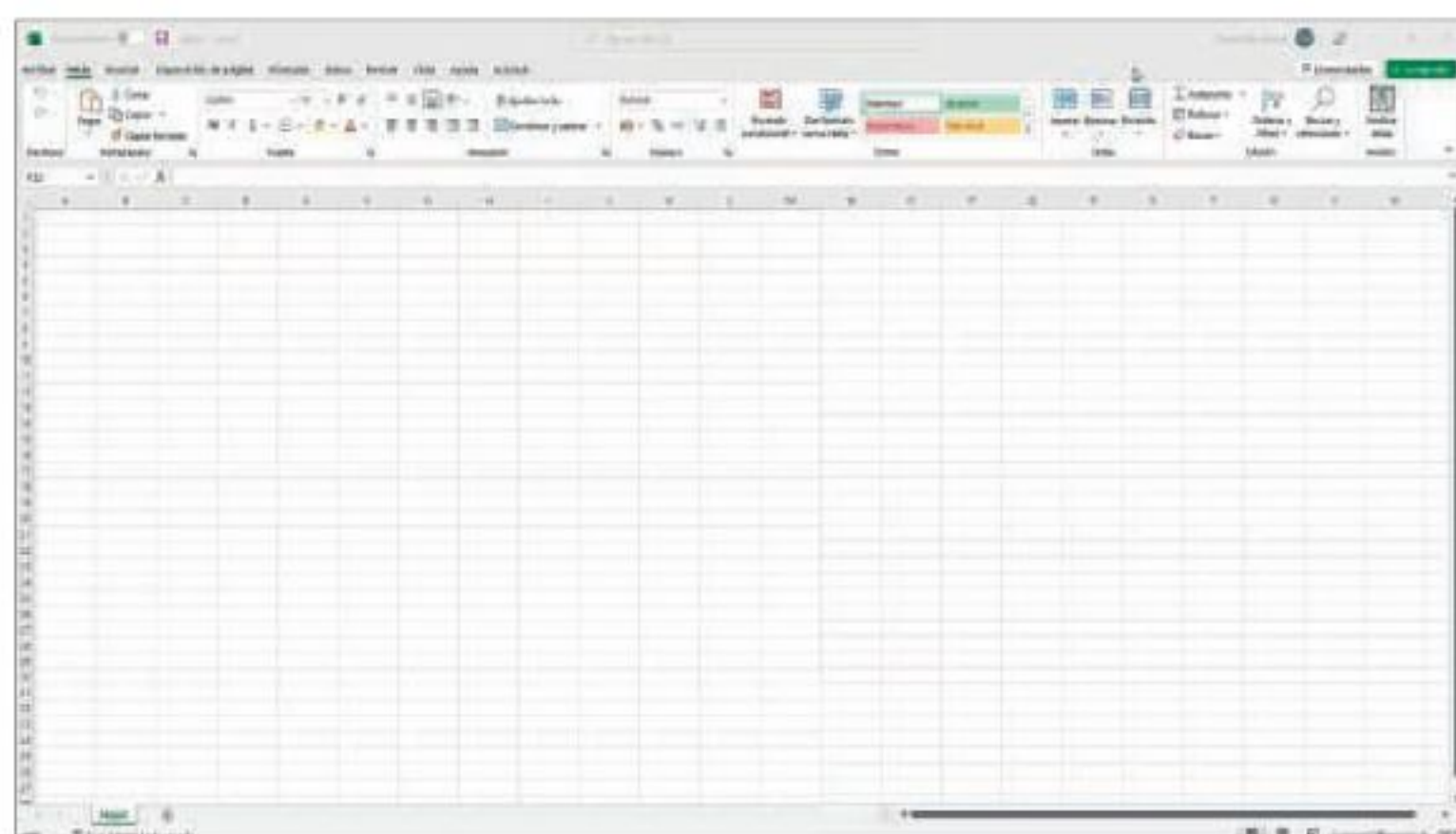


Figura 4.10. Excel.

4.1.2. Base de datos

Si en la pantalla representada en la Figura 4.8 picamos en Access, aparece la pantalla que mostramos en la Figura 4.11. Siguiendo la misma línea que con Excel, ahora toca utilizar los tutoriales para aprender a manejar el programa.

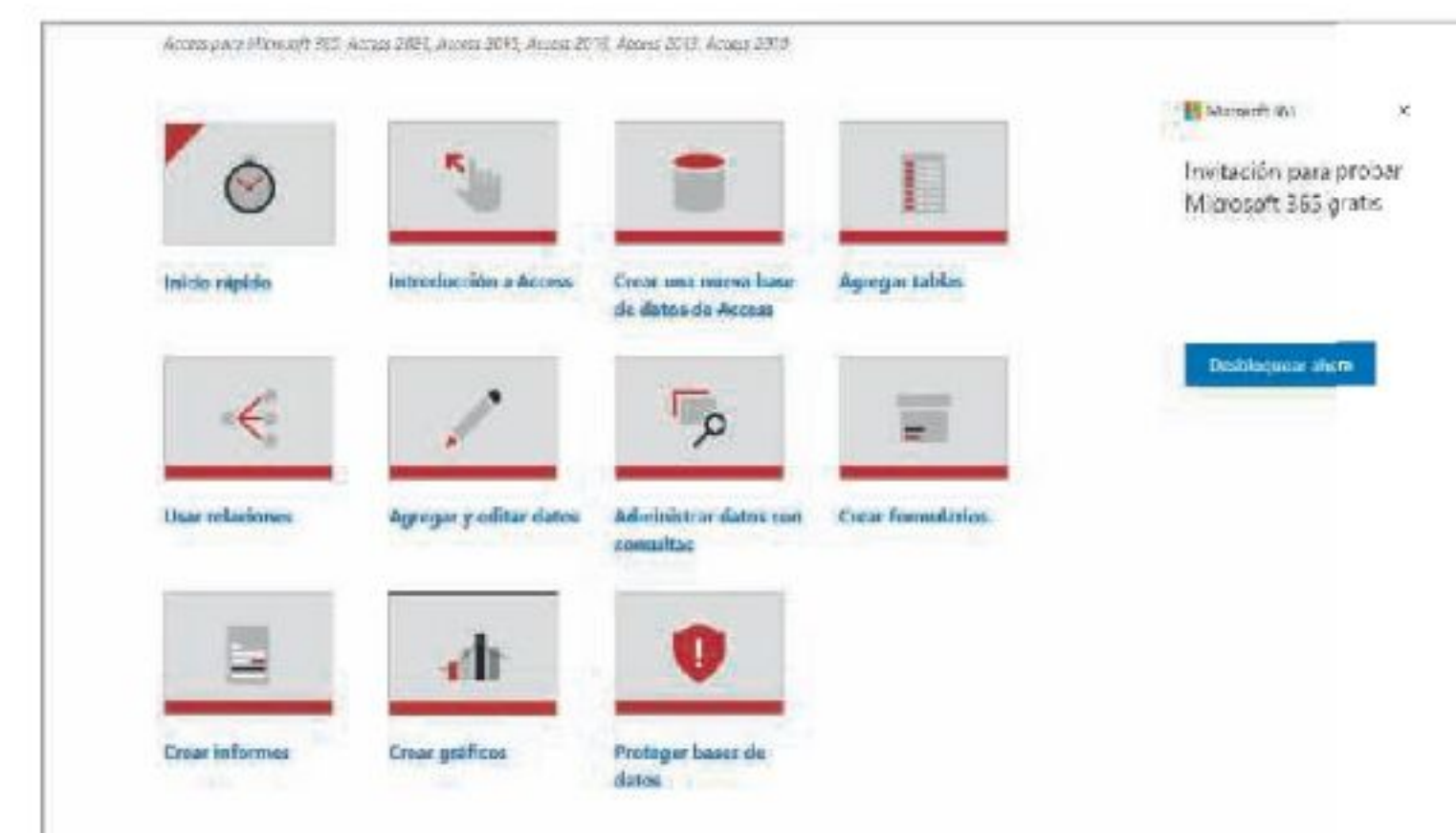


Figura 4.11. Access.

Entrando en Access vemos la pantalla que mostramos en la Figura 4.12, Base de datos en blanco.

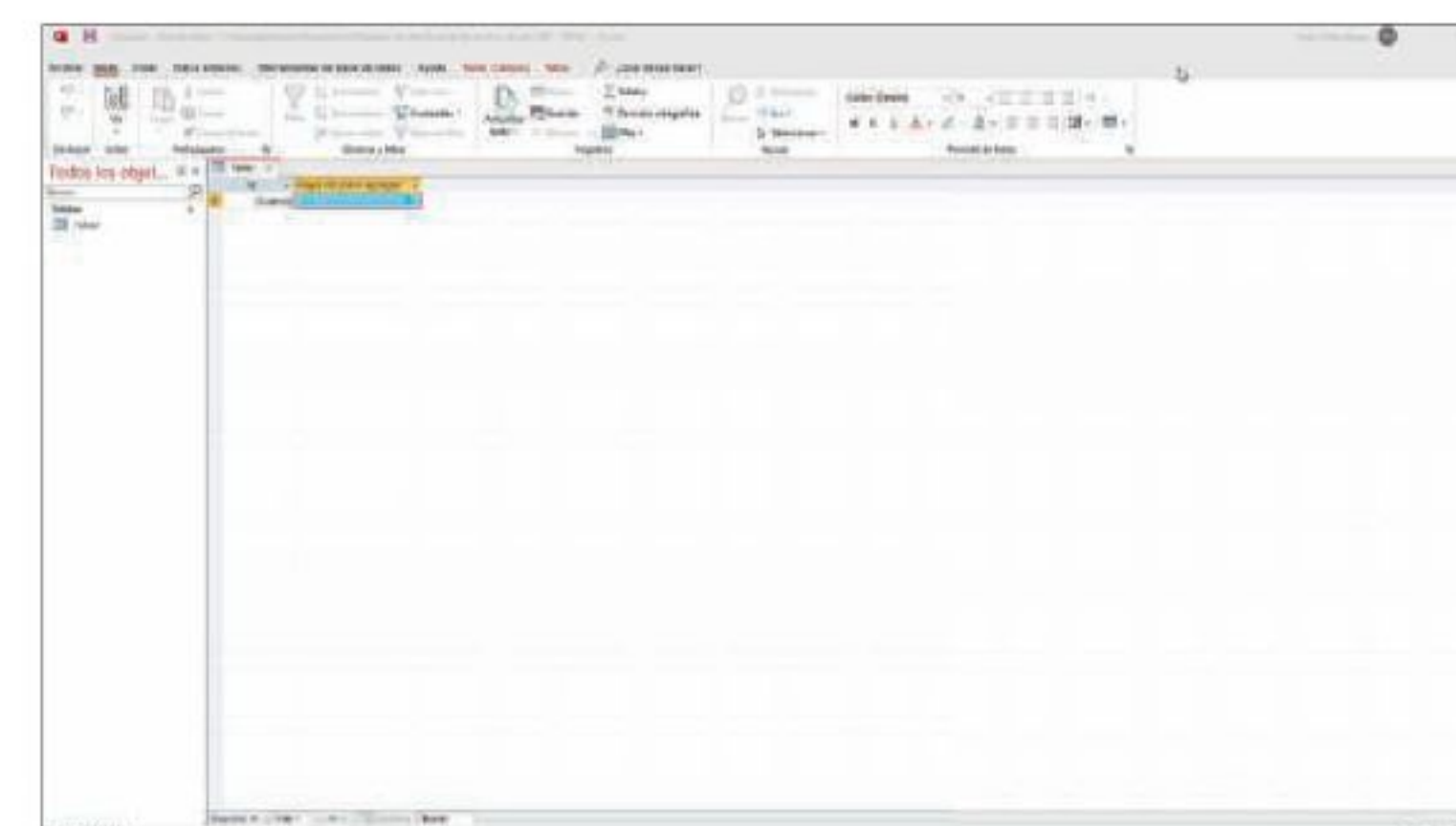


Figura 4.12. Access.

Para hacer una base de datos en Access hay que empezar definiendo los campos (datos) que vamos a utilizar y que podemos cargar de dos maneras: directamente en una tabla, que no es lo más adecuado, y mediante un formulario de entrada de datos, que es la forma correcta de actuar; hay que aprender a hacer tablas y formularios.

En esta fase del proceso de creación de una base de datos conviene saber que se puede importar, o copiar, una tabla de Excel para crear una base de datos en Access.

La forma habitual de extraer información de una base de datos es mediante consultas e informes, otras dos cosas que hay que aprender.

Antes de pasar a las actividades, recordemos que solo se aprende a manejar un programa si se trabaja con él; es un proceso de aprendizaje que requiere esfuerzo y dedicación, pero la experiencia del autor con estudiantes universitarios es que pocas personas utilizan Excel con un nivel medio o alto y muchas menos Access, por lo que usar estos programas, mejor todo el paquete de Microsoft 365, puede ser una importante ventaja a la hora de encontrar trabajo.

► ACTIVIDAD PROPUESTA 4.1

Uso de Excel

Como ya hemos indicado, Excel es una hoja de cálculo muy potente, con muchas funcionalidades, pero el uso básico es bastante sencillo. Veamos un ejemplo de la vida cotidiana.

Adela ha comprado una bicicleta estática para hacer ejercicio en su casa; la aplicación de la bicicleta registra los kilómetros recorridos, el tiempo, en minutos, y las calorías consumidas. Ha decidido llevar un registro para ver cómo progresa, si aumentan los km que recorre y las calorías que quema, el coste por caloría y por km y las calorías quemadas por km. Para ello, decide utilizar una hoja de cálculo, Excel; por cierto, la bicicleta ha costado 297 €.

Lo primero es pensar qué campos va a tener la tabla con la que se va a trabajar: fecha, km, tiempo y calorías. Veamos qué aspecto tiene la tabla, que se muestra en la Figura 4.13, con los datos del mes de marzo de 2022.

Con estos datos, haga lo siguiente:

- Calcule los km y las calorías totales del mes (sugerencia: *pestaña de inicio>Autosuma*).
- Calcule coste por km y por caloría (sugerencia: *pestaña de inicio>f_x>funciones matemáticas>cociente*).
- Calorías por km (sugerencia anterior o también se puede hacer con la tecla de dividir del teclado).
- Gráfico de calorías por día (sugerencia: *insertar>Gráficos recomendados*).

Unos cálculos sencillos y un gráfico nos dan mucha información. Sigamos practicando.

Fecha	Km	Tiempo	Cal
3/1/2022	16,77	35	481
3/2/2022	18,32	35	519
3/3/2022	18,35	35	520
3/4/2022	18,42	35	523
3/5/2022	18,32	35	519
3/6/2022	18,78	35	538
3/7/2022	18,78	35	537
3/8/2022	18,56	35	528
3/9/2022	18,24	35	516
3/10/2022	18,46	35	524

Fecha	Km	Tiempo	Cal
3/11/2022	18,48	35	525
3/12/2022	18,8	35	537
3/13/2022	19,12	35	548
3/14/2022	19,28	35	554
3/15/2022	19,07	35	546
3/16/2022	19,32	35	556
3/17/2022	19,05	35	547
3/18/2022	19,41	35	559
3/19/2022	19,68	35	568
3/20/2022	19,87	35	575
3/21/2022	19,77	35	571
3/22/2022	19,99	35	579
3/23/2022	19,99	35	578
3/24/2022	20,11	35	583
3/25/2022	19,98	35	578
3/26/2022	20,78	35	602
3/27/2022	19,83	35	573
3/28/2022	20,49	35	595
3/29/2022	20,5	35	595
3/30/2022	20,31	35	589
3/31/2022	19,53	35	563

Figura 4.13. Tabla.

► ACTIVIDAD PROPUESTA 4.2

Uso de Access

Un amigo de Adela le dice que es más cómodo procesar los datos mediante Access, con un formulario, para ir completando la tabla.

Con los datos de la tabla de la Actividad propuesta 4.1, realice una tabla en Access y un formulario para introducir los datos.

4.2. Retoque básico de imágenes

El retoque de fotografías mediante Photoshop o, de forma más burda, eliminar algo o a alguien que aparezca en la foto es algo que se realiza habitualmente en los medios, con fines no siempre lícitos.

Pero, sin llegar a esos extremos, hay muchas razones para retocar una imagen, desde el adorno de una foto para el regalo del día de la madre hasta el retoque profesional de imágenes publicitarias o simplemente como pasatiempo.

El programa más utilizado es Adobe Photoshop que, como todo el software de Adobe, es muy bueno, pero no precisamente barato, aunque ofrece la posibilidad de probarlo gratis y tiene licencias para educación a precios reducidos.

Lo recomendable para iniciarse en estos menesteres es recurrir a algún programa gratuito y dar el salto a las herramientas profesionales solamente si se necesitan.

Veamos una lista de programas y aplicaciones para retocar fotografías e imágenes:



20 programas y aplicaciones gratis para retocar fotos

Te traemos una colección con 20 programas y aplicaciones gratis para editar fotos y hacer tus retoques, ya sean rápidos y sencillos o algo más profundos. Vamos a intentar ofrecerte tanto las más populares como otras menos conocidas, y que podrían servirte de alternativa si quieres explorar en busca de nuevas herramientas.

Vamos a centrarnos sobre todo en las aplicaciones para PC, aunque también vamos a incluir algunas aplicaciones web para usar desde cualquier navegador, y otras móviles. También tendrás algunas apps para móvil y Windows adaptadas al PC, con el punto en común de tener un coste gratuito.

Darktable

Darktable es un programa de código abierto que ha sido creado para aspirar a sustituir a otros programas de pago, ofreciendo también todas las herramientas necesarias para el retoque fotográfico. Además, otra de sus grandes bazas es que es totalmente multiplataforma* y gratuito, estando disponible para Windows, macOS, FreeBSD y múltiples distribuciones de GNU/Linux.

Esta aplicación está enfocada al tratamiento de las fotos que vienen directamente de la cámara fotográfica en formato RAW, para hacer las veces de revelado digital. Sin embargo, también tiene muchas otras opciones de retoque que te pueden servir.

Fotor

Esta es una alternativa un poco diferente al resto de la lista, porque no es una aplicación o programa como la mayoría que hemos tratado, sino una aplicación web que ejecutas desde el navegador. Fotor no es una aplicación que busque darte todas las opciones del mundo, sino que está diseñada para permitirte hacer retoques rápidos con un solo click.

Por lo tanto, te ofrece varias opciones de mejoras rápidas para tus fotos, que la convierten en una herramienta rápida de utilizar. La mala noticia es que, si solo quieres retocar partes concretas de una foto, posiblemente se te quede corta. Tiene una versión gratuita y una de pago, siendo la gratis bastante completa con opciones como la de editar grupos de fotos.

GIMP

GIMP es posiblemente una de las mejores aplicaciones de edición fotográfica que te puedes encontrar. Y no solo eso, sino que es de código abierto y totalmente gratuita, lo que quiere decir que toda la comunidad puede ver cómo funciona y ayudar a solucionar fallos, y que nunca vas a tener que pagar nada por utilizarla.

Se trata de un programa pensado para ser una alternativa completa al Photoshop de pago, por lo que no le van a faltar las opciones más avanzadas para editar tus fotografías, trabajar con capas y demás. También ofrece las opciones más sencillas, filtros y



muchos otros detalles para usarla tanto para ediciones rápidas como para creaciones más complejas.

Glimpse

Glimpse es un fork de GIMP, lo que quiere decir que sus creadores han utilizado el código abierto de GIMP para crear a partir de él una aplicación derivada. Se trata de una alternativa que busca acercar su interfaz a Photoshop para que se parezca más, y que los usuarios que están acostumbrados a la aplicación de Adobe tengan más fácil el salto.

Se trata de un programa muy joven que nace tras los desencuentros con el mod de GIMP llamado PhotoGIMP, y que buscaba precisamente «photoshopizar» GIMP. Si quieres darle una oportunidad, es un proyecto que irá creciendo con el paso de los meses y la llegada de nuevas versiones.

inPixio

Cambiando un poco de tercio, inPixio es otro excelente editor gratuito de fotos con el que puedes hacer varios tipos de retoques. Pese a ser gratis, no solo te ofrece una gran cantidad de filtros, sino que también añade muchísimas opciones de edición que van desde efectos como hacer la foto antigua hasta muchas otras mejores, incluyendo recortes, ajustes en los colores y más.

Krita

Krita es un excelente programa de pintura digital diseñado especialmente para artistas que trabajan con ilustración, historietas, arte conceptual, pintura, y demás. Es una herramienta gratuita y de software libre, con versiones para Windows, Linux y macOS.

Tiene una interfaz del usuario intuitiva que no se interpone en tu trabajo, con paneles que puedes mover y personalizar para adecuarlos a tu estilo de trabajo. También cuenta con estabilizadores de pincel, paleta emergente, motores de pincel, modo de envoltura y administrador de recursos. Y evidentemente, como imaginas, también te va a servir para retocar fotografías, aunque quizá no de forma tan intuitiva.

Paintnet

Es otro de los editores de fotografía más populares y veteranos del panorama. Originalmente fue patrocinado por Microsoft, formando parte de un proyecto de algunos alumnos universitarios. Y después de eso, la herramienta empezó a volar por sí misma y a seguir evolucionando por su cuenta dentro del ámbito educativo.

Inicialmente, Paint.NET buscaba ser un sustituto del mítico Paint de Microsoft, pero con el paso de los años ha ido convirtiéndose en una herramienta mucho más completa y con opciones bastante avanzadas, como añadir capas, efectos especiales, y todo tipo de ediciones avanzadas.



Photo Pos

Este es un programa profesional que puedes bajar gratis, y que combina varias opciones gratuitas con otras de pago a la hora de permitirte retocar tus fotos. La herramienta gratuita es suficiente para la mayoría de los retoques sencillos, contando con una interfaz que busca la sencillez de uso para que no te pierdas en los menús como puede pasar con Photoshop o GIMP.

Una buena característica de esta aplicación es que si pese a sus esfuerzos te parece muy complicada de entender, también ofrece un diseño opcional para usuarios primerizos, que lo readapta todo a una estética basada en filtros. La gran limitación de esta versión gratuita es que solo puedes exportar tus fotos a una resolución máxima de 1.024×1.024 píxeles.

Photopea

Seguimos ahora con otra aplicación web. Existen una gran cantidad de editores de fotos online, pero en esta lista vamos a proponer pocos para centrarnos en las aplicaciones instalables. Sin embargo, Photopea es un editor orientado al uso profesional, una alternativa a Photoshop y GIMP, tan bueno que merece la pena mantenerlo aquí.

Para ello, cuenta con características como poder trabajar con capas y máscaras, modos de fusión para combinar capas, selecciones, y ajustes como el tono, la saturación, desenfoques o timidez. Todo lo que ofrecen los grandes, junto al resto de opciones básicas. La diferencia con otras alternativas es que tiene una interfaz muy similar a Photoshop, buscando ser una solución online para aquellos acostumbrados a trabajar con el editor de Adobe.

Photoroom

Una herramienta que tiene varias versiones, desde la versión móvil que tienes para Android, iOS o Windows 10 adaptada al escritorio, hasta una versión gratuita especialmente hecha para Windows. Es una alternativa a Snapseed y VSCO para ediciones rápidas y sencillas, con una buena colección de ajustes sencillos y presets. Más enfocada a compartir fotos en redes sociales, pero que sirve para retoques rápidos.

Photoscape

Personalmente, llevo ya varios años utilizando PhotoScape X en Windows 10, y todas las capturas que veis editadas en Xataka Basics han sido editadas con esta aplicación. Es una herramienta que tiene muchas funciones, desde su visor de fotos hasta su completo editor, centrado en las funciones básicas, pero también con varias avanzadas.

Vas a poder aplicar todo tipo de efectos de color y filtros a tus fotografías, recortes y transformaciones, añadir figuras, combinarlas y crear collages. También puedes editar varias fotos a la vez, trabajar con capas, aplicar marcos o trabajar con imágenes en RAW. Es una herramienta entre medio de las básicas y las avanzadas, que intenta ponértelo fácil.

© Ediciones Paraninfo

Photoshop Express

Photoshop Express es el hermano menor de la potente aplicación fotográfica de Adobe. No tiene tantas opciones avanzadas, pero ofrece muchas de las opciones necesarias para hacer buenas ediciones fotográficas siendo una aplicación totalmente gratuita. Eso sí, con compatibilidad reducida a archivos de cámara sin formato, y archivos con formatos JPG y PNG.

Por lo demás, la aplicación tiene una interfaz adaptada a teléfonos móviles, con elementos táctiles y de fácil acceso. Aun así, no debes preocuparte, porque además de Android e iOS, también hay una versión en la Microsoft Store para descargarlo en Windows. En todos los casos, es una aplicación gratis.

Picasart

Es uno de los más populares y completos editores de fotos para dispositivos móviles, aunque también te lo puedes encontrar en la tienda de aplicaciones de Windows para tu PC. Con su versión gratuita no solo puedes crear collages de hasta 10 imágenes, sino también puedes editar vídeos y fotos. Para ello cuentas con una galería de herramientas que te permite editar la imagen con diferentes efectos visuales, así como recortarlas a tu gusto.

La aplicación tiene diferentes proporciones prediseñadas para poder subirlas a diferentes redes sociales y webs. Puedes elegir utilizar las proporciones de Instagram, pero también crearlas para Facebook, Twitter, Pinterest o YouTube. Tampoco le faltan las herramientas básicas de edición. Tiene una versión de pago con sincronización entre dispositivos y opciones de edición más avanzadas.

Pinta

Esta herramienta es una alternativa a Paint de código abierto, multiplataforma, y que también es gratuita. Eso sí, pese a ser una competencia directa de Paint, que no ha entrado en la lista por sus limitaciones, tiene algunas opciones de más con las que puedes hacer algunos retoques básicos de fotografía.

Además de las opciones de dibujo clásicas de Paint, Pinta también incorpora ajustes y efectos para la edición fotográfica, así como múltiples capas para trabajar, un historial completo de cambios, y diferentes visualizaciones para la interfaz. Está disponible tanto para GNU/Linux como para Windows, macOS y FreeBSD.

Pixlr

Es otra potente herramienta web de edición fotográfica. En su web vas a encontrarte dos tipos de producto, un Pixlr E centrado para la edición más profesional fotográfica y con soporte hasta para imágenes en 4K, y un Pixlr X para las ediciones rápidas con opciones más sencillas para no perder mucho tiempo.

© Ediciones Paraninfo

**Polarr**

Polarr es una aplicación que se hizo popular cuando su versión web fue de las primeras en ofrecer soporte para el revelado digital de archivos RAW. Pero también es un programa gratuito para Windows que puedes descargar en la Microsoft Store, ofreciéndote toda su potencia de forma nativa para no depender de tu conexión.

Es una herramienta bastante completa, que te permite editar por capas y tiene su sistema de filtros para hacer ajustes rápidos en tus fotos. También tiene opciones avanzadas de edición, con funciones de retoque, histograma, efectos, y todas las herramientas básicas que caben esperar en un programa como este.

Rawtherapee

Es una aplicación que busca ser una alternativa para Darktable en el revelado digital de las fotos, y que también es gratuita y de código abierto, teniendo versiones para GNU/Linux, y las versiones de 64 bits de macOS y Windows 10. Como su nombre indica, ha sido pensada para la edición de fotos en formato RAW, aunque también sirve para el resto de los formatos fotográficos comunes.

Con su motor fotográfico vas a poder realizar completas gestiones en el color de tus fotos, y también en elementos como su tonalidad y su exposición. La herramienta intenta mantener el equilibrio de ofrecer una interfaz que sirva tanto para los usuarios expertos como para los primerizos en este tipo de edición fotográfica.

Snapseed

Se trata de otra aplicación fotográfica enfocada a los dispositivos móviles. De hecho, lleva años siendo una de las mejores en este campo, sobre todo por ofrecer una interfaz por gestos sencilla de utilizar junto a un buen elenco de herramientas. Todo funciona a través de deslizar el dedo para cambiar de ajustes y cambiar el nivel de cada ajuste.

Con Snapseed vas a poder desde hacer sencillos recortes hasta ajustes avanzados como modificar la orientación de una cara o borrar objetos. Su principal baza es que es totalmente gratis, sin anuncios ni sorpresas. Por lo tanto, tienes aquí ya todo lo que vayas a necesitar para editar fotos desde las limitaciones del tamaño de una pantalla de móvil.

VSCO

A medias entre red social y editor de fotos para smartphones, VSCO es una de esas alternativas que no puede faltarte en el móvil, sobre todo si eres usuario de redes como Instagram. Es una app especializada en permitirte realizar ediciones rápidas que luego puedes compartir rápidamente en redes sociales.

Por una parte, la app ofrece las clásicas herramientas de edición básicas presentes en todo este tipo de aplicaciones, y por la otra, tiene una gran selección de ajustes



preestablecidos y efectos listos para ser utilizados. Además, también puedes crear plantillas basadas en tus propias configuraciones personalizadas poder reutilizarlas rápidamente. Tiene una versión de pago con todavía más preconfiguraciones y filtros.

Windows Fotos

Y vamos a terminar con el visor fotográfico que viene preinstalado en Windows 10, y que es gratuito para todos los usuarios del sistema operativo. Fotos, tiene varias herramientas para retoques rápidos para tus fotos. No son herramientas muy avanzadas, básicamente filtros y algunos ajustes rápidos, pero para apaños rápidos puede serte útil saber que no necesitas instalar nada para lo esencial.

Además de las ediciones rápidas, Fotos también tiene otras funciones como la de dibujar sobre tu foto, añadir efectos 3D como lluvia o confeti, texto animado o la posibilidad de crear vídeos con música⁵.

Cuando buscamos información en la red y recurrimos a las fuentes adecuadas, la cantidad y calidad de la información obtenida puede resultar abrumadora; no hay más que ver la lista anterior.

El objetivo es proporcionar al lector la información necesaria para que conozca los recursos disponibles y que pueda trabajar con los distintos programas para elegir el que más se adecue a sus necesidades. Hay más recursos, pero, la lista de «los mejores» sirve para iniciarnos en el tema.

Si no vamos a hacer un uso profesional del retoque de imágenes, la recomendación del autor es empezar por Windows Fotos y seguir con Photoshop Express; es una buena forma de iniciarnos en el retoque de imágenes y puede servir como introducción a Photoshop si fuera necesario, pero no está de más conocer el resto de los programas.

En la Figura 4.14 mostramos una fotografía de la carpeta *Imágenes* (que es como se denomina Fotos en Windows 10) con el desplegable en el que aparecen las distintas posibilidades que ofrece el programa para el retoque de imágenes. No nos olvidemos de los demás iconos que vemos en la imagen. Son operaciones muy sencillas, pero sirven para iniciarse en este campo.

Para trabajar con Photoshop Express (Figura 4.15), debemos buscar en internet «Photoshop Express» y seguir las instrucciones. Es un poco farragoso, pero tiene muchas opciones y es una forma de progresar en el retoque de imágenes. Para retocar una imagen hay que trabajar con los iconos de la izquierda.

⁵ <https://www.xataka.com/basics/21-programas-aplicaciones-gratis-para-retocar-fotos>



Figura 4.14. Imágenes.

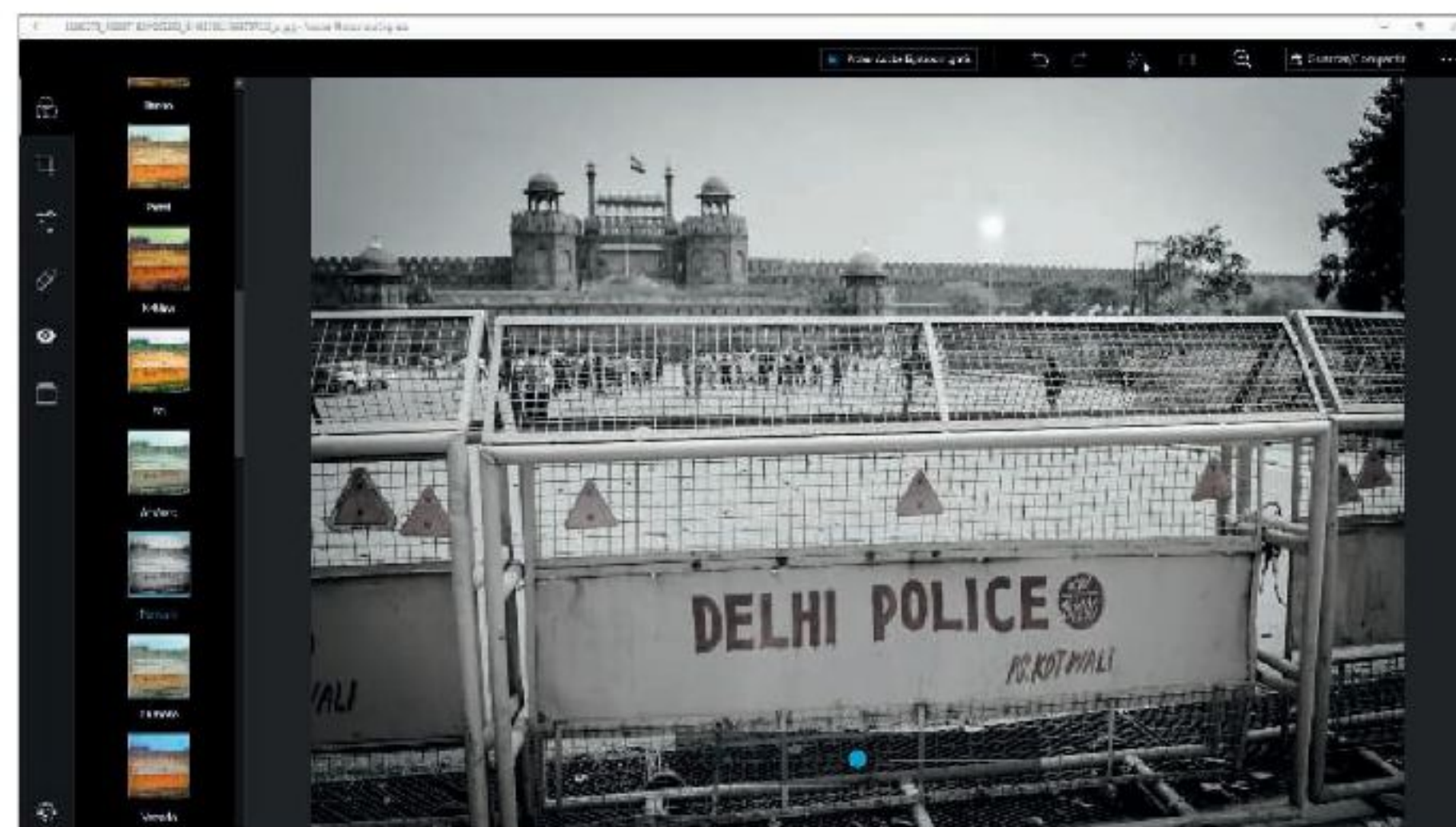


Figura 4.15. Photoshop Express.

► ACTIVIDAD PROPUESTA 4.3

Retoque de imágenes

Elija una fotografía y trabaje con ella en Imágenes (Fotos) de Windows y con Photoshop Express. Le recomendamos que vaya tocando en todos los iconos y vea qué puede hacer y lo que sucede cuando lo hace.

© Ediciones Paraninfo

4.3. Derechos de autor y licencias

Antes de comentar el uso de la información que hay en la red, veamos unas definiciones extraídas del diccionario de la RAE.

Propiedad intelectual, *derecho de explotación exclusiva sobre las obras literarias o artísticas, que la ley reconoce a su autor durante un cierto plazo*⁶.

Derechos de autor, *derecho que la ley reconoce al autor de una obra intelectual o artística para autorizar su reproducción y participar en los beneficios que esta genere*⁷.

Licencia, *autorización que se concede para explotar con fines industriales o comerciales una patente, marca o derecho*⁸.

Dos definiciones más:

Copyright, *el símbolo del Copyright © informa al público que una obra es original y que su uso, reproducción, transformación, publicación... está sujeta a derechos de autor*⁹.

Copyleft, *es un movimiento social y cultural que, frente al lema tradicional del Copyright de «todos los derechos reservados», propone la opción de compartir y reutilizar las obras impulsando el uso de licencias libres, con las que el autor se puede reservar «algunos derechos»*¹⁰.

En el contexto de la red, el concepto de «obra literaria o artística» se puede hacer extensivo a la información publicada por personas o instituciones y a los contenidos disponibles para su uso y disfrute.

Propiedad intelectual, derechos de autor y copyright conforman el esquema que define la manera en la que un autor pone a disposición del público, por ejemplo, un libro; es habitual y se basa en la justa contraprestación al trabajo del autor y al posterior proceso de edición, impresión, etc. Normalmente este tipo de obras no son gratuitas, se venden, sea en papel o en formato digital.

Este esquema es aplicable a la música, las producciones audiovisuales, los artículos científicos, la prensa escrita, etc.; es decir, a toda aquella información sujeta a propiedad intelectual.

La irrupción de las TIC, y en especial de internet, han producido un cambio total en la forma de poner contenidos a disposición del público, lo que ha generado toda una corriente de pensamiento que aboga por la libertad total en la red; libertad que, según esta tendencia, debería dar lugar a que todos los contenidos de la red fueran libres.

⁶ <https://dle.rae.es>

⁷ <https://dle.rae.es>

⁸ <https://dle.rae.es>

⁹ <https://www.mondragon.edu/es/web/biblioteca/propiedad-intelectual#titulo1>

¹⁰ <https://www.mondragon.edu/es/web/biblioteca/propiedad-intelectual#titulo1>

© Ediciones Paraninfo



Actualmente, hay muchos contenidos libres en la red y mucha de la información que consultamos es de acceso libre. También hay una gran cantidad de software libre, pero es el autor, persona física o jurídica, el que decide que sus obras sean libres y gratuitas; él es el único que tiene la potestad de regalar su obra, el fruto de su trabajo; los usuarios no deben arrogarse ese derecho.

Los derechos de autor están regulados por la Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que se puede consultar en la página del BOE¹¹.

No respetar la propiedad intelectual y, por tanto, conculcar los derechos de autor, en el contexto que nos ocupa, recibe el nombre de piratería y está penado por la ley. Recordemos los muchos cierres de páginas de descargas que se dieron en su día.

Para conocer el punto de vista de los autores se recomienda visitar el sitio de CEDRO:

Somos el Centro Español de Derechos Reprográficos (CEDRO), la asociación sin ánimo de lucro de autores y editores de libros, revistas, periódicos y partituras, editadas en cualquier medio y soporte.

Nos encargamos de defender y gestionar de forma colectiva los derechos de propiedad intelectual que se derivan de la utilización secundaria (reproducción, distribución, comunicación pública y transformación) de estas publicaciones.

En 1988 fuimos autorizados por el Ministerio de Cultura para llevar a cabo esta actividad.

Nuestra misión es representar y defender los legítimos intereses de autores y editores de libros y publicaciones periódicas, facilitando y promoviendo el uso legal de sus obras¹².

Pero el uso de las TIC y de internet como medio de difundir información ha dado lugar a situaciones no previstas en su día; como en muchas ocasiones, la tecnología tira de la ley y la supera; recordemos el concepto de Copyleft, que propone la opción de compartir y reutilizar las obras impulsando el uso de licencias libres, con las que el autor se puede reservar «algunos derechos».

Como vemos, el concepto de copyleft aboga por flexibilizar el uso de los contenidos, de modo que se respeten aquellos derechos que el autor considera oportunos:

¹¹ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-11404

¹² <https://www.cedro.org/inicio>



¿Qué son las licencias libres?

Son licencias que defienden un uso más libre y compartido de las obras y otorgan a los y las autoras la posibilidad de no ejercer todos los derechos de explotación previstos en la ley de propiedad intelectual: pueden establecer sus propios límites permitiendo a los autores/as tener un mayor control sobre los derechos de sus obras y una gestión más sencilla. De esta manera facilitan a los usuarios un mejor acceso a las obras y un uso de estas con menos restricciones.

Entre las licencias libres existen también unas licencias denominadas Copyleft, muy utilizadas en informática, que garantizan el derecho de cualquier usuario a utilizar, modificar y redistribuir una obra siempre que comparta las obras derivadas que vaya a crear con una licencia igual o equivalente.

A nivel general las licencias libres más utilizadas actualmente para obras de creación variadas son las llamadas licencias Creative Commons.

¿Qué son las licencias creative commons?

Las licencias CC permiten a los autores y autoras ceder, bajo ciertas condiciones, algunos de los derechos sobre sus obras y mantener otra parte de estos¹³.

Creative Commons es una organización no gubernamental y sin ánimo de lucro que ofrece, a autores y creadores, licencias y herramientas libres con las que gestionar los derechos sobre sus obras y poder compartir, de forma sencilla, su trabajo y su conocimiento.

Las CC se pueden aplicar a cualquier tipo de contenidos creativos, incluyendo recursos educativos, música, fotografías, bases de datos, información pública y gubernamental...

Cada licencia CC detalla qué derechos cede el autor, bajo qué condiciones y qué pueden hacer los usuarios con la obra, sobre todo en el caso de que quieran volver a publicarla o modificarla. No existe una única licencia, sino que, a voluntad del autor, se pueden hacer diferentes combinaciones. En todas ellas es imprescindible el reconocimiento de la autoría de la obra.

Condiciones básicas

Estas son las cuatro condiciones básicas que se combinan en las licencias CC: Reconocimiento, Uso No comercial, No Derivados y Compartir Igual.

Reconocimiento-Atribución (BY), por el que el autor permite que otros copien, distribuyan y muestren su obra (u obras derivadas de la misma) siempre que citen su autoría.

¹³ <https://www.mondragon.edu/es/web/biblioteca/propiedad-intelectual#titulo1>



Uso No comercial-Non Commercial (NC), el autor limita la explotación de la obra a usos no comerciales, por lo que permite que otros copien, distribuyan y muestren su obra (u obras derivadas de la misma) sin fines comerciales.

No Derivados-No Derivatives (ND), permite reutilizar la obra, pero no que la obra sea modificada, ni que se creen obras derivadas de la original. El autor permite que otros copien, distribuyan y muestren su obra como fue creada, sin que se realicen modificaciones.

Compartir Igual-Share Alike (SA), que permite reutilizar y modificar la obra, pero incluye la condición de que las obras derivadas que se creen sean publicadas bajo la misma licencia. El autor permite que otros distribuyan trabajos derivados de su obra siempre que lo hagan bajo una licencia igual a la de la obra original¹⁴.

¿Cuál es la conclusión?

La conclusión de lo expuesto en este apartado es que es el autor el único que puede decidir cómo publicar su obra y los demás tenemos que respetar esa decisión, dentro de los márgenes definidos por la ley.

Para ampliar información y tener una visión de conjunto, recomendamos visitar el sitio sobre derechos de autor y propiedad intelectual de la Universidad de Mondragón¹⁵.

► ACTIVIDAD PROPUESTA 4.4

Licencias CC

Vaya a Wikipedia y vea el tipo de licencia CC bajo la que se publica este wiki.

► ACTIVIDAD PROPUESTA 4.5

Copyright

Si es usted docente, le puede interesar saber cómo puede utilizar material sometido a copyright sin comprar, por ejemplo, el libro.

Busque información.

¹⁴ <https://creativecommons.org>

¹⁵ <https://www.mondragon.edu/es/web/biblioteca/propiedad-intelectual#titulo1>



ACTIVIDADES FINALES

DE COMPROBACIÓN

4.1. Es recomendable introducir los datos en una base de datos mediante un formulario:

- a. Falso.
- b. No se puede hacer así.
- c. Verdadero.
- d. No, es muy farragoso.

4.2. Photoshop Express:

- a. Es de Google.
- b. Es de Microsoft.
- c. Es de Adobe.
- d. Es una extensión de Mozilla.

4.3. Derecho que la ley reconoce al autor de una obra intelectual o artística para autorizar su reproducción y participar en los beneficios que esta genere:

- a. Derecho de autor.
- b. Muchas de propiedad.
- c. Derecho de publicación.
- d. Derecho de uso y disfrute.

4.4. Automatización, mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas:

- a. Domótica.
- b. Informacionática.
- c. Electromática.
- d. Ofimática.

4.5. Los derechos de autor están regulados por:

- a. La Ley de Propiedad Intelectual.
- b. El Código de Comercio.
- c. Los derechos de autorización.
- d. Las tres respuestas anteriores son correctas.

4.6. Licencias que otorgan a los autores la posibilidad de no ejercer todos los derechos de explotación previstos en la ley de propiedad intelectual:

- a. Wikis.
- b. Comunidades.
- c. Ciberlicencias.
- d. Licencias libres.

**4.7. Las cuatro condiciones de las licencias CC son:**

- a. No Reconocimiento, Uso comercial, No Derivados y Compartir Igual.
- b. Reconocimiento, Uso No comercial, No Derivados y No Compartir.
- c. Reconocimiento, Uso comercial, Derivados y Compartir Igual.
- d. Reconocimiento, Uso No comercial, No Derivados y Compartir Igual.

4.8. El autor es el único que puede definir bajo qué licencia se explota su obra:

- a. Depende del tipo de obra.
- b. Depende del tipo de autor.
- c. Verdadero.
- d. Falso.

4.9. Autorización que se concede para explotar con fines industriales o comerciales una patente, marca o derecho:

- a. Comunidad de uso.
- b. Pirateo.
- c. Permiso.
- d. Licencia.

4.10. Programa que opera con tablas formadas por filas y columnas de celdas que contienen información numérica y fórmulas o texto, y las presenta en una pantalla:

- a. Cálculo digital.
- b. Automatización digital.
- c. Calcumática.
- d. Hoja de cálculo.

4.11. Derecho de explotación exclusiva sobre las obras literarias o artísticas, que la ley reconoce a su autor durante un cierto plazo:

- a. No existe tal derecho.
- b. Propiedad intelectual.
- c. Derecho de publicación.
- d. Propiedad artística.

4.12. Apache OpenOffice:

- a. Paquete de ofimática de pago.
- b. Paquete de ofimática Google.
- c. Paquete de ofimática de Apple.
- d. Paquete de ofimática libre.

4.13. Programas para retocar imágenes:

- a. GIMP.
- b. inPixio.
- c. Fotor.
- d. Las tres respuestas anteriores son correctas.

4.14. Windows Fotos:

- a. Solo sirve para guardar fotografías.
- b. También aparece como *Imágenes* en el explorador.
- c. No permite retocar imágenes.
- d. Las tres respuestas anteriores son correctas.

4.15. Conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información:

- a. Blog.
- b. Wiki.
- c. Foro.
- d. Base de datos.

DE APLICACIÓN**4.16.** Realice la Actividad propuesta 4.1 con la Hoja de cálculo de Google Docs.**4.17.** Realice la Actividad propuesta 4.1 con la Hoja de cálculo de Apache OpenOffice.**4.18.** Realice la Actividad propuesta 4.1 con la Hoja de cálculo de LibreOffice.**4.19.** Tras hacer la Actividad propuesta 4.1 con las cuatro hojas de cálculo citadas, ¿cuál le parece mejor?**4.20.** Realice la Actividad propuesta 4.2 con la Base de datos de Apache OpenOffice.**4.21.** Realice la Actividad propuesta 4.2 con la Base de datos de LibreOffice.**4.22.** Tras hacer la Actividad propuesta 4.2 con las tres bases de datos citadas, ¿cuál le parece mejor?**4.23.** Elija un programa de retoque de imágenes que no sea ni Fotos ni Photoshop Express y retoque una fotografía cualquiera. ¿Qué le parece?**4.24.** Lea detenidamente la información sobre propiedad intelectual, derechos de autor, etc. de la Universidad de Mondragón que se cita en el Apartado 4.3. ¿Cuáles son sus conclusiones?**4.25.** Visite el sitio de Creative Commons para familiarizarse con este tipo de licencias y conocer lo que pretenden.**4.26.** Busque noticias de prensa sobre la defensa, o vulneraciones, de la propiedad intelectual, léalas y saque sus propias conclusiones.



- 4.27. Entre en la página de la Sociedad de Autores (SGAE), vea la información sobre derechos de autor y similares y saque sus propias conclusiones.
- 4.28. Busque información sobre el pirateo en internet. Se trata de hacerse una idea de la situación actual y lo que cuesta.
- 4.29. Busque y visite páginas de descarga tipo eMule; esta tiene un blog, léalo. ¿Utiliza sitios de este tipo? ¿Qué le parecen?
- 4.30. Tras estudiar la Unidad 4 y hacer las actividades debe tener una opinión sobre qué tipo de contenidos son o, en su opinión, deberían ser libres y cuáles no. Reflexione sobre ello, procurando tener en cuenta distintos puntos de vista.

5



Seguridad

En la red hay amenazas de muchos tipos, que van desde la «simple» molestia, a veces no tan simple, hasta las suplantaciones de identidad, el robo de información y otras; lo más importante es ser prudente, pero no siempre basta con actuar con cuidado y sensatez.

En esta unidad comentamos las herramientas de las que disponemos para proteger nuestros equipos, la información que contienen y la que gestionan.

Indicamos la forma de proteger los dispositivos, los ordenadores y los móviles o las tabletas, y la red a la que, en muchas ocasiones, están conectados.

Contenido

- 5.1. Protección del ordenador
- 5.2. Protección del dispositivo móvil
- 5.3. Protección de la red de datos

5.1. Protección del ordenador

La protección del ordenador, y de los dispositivos en general, se puede tratar desde dos puntos de vista: la protección del hardware, que implica evitar daños de cualquier tipo que puedan alterar el funcionamiento del equipo causando pérdidas o deterioros en la información, y la protección frente a amenazas externas al usuario causadas por distintos tipos de software, cuya finalidad suele ir más allá del mero daño y que, en muchas ocasiones, tiene propósitos delictivos.

La protección del hardware requiere evitar golpes, temperaturas excesivamente altas o bajas, contacto con sustancias inadecuadas, variaciones anormales del suministro eléctrico, etc.; en general, requiere seguir las instrucciones del fabricante del equipo y asegurar un suministro eléctrico correcto cuando el equipo esté conectado a la red eléctrica.

Dentro de esta categoría, podríamos incluir el uso de periféricos que tengan las características adecuadas para un correcto funcionamiento con el equipo.

No hay que olvidar las actualizaciones del software: hay que insistir en la conveniencia de trabajar con las últimas versiones y no solo por cuestiones de seguridad.

Pero, aunque se hayan tomado todas las medidas para el óptimo funcionamiento del equipo, estamos expuestos a amenazas externas, tanto procedentes de la red como de los dispositivos que podamos conectar a nuestros equipos, cualquiera que sea la forma de conexión.

Lo que vamos a comentar a continuación es cómo prevenir este tipo de amenazas.

Pero antes, veamos una serie de definiciones:

ARGOT TÉCNICO

- **Ciberseguridad:** *la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio.*

Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos¹.

¹ https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

- **Virus:** *programa introducido subrepticamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada².*
- **Malware:** *software malicioso³.*
- **Antivirus:** *dicho de un programa: que detecta la presencia de virus y puede neutralizar sus efectos⁴.*
- **Antimalware,** *el antimalware es un programa diseñado para detectar y eliminar un software malicioso que ha entrado en el sistema de un dispositivo informático para causar un daño específico⁵.*
- **Firewall (cortafuegos):** *un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red, entrante y saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.*

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas, en las que se puede confiar, y redes externas que no son de confianza, como internet.

Un firewall puede ser hardware, software o ambos⁶.

Como vemos, el concepto de malware es más amplio que el de virus y, por tanto, la función del antimalware es más general que la del antivirus.

A la hora de revisar la protección de nuestros dispositivos hay que conocer la protección que ofrece el sistema operativo que estemos utilizando, pues los SO suelen tener un determinado nivel de protección.

² <https://dle.rae.es/virus?m=form>

³ <https://es.malwarebytes.com/malware>

⁴ <https://dle.rae.es/antivirus?m=form>

⁵ <https://estafados.red/que-es-antimalware/#:~:text=Qué%20Es%20ANTIMALWARE%2C%20Tipos%20Y%20Ventajas%20de%20Proteger,Conclusión%3A%20Protégete%20con%20un%20antimalware%20en%20Internet.%20>

⁶ https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html



Figura 5.1. Ciberseguridad.

5.1.1. Antivirus o antimalware

En primer lugar, comentaremos los programas comerciales, tanto los gratuitos como los de pago, que requieren instalación en el dispositivo; en algunos casos, vienen instalados de fábrica, pero son programas ajenos al ordenador.

Después, revisaremos la protección que ofrecen los sistemas operativos.

Hay que tener en cuenta que los programas comúnmente denominados antivirus suelen ser antimalware, por lo que, a la hora de elegir uno, no solo hay que considerar la protección contra virus sino contra diversos tipos de software malicioso.



Figura 5.2. Antivirus.

Veamos la opinión de los expertos, con información actualizada en mayo de 2022:

Mejor antivirus Windows 10 en 2022

¿Cuáles son los mejores antivirus que podemos usar? Según los datos publicados por AV-Test nos muestran que varios antivirus consiguieron la calificación «Top Product», pero no todos ellos cuentan con 6 puntos en todas las categorías. Ten en cuenta que los análisis se realizan de forma periódica por lo que el porcentaje puede no coincidir entre los que aparezcan en el texto y los que aparezcan en el análisis en el momento de la consulta, pero siempre será muy similar y el porcentaje de diferencia de un mes a otro será prácticamente insignificante. Ante la misma puntuación podrás elegir el que más te guste según su interfaz, sus funciones o incluso si tienes acceso gratuito a cualquier otro según tu compra, etcétera.

AhnLab V3 Internet Security 9.0 - 18 puntos

Según el análisis realizado sobre el antivirus AhnLab V3 Internet Security 9.0 podemos decir que es uno de los más recomendables y con altas puntuaciones en todas las categorías. Consigue la máxima puntuación en todos los apartados posibles.

Las valoraciones globales de este antivirus son de 6 sobre 6 en todos los aspectos, lo que se considera que es un producto TOP considerado por el test. Uno de los únicos que consigue la máxima puntuación en todos los apartados y totalmente recomendable.

Avira Antivirus Pro 15.0 - 16,5 puntos

Avira era uno de los mejores antivirus según los datos registrados a principios del año 2022, pero bajó en cuanto a calidad en los análisis de junio y mayo haciendo que su puntuación pasase de ser la mejor a ser algo inferior. Fallos puntuales no hacen que consiga la excelencia en la protección contra ataques de día 0 provenientes de internet y tampoco el 100 % de protección en detección de malware. Aun así, una opción recomendable.

BitDefender Internet Security 24.0 - 17,5 puntos

Un clásico entre los antivirus que cuenta con varias opciones de uso según queramos utilizarlo para el hogar o para empresa, por ejemplo. BitDefender cuenta con protección para dispositivos y no solo para PC sino también protege Mac, dispositivos móviles o incluso tiene soluciones para hogares inteligentes.

Bullguard Internet Security 20.00 - 17 puntos

Bullguard es un antivirus de pago pero que podemos descargar de gorma gratuita para probar su protección durante 30 días sin ningún coste. Después, debemos pagar. Tiene todo tipo de funciones, opciones para hacer copias de seguridad, cortafuegos o antivirus y hay varios paquetes disponibles en función de lo que necesitemos o lo que nos preocupe. Es uno de los antivirus considerados como TOP.

**ESET Internet Security 13.1 y 13.2 - 17.5 puntos**

Uno de los más conocidos, habituales y recomendables. ESET también saca sobresaliente en el test mencionado y tiene varios paquetes diferentes para el hogar, para empresas. Tiene protección multidispositivo con opciones y herramientas como almacenamiento de contraseñas, seguridad en compras online, cifrado de datos y archivos, protección en la red wifi, etcétera.

F-Secure SAFE 23 - 17,5 puntos

F-Secure está considerado como otro de los productos «top» por parte de este test y nos ofrece protección total en línea. Es de pago, pero cuenta con versión completa gratis durante 30 días en la que no solo proteges tu ordenador con Windows sino todo tipo de dispositivos quedan protegidos frente a virus y ransomware, asegurando compras seguras o con control parental.

McAfee Total Protection 23 - 17,5 puntos

McAfee Total Protection tiene un precio de unos cuarenta euros al año en el paquete Hogar y promete proteger a toda la familia. Avisa en caso de virus, malware, spyware o ransomware y ofrece protección de privacidad en varios niveles. Por ejemplo, destruye archivos confidenciales, elimina cookies... Hay opción para contratar el antivirus para solo un dispositivo o para varios.

Kaspersky Internet Security 20 - 18.0 puntos

Es uno de los antivirus para Windows 10 que seguro que te suena con todo tipo de productos disponibles. Ha sido galardonado por múltiples empresas de seguridad e incluye protección para ordenadores Windows, pero también paquetes con seguridad para ordenador, teléfono y móvil. Se incluyen funciones como una VPN gratuita, pagos seguros y transacciones por internet sin riesgos, protección para webcam, antivirus, anti pirateo.

NortonLifeLock Norton 360 22.20 - 18.0 puntos

Norton es otro de los considerados por AV Test como productos TOP o mejores antivirus para Windows con la nota máxima que se puede conseguir en el sistema de puntuación. Norton 360 cuenta con planes de diferentes tipos e incluso un plan específico para gamers. Añaden control parental, protección a través de VPN, copias de seguridad en la nube, firewall inteligente o protección contra amenazas en tiempo real.

Trend Micro Internet Security 16.0 - 17.5 puntos

Quizás este antivirus no es el que tiene más nombre a día de hoy, pero viene de una de las compañías con más historia en la seguridad informática como es Trend Micro, compañía mitad japonesa mitad norteamericana. Este software está indicado especialmente para actuar de escudo de los ordenadores de nuestros hogares, al contrario de otros que

pueden ser más idóneos para un ámbito empresarial. Sus tecnologías propias de detección, escaneo y eliminación son muy efectivas, y además posee un control parental que bloqueará webs sensibles para los menores de la casa y permitirá configurar las horas de acceso a internet que queramos. Su funcionamiento está muy bien optimizado, por lo que es ideal para aquellos ordenadores que tienen un hardware no tan actualizado.

VIPRE AdvancedSecurity 11.0 - 17.5 puntos

VIPRE AdvancedSecurity es un antivirus que va muy en la línea del anterior, ya que está pensando especialmente para ordenadores de casa que no posean un hardware muy potente, puesto que sus responsables lo han optimizado al máximo para ello. La misma herramienta incluye otros servicios muy útiles como por ejemplo un completo buscador en nuestro ordenador o una función que borrará archivos muy antiguos que tengamos almacenados. Tanto su interfaz como su proceso de instalación es de lo más sencillo, aunque es cierto que esta es algo lenta en comparación a los otros antivirus que tenemos en la misma lista. Además, parece que no está siendo actualizada con la frecuencia que debería, por lo que el malware más reciente podría saltárselo y afectar a nuestro ordenador⁷.

A cada programa se le ha asignado una puntuación; veamos cuál es el criterio para calificarlos:

¿Cómo se analizan los antivirus?

Como ya os hemos explicado, AV-Test es una organización independiente que publica análisis de los principales antivirus para Windows y Android según diferentes criterios. Gracias a su estudio cada determinado mes podemos saber qué antivirus es el mejor, cuál ha sido renovado con buenas funciones de seguridad y cuál es fiable para poder encontrar todo tipo de malware. AV Test nos permite tener información actualizada, reciente. Todos los meses tenemos novedades para diferentes plataformas por parte de esta empresa con sede en Magdeburgo (Alemania). Llevan más de 15 años dedicados a esto, algo que no evita las suspicacias de usuarios y fabricantes (como en cualquier otro terreno) Aun así, sus pruebas son concienzudas y utilizan una metodología a la que se le pueden poner pocas pegas.

AV-Test dispone de laboratorios de prueba equipados con más de 200 puestos de trabajo idénticos y más de 200 servidores con una capacidad superior de 2.500 terabytes para procesar y almacenar una de las bases de datos de malware más grandes del mundo. En el apartado Windows, el que nos ocupa ahora, se someten los antivirus a varias pruebas diferentes:

Protección: Comprueban el nivel de protección frente al malware más actual (real-world test), así como frente a programas maliciosos muy comunes. Como explican desde la propia web, «contiene los resultados de las pruebas relativas a la protección contra malware y otros ataques».

⁷ <https://www.adslzone.net/esenciales/windows-10/mejores-antivirus-windows-10>



Rendimiento: Miden el rendimiento del ordenador, por ejemplo, al acceder a páginas web, descargar programas y otros escenarios de prueba que reflejan el uso diario. Aquí vemos el impacto o ralentización que genera el programa.

Usabilidad: Comprobación de en qué medida el uso de los productos probados limita la usabilidad mediante falsas alarmas, en caso de existir. O si hay posibles limitaciones en el uso de internet derivadas del uso de los diferentes productos.

Funciones y extras: Además, se informa acerca de la selección de funciones de protección adicionales si existen.

Según los análisis relacionados por AV Test os antivirus para Windows 10 pueden conseguir un máximo de 6 puntos por categoría. Una solución que no tenga los 6 puntos no es un mal antivirus, pero sí es posible que tenga problemas en un apartado en concreto que le impidan rendir al máximo como otras alternativas. En cualquier caso, podemos ver el análisis en profundidad.

AV-Test otorga la calificación «Top Product» a los mejores productos analizados en esa ocasión, pero eso no implica que todos tengan 6 puntos en las 3 categorías. Solemos tener productos top con 5,5 puntos siempre y cuando compensen con el resto de las puntuaciones. Sin embargo, siempre intentaremos priorizar a los que tienen mejor puntuación y podemos comparar unos con otros en función de los posibles fallos. Lo explican desde la página web. Para Windows los productos que consiguen el premio TOP Product son productos a partir de una puntuación total de 17,5 puntos siendo la máxima 18 puntos. Cada categoría tiene seis puntos y la publicación de los análisis es bimensual, aunque la periodicidad de la prueba es mensual. Para conseguir el sello AV-TEST (no top, sino el sello que los hace ser fiables) es necesario un mínimo de diez puntos en total en Windows.

La cosa cambia en otros sistemas operativos porque en el caso de MacOS la periodicidad es semestral y también la publicación, aunque las categorías se mantienen y también los puntos mínimos para la concesión del sello. En Android la publicación es bimensual y la periodicidad de la prueba. Se mantienen los seis puntos por categoría máximos, la concesión del sello con mínimo diez puntos y la puntuación total máxima obtenida es 18 puntos. Además, las categorías son las mismas: protección, rendimiento y usabilidad⁸.

¿Cómo podemos elegir el más adecuado?

¿Cómo puedo elegir yo mismo el mejor antivirus?

Aunque ya te hemos dado todas las claves de los mejores antivirus para Windows 10, incluyendo pruebas de rendimiento, impacto en el PC, detección de amenazas y mucho más, debes ser tú el que tome la decisión final. Lo cierto es que la opción fácil sería quedarse con Windows Defender que ofrece un buen resultado a coste, pero si decidimos ir a por otra opción, ya sea gratuita o de pago, debemos considerar lo siguiente:

⁸ <https://www.adslzone.net/esenciales/windows-10/mejores-antivirus-windows-10>

Aprovechar la prueba gratis: Muchas de las soluciones de pago enumeradas anteriormente cuentan con una prueba gratuita que suele durar entre 7 días y 30 días. Este es el periodo ideal para que podamos probarla a fondo antes de decidir. Tampoco debemos perder de vista los reembolsos, ya que alguna no nos deja probar el antivirus gratis, pero sí nos devuelven el dinero.

Funciones necesarias: La protección básica de todos los antivirus es bastante parecida, pero las grandes diferencias están en las funciones especiales o añadidas. Por ejemplo, si vamos a navegar mucho en redes wifi públicas, es posible que queramos valorar la compra de una solución con VPN integrada.

Dispositivos compatibles: Aunque estamos hablando de Windows 10, lo cierto es que todos tenemos más dispositivos susceptibles de ser infectados en casa, desde el móvil a la tableta. Por ese motivo, algo que podemos valorar es la compra de una protección que incluya varios dispositivos. Tenemos algunas de McAfee hasta en 10 dispositivos o Panda, aunque en este caso no es compatible con todos los móviles.

Exigencia para el sistema: Lo mejor es encontrar un antivirus que no sea muy exigente para el sistema, sobre todo si no contamos con un ordenador extremadamente potente. Debemos ser cuidadosos en este sentido, ya que existen antivirus que pueden hacer que nuestro sistema vaya bastante más lento y a la larga empeora nuestra experiencia de usuario. Para conseguir que el antivirus no afecte al comportamiento del PC, lo mejor es ver cuáles son los requerimientos que marca la empresa del software para con el hardware del quipo. De esta manera sabremos si nuestro ordenador puede llevar ese antivirus que tanto nos gusta.

Interfaz intuitiva: Si no tenemos mucha experiencia en el mundo de los antivirus, siempre será mejor contar con uno que tenga una interfaz que se entienda bien e intuitiva. Esto nos va a permitir manejar el software con mayor soltura y encontrar todo aquello que nos haga falta sin tener que dar excesivas vueltas.

Actualizaciones: Este otro de los temas fundamentales en un buen antivirus, ya que de las actualizaciones dependerán buena parte de las capacidades para protegernos en tiempo real y sobre todo de amenazas que puedan ir apareciendo con el tiempo, puesto que todos sabemos que el mundo de los virus es muy cambiante y debemos tener un sistema que sepa adaptarse a los nuevos retos en este apartado. es decir, que se actualice lo suficientemente rápido como para combatir virus que acaben de aparecer⁹.

Los programas citados son de pago y son los mejores para Windows 10 (según el criterio comentado). También hemos visto cómo elegir el más adecuado, pero puede suceder o que no trabajemos con Windows 10 o que queramos un antivirus gratuito. En este caso, deberemos buscar la información correspondiente y aplicar los criterios indicados en la elección del antivirus.

⁹ <https://www.adslzone.net/esenciales/windows-10/mejores-antivirus-windows-10>

En la misma fuente se comentan las características de Windows Defender:

Windows Defender

Antes de terminar, toca hablar de Windows Defender, la solución de seguridad gratuita e integrada dentro del sistema operativo de Microsoft. En los últimos años ha ido mejorando notablemente y lo cierto es que es más que suficiente para la inmensa mayoría de los usuarios. Según los test realizados por la mencionada empresa, Windows cuenta con un antivirus potente. Tiene un 100 % en los últimos dos meses analizados en el apartado «protección contra ataques de día 0 provenientes de internet, incluidos los correos electrónicos y las páginas web maliciosas». También cuenta con alta protección en detección de malware con un 100 % en el total y con un 99,3 % de promedio en la industria. Es decir, el de Microsoft es mejor que la media.

Tampoco encontramos problemas en rendimiento ni en usabilidad, apartados en los que aprueba con nota. Durante los meses analizados no hay falsas alarmas o bloqueos y solo un caso de detección errónea como malware de softwares seguro. Además, el test muestra que no hay bloqueos erróneos ni comete errores de avisos¹⁰.



Figura 5.3. Windows Defender.

La seguridad del SO (Windows) es buena y, por lo tanto, la decisión de incorporar un antivirus al ordenador dependerá del uso que hagamos del mismo.

5.1.2. Firewall

Recurramos a los expertos, como siempre hacemos:

Firewall: qué es un cortafuegos, para qué sirve y cómo funciona

Vamos a explicarte qué es un firewall o cortafuegos, soluciones diseñadas para proteger tu ordenador que pueden complementarse o integrarse en un antivirus. Son tipos de protección que posiblemente ya estés utilizando sin darte cuenta, pero eso no quiere decir que debas preocuparte y no conocer lo que hacen y lo que no hacen.

¹⁰ <https://www.adslzone.net/esenciales/windows-10/mejores-antivirus-windows-10>



Figura 5.4. Cortafuegos.

Qué es un cortafuegos y para qué sirve

El cortafuegos o firewall en inglés, en el mundo de la informática es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales. Se trata de una de las primeras medidas de seguridad que empezó a implementarse en los ordenadores tras el nacimiento de internet.

Su origen se remonta a finales de la década de los años 80, cuando internet daba sus primeros pasos y los primeros hackers descubrieron que con esta nueva red podían infiltrarse y hacer travesuras en los ordenadores de otras personas, lo que llevó a una serie de importantes violaciones de seguridad y ataques de malware.

Con el tiempo fueron evolucionando para conseguir analizar mejor la información entrante y filtrar las posibles amenazas. La finalidad siempre ha sido la misma que siguen teniendo hoy, la de establecer unos criterios de seguridad, y filtrar todas las comunicaciones que entran o salen del ordenador para interceptar las que no cumplan con ellos y dejar pasar al resto.

Estos criterios van variando y evolucionando con el tiempo, para mantenerse actualizados frente a unos ataques también en constante evolución. Es importante que sepas que los cortafuegos no eliminan el malware que intenta entrar, solo trata de bloquear su acceso. Si ya tienes un virus en el ordenador el cortafuegos no podrá hacer tanto, y tendrás que combinarlo con un antivirus.



Cómo funcionan los cortafuegos

Los cortafuegos pueden ser de dos tipos, pueden ser software, de hardware o una combinación de ambos. Esto quiere decir que pueden ser aplicaciones que instales en tu ordenador o dispositivos que se conecten a él para controlar el tráfico.

Los cortafuegos físicos pueden ser productos independientes o venir directamente integrados en un router. Los independientes se suelen situar entre el punto de acceso a internet y el switch que se encarga de distribuir la conexión entre los ordenadores de una misma red. El hecho de que vaya antes de la distribución de la red entre los equipos significa que todos los que haya en una red interna quedan protegidos.

Son buenos para muchos ataques exteriores, sobre todo para las redes internas e intranets. Esto les convierte en buenas herramientas para empresas y grandes redes. Pero no son tan seguros con muchos tipos de ataque que vengan a través de otra aplicación, como los troyanos o las amenazas que recibes a través de correos electrónicos fraudulentos.

Los más populares en los usuarios de a pie son los cortafuegos en forma de software, que son aplicaciones que pueden instalarse en los ordenadores. Además de interceptar los intentos de acceso desde el exterior también suelen incluir protecciones adicionales contra los troyanos y virus de correo más comunes. Su desventaja es que solo protegen de manera individual a cada ordenador que los tiene instalados.

Ahora vamos a hablar de sus funciones. Como te hemos explicado, los cortafuegos se sitúan entre la red local e internet, y su misión es protegerte bloqueando el tráfico no solicitado o que considere peligroso. Pero puede hacer otras cosas, como aprovechar que analiza el tráfico que entra o sale para configurar filtros para diferentes tipos de tráfico con los que decidir qué hacer con él.

En estas configuraciones se pueden hacer muchas cosas, como por ejemplo permitir únicamente las conexiones a servidores de direcciones IP concretas, descartando el resto por seguridad. Esto evidentemente a nivel doméstico no es muy efectivo, te impide navegar con facilidad, pero en ámbitos empresariales o más cerrados puede servir.

Al poder analizar el tráfico saliente, también pueden llegar a detectar si hay algún malware comunicándose con la red, monitorizando el uso de redes empresariales, o filtrando el tráfico. Además, también puede configurarse, por ejemplo, para que solo el navegador de los ordenadores de una empresa pueda conectarse a internet, bloqueando el acceso del resto de aplicaciones por seguridad.

Que no te hagan bajar la guardia

Siempre puedes instalar aplicaciones de firewall de terceros. Pero has de saber que sistemas operativos como Windows 10 ya llevan cortafuegos integrados, y muchos de los routers que hay hoy en día también tienen sus módulos para filtrar posibles amenazas, aunque suelen ser protecciones bastante básicas.

Aun así, tanto si tienes un cortafuegos integrado como si decides comprar o instalar uno, nunca debes delegar exclusivamente en él a la hora de protegerte. Sí, añaden una capa de seguridad extra a tu ordenador, pero eso no significa que no vayas a estar amenazado por ningún tipo de malware.

Lo mejor siempre es complementar tus protecciones. Si tienes un sistema operativo como Windows 10, que integra un antivirus propio con firewall, es verdad que posiblemente no necesites instalar aplicaciones de terceros. Pero eso no evita que tengas que seguir tomando muchas precauciones y navegar con precaución para evitar las amenazas más comunes. Lo mismo pasa si tienes solo un firewall o un antivirus, puedes complementarlos aunque sin dejar de bajar la guardia¹¹.

Los sistemas operativos pueden incorporar sus propios antivirus y firewall, como es el caso de Windows, y los antivirus también suelen incorporar esta función, pero también existen programas firewall, que conviene conocer; a continuación, listamos algunos de ellos, gratuitos, los mejores según la fuente consultada¹².

- SolarWinds Network Firewall Security Management.
- ZoneAlarm.
- Comodo Firewall.
- TinyWall.
- Netdefender.
- Glasswire.
- PeerBlock.
- Firewall AVS.
- OpenDNS.
- Norton Free Firewall

5.1.3. Conclusión

Ya sabemos lo que son los antivirus, antimalware y cortafuegos, conocemos el nombre de muchos de ellos y los criterios para elegir el más adecuado a nuestras necesidades.

Pero hay que hacer algunas consideraciones a la hora de pensar en instalar algunos de estos programas.

En primer lugar, hay que aprovechar al máximo las características de seguridad del sistema operativo, del navegador y buscador e incluso del operador de internet con el que trabajemos¹³. Si con estos servicios el equipo está suficientemente protegido, no hace falta nada más; no obstante, se suele recomendar instalar un antivirus a pesar de todo.

¹¹ <https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona>

¹² https://protecciondatos-lopd.com/empresas/mejores-firewall-windows/#Los_mejores_Firewall_para_Windows

¹³ <https://www.movistar.es/particulares/conexion-segura>



Como hemos visto, hay programas gratuitos y de pago y, normalmente, las versiones gratuitas son menos potentes que las de pago, pero pueden ser suficientes.

No olvidemos que el mejor antivirus es la prudencia y que la intensidad de la protección dependerá de la importancia de la información manejada.

Ahora ya podemos elegir el programa que nos dé la mejor protección para el uso que hagamos de nuestros equipos.

► ACTIVIDAD PROPUESTA 5.1

Antivirus

Hasta ahora hemos tratado el tema del antivirus referido, sobre todo, a Windows y a los PC.

¿Qué sucede con los Mac? ¿Es verdad que son inmunes a los virus?

Busque información al respecto para contestar estas preguntas.

5.2. Protección del dispositivo móvil

Para entender que una inadecuada protección del móvil, unida a un uso discutible del mismo, puede dar lugar a problemas para mucha gente, permítanme comentar un caso real.

Durante un fin de semana, el autor y otras muchas personas que trabajaban en la misma empresa recibieron una gran cantidad de correos maliciosos (40 o 50 mensajes por destinatario); no eran especialmente peligrosos, pero sí muy molestos y si se eliminaban volvían a recibirse en grandes cantidades.

El resultado de la investigación, llevada a cabo por los técnicos de la empresa, mostró que se había estado utilizando un móvil personal para ver el correo corporativo (Gmail) y por ahí había entrado el ataque.

El uso del móvil es cada vez más frecuente y a estos dispositivos se les van incorporando funciones que manejan información sensible, como medios de pago. El uso del móvil como herramienta de seguridad va en aumento, por ejemplo mediante las dobles verificaciones para entrar en el correo dando la conformidad desde el móvil.

Pero estas aplicaciones del móvil van a más; de hecho, parece que Google quiere eliminar las contraseñas y utilizar el móvil como medio de autenticación¹⁴, y hay que tener en cuenta que, en muchas ocasiones, este dispositivo sirve para conectarse a redes públicas, que suelen ser especialmente vulnerables.

¹⁴ https://www.xataka.com/aplicaciones/google-quiere-futuro-contrasenas-este-su-plan-para-conseguirlo-todos-dispositivos?utm_source=NEWSLETTER&utm_medium=DAILYNEWSLETTER&utm_content=POST17&utm_campaign=06_May_2022+Xataka&utm_term=CLICK+ON+TITLE

En resumen, hay que hacer un uso responsable del móvil y hay que tenerlo adecuadamente protegido, especialmente cuando desde el móvil accedemos a aplicaciones corporativas, lo que hace que sea mucho más apetecible hackearlo para obtener información sensible de la empresa.

El móvil es uno de tantos aparatos que se han incorporado a nuestra vida cotidiana y que, como todo, tiene sus ventajas y sus inconvenientes; hay que aprender a manejarlo, pero el correcto uso del móvil va mucho más allá de hacernos fotos. Recomendamos leer detenidamente el documento *Uso seguro de Android*¹⁵, teniendo en cuenta que la tecnología avanza y que conviene mantenernos actualizados.

Hagamos un uso responsable y prudente de nuestros móviles y veamos qué medios de protección podemos utilizar; pero, antes de comentar los antivirus disponibles, veamos unas recomendaciones sobre el uso de antivirus en el móvil:

¿Antivirus en el móvil?

De la misma forma que existen virus informáticos para ordenadores, existen virus informáticos para teléfonos inteligentes. Los creadores de virus cada día dedican más recursos a intentar infectar y comprometer los dispositivos móviles, ya sea para robar información, contraseñas, información personal, o sencillamente para controlarlos y poder lanzar ataques desde estos, exactamente igual que con los ordenadores. El hecho de que casi todo el mundo tenga un teléfono propio el cual suele estar conectado a internet todo el día, los convierte en un objetivo muy atractivo para este tipo de delincuentes.

Si bien es verdad que la forma de funcionar de los virus para móvil es muy similar a la de los ordenadores, en los móviles existen ciertas limitaciones en cuanto a la forma de propagación: la forma más común de infección es por descargar e instalar aplicaciones desde fuentes no fiables y en menor medida por abrir ficheros infectados.

Es cierto que los antivirus para móviles aún no son tan maduros como en los ordenadores convencionales, y que su utilización no garantiza que podamos instalar cualquier tipo de aplicación sin riesgo de infección, pero hoy por hoy, junto al sentido común, son la mejor arma que tenemos, así que la respuesta es SÍ, debemos instalar un antivirus en nuestro dispositivo móvil.

No obstante, recordemos que no por ello podemos bajar la guardia en el resto de buenas prácticas: no instalar aplicaciones de fuentes poco fiables (generalmente copias ilegales), no abrir ficheros sospechosos (correo, mensajería instantánea, internet), y tener siempre tanto el sistema operativo como las aplicaciones lo más actualizadas posible¹⁶.

¹⁵ https://concienciat.gva.es/wp-content/uploads/2018/03/info_guia_uso_seguro_android.pdf

¹⁶ https://concienciat.gva.es/wp-content/uploads/2018/03/info_guia_uso_seguro_android.pdf

Veamos otra opinión:

¿De verdad necesitas un antivirus?

Es la pregunta de la década. Ahora las aplicaciones para Android tienen mucho más restringido lo que pueden y no pueden hacer, incluyendo el comportamiento típico del malware como robar datos, expandirse a otros dispositivos o hacer todo tipo de estropecios. Es común trazar el paralelismo de los antivirus en Windows al móvil, aunque son dos sistemas completamente distintos.

Sin embargo, Android dista mucho de ser un sistema perfecto o invulnerable a amenazas. Con más frecuencia de la que nos gustaría, recibimos noticias de malware encontrado dentro y fuera de la tienda de Google, demostrando que, en la guerra constante de Google contra el malware, algunas batallas se ganan y otras se pierden. ¿Está recomendado, por tanto, instalar un antivirus en el móvil?

La respuesta corta es sí, pero con un matiz importante: los móviles Android ya tienen un antivirus integrado, Google Play Protect. Play Protect sirve como línea de defensa contra malware conocido y hace las labores de protección básicas de un antivirus: analizar aplicaciones y decirte si alguna de ellas es malware. En caso afirmativo, te muestra un aviso antes de que la instales, o incitándote a desinstalarla, si ya está en el sistema¹⁷.



Figura 5.5. Google Play Protect.

No nos asustemos, ambas opiniones no son contradictorias. La primera es general, hay móviles de muchos tipos; y la segunda es solo aplicable a los móviles Android. La sugerencia del autor es que, si nos sentimos más cómodos, debemos instalar un antivirus en el móvil, aunque sea Android; puede no ser necesario, dependiendo del uso que le demos, pero no molesta.

Para aquellas personas que estén interesadas en los antivirus para el móvil, dos fuentes de información:

- Los 9 mejores antivirus gratis para el móvil¹⁸.
- Los mejores antivirus para móviles¹⁹.

Ya tenemos los medios para tomar la decisión más adecuada.

¹⁷ <https://www.xatakandroid.com/listas/9-mejores-antivirus-gratis-para-movil>

¹⁸ <https://www.xatakandroid.com/listas/9-mejores-antivirus-gratis-para-movil>

¹⁹ <https://ayudaleyprotecciondatos.es/2021/07/01/mejores-antivirus-movil>

► ACTIVIDAD PROPUESTA 5.2

Google Play Protect

- ¿Sabe lo que es Google Play Protect?
- ¿Sabe encontrarlo en su móvil Android?

► ACTIVIDAD PROPUESTA 5.3

Estar al día

- Los móviles evolucionan y su uso aumenta constantemente y, por eso, para no perderse o quedarse anticuado conviene estar actualizado.
- ¿Conoce algún sitio en la red que envía noticias periódicas para mantenerse al día?

5.3. Protección de la red de datos

En la Unidad 1, Apartado 1.5, definimos la red de datos: *el término red hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas*. Lo que nos interesa de esta definición es el hecho de que la red está formada por sistemas conectados entre sí, sistemas formados por dispositivos.

El concepto de red abarca desde internet, la red por antonomasia, hasta la pequeña red doméstica; para ilustrar de forma sencilla los conceptos anteriores recurrimos a las definiciones de la RAE, que entre las múltiples acepciones de red cita las dos siguientes:

10. *f. Inform. Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información.*
11. *f. Inform. Internet²⁰.*

Desde el punto de vista de la ciberseguridad, que es de lo que realmente estamos hablando en esta unidad, hay que proteger una determinada red contra amenazas interiores y exteriores, puesto que las redes, con independencia de su tamaño, suelen estar conectadas a internet.

²⁰ <https://dle.rae.es/red?m=form>

Al igual que con los dispositivos, la protección debe estar en consonancia con lo que queramos proteger (no es lo mismo proteger la red de transporte ferroviario de un país que una pequeña red doméstica), pero, en cualquier caso, hay que aplicar los medios adecuados.

No vamos a tratar la protección de las grandes redes públicas o privadas, eso queda en manos de profesionales, pero vamos a aprender a proteger nuestra red doméstica, aunque muchos de los conceptos sean aplicables a redes más grandes.



Figura 5.6. Protección de la red de datos.

¿Cuáles son las amenazas interiores que puede sufrir una red?

De la definición de red como *conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información* deducimos que hay equipos de distintos tipos, cables, conexiones y toda clase de dispositivos conectados a la red y de aparatos que hacen posible dicha conexión. Todo este hardware es susceptible de fallar y debe estar correctamente utilizado y mantenido, sin olvidar el suministro eléctrico y las condiciones ambientales.

Pero también hay que tener en cuenta a las personas que usan los equipos. Un mal uso de estos, no tanto del equipo en sí, como de la forma en que tratemos la información, sea el software o el uso de este para la gestión de la información, puede causar graves daños; los errores y los comportamientos irresponsables, e incluso delictivos, son frecuentes, por lo que la organización debe tomar las medidas oportunas.

Cuando la «organización» es una familia y la red es la red doméstica también hay que tomar las precauciones adecuadas, que pasan por enseñar el uso de los dispositivos y por adaptar estos y sus funcionalidades a la edad y condición de los usuarios; la imaginación de una persona de 10 años no tiene límite.

Hay que ser consciente de que, muchas veces, la parte más vulnerable de la red no son los equipos, son las personas.

Supongamos, en un alarde de optimismo, que las amenazas internas están controladas (pero seamos sensatos y no nos descuidemos). Veamos las amenazas exteriores y para ello conviene definir el concepto de seguridad de red:

En un nivel básico, la seguridad de red es la operación de proteger datos, aplicaciones, dispositivos y sistemas que están conectados a la red.

Aunque la seguridad de red y la ciberseguridad se superponen de muchas maneras, la seguridad de red se define con mayor frecuencia como un subconjunto de la ciberseguridad. Usando la tradicional «analogía del castillo y el foso» o un enfoque de seguridad basado en el perímetro, en el que su organización es su castillo y los datos almacenados dentro del castillo son las joyas de la corona, la seguridad de red se preocupa más por la seguridad dentro del muros de castillo.

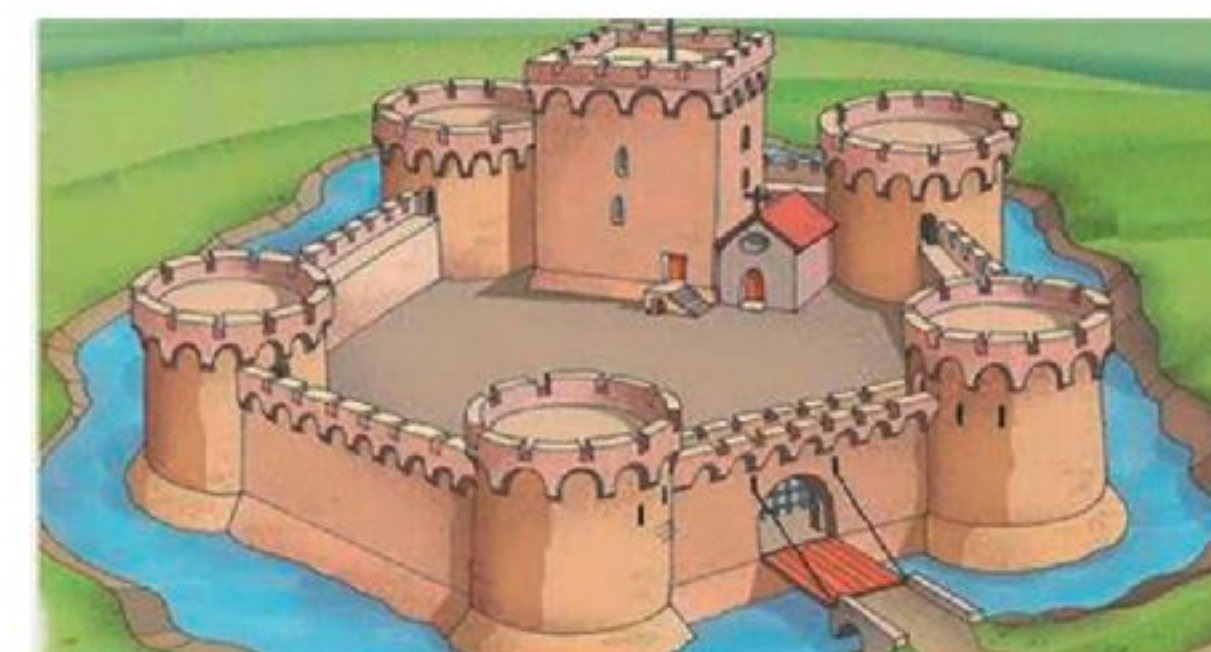


Figura 5.7. Castillo y foso.

En este escenario basado en el perímetro, el área dentro de los muros del castillo puede representar la infraestructura de TI de una empresa, incluidos sus componentes de red, hardware, sistemas operativos, software y almacenamiento de datos. La seguridad de red protege estos sistemas del malware/ransomware, ataques distribuidos de denegación de servicio (DDoS), intrusiones en la red y más, creando una plataforma segura para que los usuarios, las computadoras y los programas realicen sus funciones dentro del entorno de TI.

A medida que las organizaciones migran a entornos híbridos y multinube, sus datos, aplicaciones y dispositivos se dispersan en diversas ubicaciones y geografías. Los usuarios desean acceder a los datos y sistemas empresariales desde cualquier lugar y dispositivo. Por lo tanto, el enfoque tradicional basado en el perímetro de la seguridad de red está desapareciendo gradualmente. Un enfoque de confianza cero de la seguridad, en el que una organización nunca confía y siempre verifica el acceso, se está convirtiendo rápidamente en el nuevo método para fortalecer la postura de seguridad de una organización²¹.

²¹ <https://www.ibm.com/es-es/topics/network-security>



El planteamiento de IBM define la seguridad de red teniendo en cuenta el entorno cambiante y la tendencia creciente a trabajar en la nube.

Aunque el documento citado de IBM es muy completo, vamos a recurrir a otro de los grandes (Cisco) para ver los tipos de seguridad o protección de red:

Tipos de seguridad de red

Firewalls

Los firewalls ponen una barrera entre su red interna de confianza y las redes externas que no son de confianza, como internet. Usan un conjunto de reglas definidas para permitir o bloquear el tráfico. Un firewall puede ser hardware, software o ambos.

Seguridad del correo electrónico

Los gateways del correo electrónico son el principal vector de amenaza para las infracciones a la seguridad. Los atacantes usan la información personal y las tácticas de ingeniería social para desarrollar campañas de suplantación de identidad (phishing) sofisticadas para los destinatarios de los dispositivos a fin de dirigirlos a sitios con malware. Una aplicación de seguridad de correo electrónico bloquea los ataques entrantes y controla los mensajes salientes para prevenir la pérdida de datos sensibles.

Software antivirus y antimalware

El «malware», abreviatura de «software malicioso», abarca los virus, gusanos, troyanos, ransomware y spyware. En algunos casos, el malware puede infectar una red y permanecer latente por días o incluso semanas. Los mejores programas antimalware no solo detectan la entrada de malware, sino que también hacen un seguimiento constante de los archivos para detectar anomalías, eliminar malware y reparar daños.

Segmentación de la red

La segmentación definida por software clasifica el tráfico de red en distintas categorías y facilita la aplicación de políticas de seguridad. Lo ideal es que las clasificaciones se basen en la identidad de los EndPoints, no solo en las direcciones IP. Puede asignar derechos de acceso basados en roles, ubicación y demás, de modo que se otorgue el nivel de acceso correcto a las personas adecuadas y se contengan y reparen los dispositivos sospechosos.

Control de acceso

No todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos. Entonces podrá aplicar las políticas de seguridad. Puede bloquear dispositivos de EndPoint que no cumplen las políticas o proporcionarles acceso limitado. Este proceso se denomina control de acceso a la red (NAC).

Seguridad de las aplicaciones

Cualquier software que utilice para operar su negocio debe estar protegido, ya sea que su personal de TI lo construya o lo compre. Lamentablemente, todas las aplicaciones pueden tener vulnerabilidades que los atacantes pueden usar para infiltrarse a la red. La seguridad de las aplicaciones abarca el hardware, el software y los procesos que se usan para corregir estas vulnerabilidades.

Análisis del comportamiento

Para detectar el comportamiento anómalo de la red, primero debe conocer el comportamiento normal. Las herramientas de análisis de comportamiento detectan automáticamente las actividades que se desvían de la norma. El equipo de seguridad entonces puede identificar mejor los indicadores de infiltración que pueden traer problemas y reaccionar rápidamente ante las amenazas.

Prevención de pérdida de datos

Las organizaciones deben asegurarse de que el personal no envíe información confidencial fuera de la red. Las tecnologías de prevención de pérdida de datos (DLP) pueden evitar que las personas carguen, reenvíen o incluso impriman información confidencial de manera no segura.

Sistemas de prevención de intrusiones

Un sistema de prevención de intrusiones (IPS) analiza el tráfico de red para bloquear ataques activamente. Los dispositivos del IPS de próxima generación (NGIPS) de Cisco logran esto al correlacionar enormes cantidades de inteligencia de amenazas globales para bloquear las actividades maliciosas y hacer un seguimiento del progreso de los archivos sospechosos y el malware por la red a fin de evitar la propagación de brotes y la reinfección.

Seguridad de dispositivos móviles

Los ciberdelincuentes cada vez se centran más en los dispositivos y las aplicaciones móviles. Obviamente, debe controlar qué dispositivos pueden acceder a la red. También debe configurar las conexiones para preservar la privacidad del tráfico de red.

Administración de eventos e información de seguridad

Los productos SIEM reúnen la información que el personal de seguridad necesita para identificar y responder a las amenazas. Estos productos tienen diferentes formas que incluyen dispositivos virtuales y físicos y software de servidor.

VPN

Una red privada virtual cifra la conexión desde un terminal a la red, generalmente por internet. Por lo general, una VPN de acceso remoto usa Ipsec o una capa de sockets seguros para autenticar las comunicaciones entre los dispositivos y la red.

Seguridad web

Una solución de seguridad web controla el uso de la web por parte del personal, bloquea las amenazas web y bloquea el acceso a sitios web maliciosos. Protege el gateway web en las instalaciones o la nube. La «seguridad web» también hace referencia a los pasos que se toman para proteger el sitio web.

Seguridad inalámbrica

Las redes inalámbricas no son tan seguras como las redes cableadas. Sin medidas de seguridad estrictas, instalar una LAN inalámbrica es como poner puertos Ethernet por doquier, incluso en el estacionamiento. Para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica²².



Figura 5.8. Seguridad de red.

El enfoque de Cisco va dirigido a empresas y es para profesionales, pero es fácilmente adaptable a nuestra red doméstica.

Ya hemos hablado acerca de firewalls, seguridad del correo electrónico, software anti-virus y antimalware, por lo que ya sabemos lo que hay que hacer.

Sobre segmentación de la red, control de acceso y seguridad de las aplicaciones ya conocemos el control parental y cómo limitar el acceso a determinados sitios; incluso los servicios tipo Amazon Prime y Netflix tienen la posibilidad de crear perfiles distintos para niños y adultos.

Respecto al análisis del comportamiento y a la prevención de pérdida de datos cabe recordar que no hay que poner cierta información en manos de todos, por ejemplo, los medios de pago, y conviene estar atentos a los cargos en la tarjeta; se pueden haber guardado datos de medios de pago en determinadas aplicaciones.

²² https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~how-network-security-works

Sobre sistemas de prevención de intrusiones, administración de eventos e información de seguridad, VPN y seguridad web, sin llegar a ciertos extremos, mediante anti-virus y los permisos y las claves de acceso adecuadas podemos mejorar la seguridad de la red doméstica.

También hemos visto cómo proteger la seguridad de los dispositivos móviles.

Respecto a la seguridad inalámbrica, ahora podemos entender mejor la razón de que la clave de la red wifi del router doméstico tenga 20 posiciones, con mayúsculas, minúsculas y números.

Pero recordemos que no hay nada mejor que la prudencia y mantenernos informados.

► ACTIVIDAD PROPUESTA 5.4

Seguridad de la red doméstica

Analice su red doméstica y vea qué vulnerabilidades presenta.
Hay una vulnerabilidad evidente, dar la clave wifi a muchas personas. ¿Lo hace?

► ACTIVIDAD PROPUESTA 5.5

VPN

¿Sabe lo que es una VPN? Busque información y reflexione sobre la conveniencia de tenerla para su uso personal.



ACTIVIDADES FINALES

DE COMPROBACIÓN

5.1. Windows Defender:

- a. Antivirus de pago de Google.
- b. No hay ningún programa con ese nombre.
- c. Antivirus de pago de Microsoft.
- d. Solución de seguridad gratuita e integrada dentro del sistema operativo Windows de Microsoft.

5.2. Sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de este con otros servicios autorizados:

- a. Cortafuegos (firewall).
- b. Solo funciona en Windows.
- c. Solo es válido para Linux
- d. Solo es válido en los Mac.

5.3. Hay que ser muy cuidadoso con las redes públicas:

- a. Sí, suelen ser muy vulnerables.
- b. No hace falta, son seguras.
- c. No, si se conecta con el móvil.
- d. Depende del dispositivo.

5.4. La protección del ordenador y de otros dispositivos se puede contemplar desde dos puntos de vista:

- a. Domótica y ofimática.
- b. Protección del hardware y amenazas externas.
- c. Legal y física.
- d. Propia y ajena.

5.5. Las amenazas contra la red de datos pueden venir de los usuarios de esta:

- a. Por desconocimiento del uso de los recursos de red.
- b. Por fallos y errores.
- c. Con fines delictivos.
- d. Las respuestas anteriores son correctas.

5.6. La seguridad de red es:

- a. El antivirus.
- b. La operación de proteger datos, aplicaciones, dispositivos y sistemas que están conectados a la red.
- c. El firewall.
- d. Las redes son seguras de por sí.

5.7. La computación en la nube está cambiando el enfoque de la seguridad de red:

- a. Pues la información está cada vez más dispersa.
- b. No se debe trabajar en la nube, es absurdo.
- c. La computación en la nube anula el concepto de ciberseguridad.
- d. No hay seguridad en la nube.

5.8. Siempre hay que tener el software actualizado:

- a. Depende del tipo de software.
- b. Depende del tipo de ordenador.
- c. Verdadero.
- d. Falso.

5.9. Las redes inalámbricas no son tan seguras como las cableadas:

- a. La seguridad no depende de la tecnología de conexión.
- b. Solo en caso de redes públicas.
- c. Facilitan el acceso de terceros mediante wifi.
- d. Son igual de seguras.

5.10. En la red doméstica hay que ser muy riguroso con las medidas de seguridad de red:

- a. No hace falta.
- b. Es caro e innecesario.
- c. No, si solo la utiliza la familia.
- d. Es absolutamente necesario.

5.11. VPN:

- a. Red privada virtual.
- b. Verificación de programas normales.
- c. Virtualización de una parte del núcleo.
- d. Propiedad virtual normal.

5.12. Protección de sistemas, redes y programas de ataques digitales:

- a. Antivirus.
- b. Firewall.
- c. Eliminación de malware.
- d. Ciberseguridad.

5.13. Conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas:

- a. VPN.
- b. Red de datos.
- c. Cipersistema.
- d. Espacio virtual de intercambio.

**5.14. Google Play Protect:**

- a. Antivirus instalado en los móviles Android.
- b. Programa de Linux que permite bajar aplicaciones.
- c. Tienda de aplicaciones.
- d. Antivirus de Microsoft.

5.15. Un buen antivirus debe estar constantemente actualizándose:

- a. Depende del antivirus.
- b. Verdadero.
- c. Es imposible.
- d. No es necesario.

5.26. Revise la configuración de seguridad de su ordenador, para asegurarse de que utiliza lo que le ofrece su SO.

5.27. Al final del Apartado 5.2 se dan dos sitios con listas de antivirus para el móvil. Vaya a estos sitios y léalos con atención.

5.28. Compruebe la seguridad de su red doméstica. ¿Está la red de su oficina suficientemente protegida?

5.29. Busque información sobre amenazas de red, hay que saber a lo que nos exponemos.

5.30. ¿Cómo se propagan los virus? Busque información.

DE APLICACIÓN

5.16. Revise las condiciones de uso y mantenimiento de su equipo, para ver si las está cumpliendo.

5.17. ¿Está su software actualizado? Revíselo y proceda en consecuencia.

5.18. Busque información sobre tipos de virus, para entender el daño que pueden causarle.

5.19. Busque información sobre tipos de software malicioso que no sean virus.

5.20. Conteste a las siguientes preguntas:

- ¿Tiene antivirus?
- ¿Tiene activado Windows Defender, caso de trabajar con Windows?
- ¿Necesita un antivirus?

5.21. ¿Utiliza su equipo personal para conectarse a la intranet de su empresa? ¿Cree que cumple los requisitos de seguridad para poder hacerlo sin peligro?

5.22. Busque antivirus gratuitos para PC y vea su calificación en AV-Test.

5.23. Haga un resumen del Apartado 5.1.1 con sus propias palabras, para asegurarse de que lo ha entendido. Comprar un antivirus puede ser una decisión importante, en determinadas circunstancias.

5.24. Visite la web de los antivirus citados en el Apartado 5.1.1, vea precios y prestaciones. ¿Trabajan con antimalware?

5.25. Visite la web de los antivirus citados en el Apartado 5.1.1. ¿Valen para el móvil?



Resolución de problemas

Los virus y los troyanos forman parte de lo que se ha denominado software malicioso: software utilizado, habitualmente, con fines delictivos.

Antes de enfrentarse al enemigo, hay que conocerlo y es lo que vamos a hacer en esta unidad. Describimos los tipos más usuales de software malicioso y sus efectos, su forma de propagarse y los síntomas de que un equipo está infectado, para terminar con una guía de actuación para protegernos de ellos y eliminarlos.

El objetivo es disfrutar de la red sin comprometer nuestra información sensible.

Contenido

6.1. Detección y eliminación de virus y troyanos

6.1. Detección y eliminación de virus y troyanos

Antes de enfrentarnos al enemigo hay que conocerlo; por eso vamos a empezar este apartado definiendo los tipos de virus y de malware.

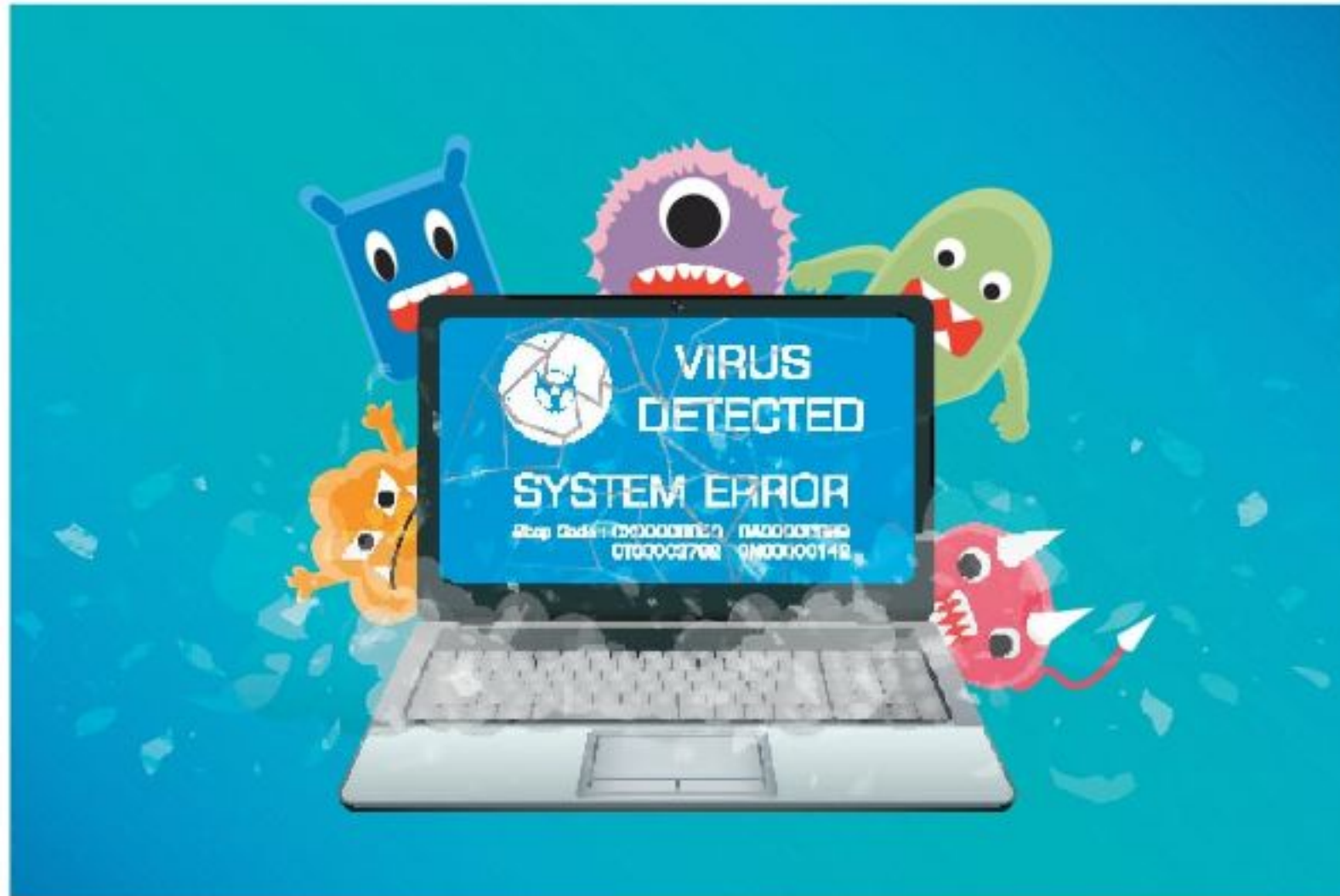


Figura 6.1. ¡Virus!

Vamos a utilizar diversas fuentes para conocer las amenazas más comunes y los sitios más adecuados para obtener este tipo de información: páginas de empresas fabricantes de antivirus, como AVG¹, y sitios oficiales, como la Oficina de Seguridad del Internauta (OSI)²; el lenguaje utilizado es un poco distinto, más técnico en el primer caso, pero conviene que nos familiaricemos con ambos enfoques.

Una definición de «virus informático» ¿Buscas una definición sencilla? Aquí tienes:

Un virus informático es un programa o fragmento de código diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de otra forma.

Los virus se diferencian de otros tipos de malware en que se replican automáticamente, es decir, son capaces de copiarse de un archivo o un PC a otro sin el consentimiento del usuario.

En definitiva, son altamente contagiosos.

Virus, malware, troyanos... ¿cuál es la diferencia?

¹ <https://www.avg.com/es/signal/what-is-a-computer-virus>

² <https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos>

No todo el software que ataca un PC es un virus. Los virus informáticos son solo una de tantas clases de malware (malicious software, software malicioso). A continuación, describimos otras clases muy comunes también:

- **Troyanos:** igual que el viejo caballo de madera infestado de atacantes del que toma su nombre, este malware simula ser software legítimo inocuo o se introduce en él a fin de engañar al usuario para abrir la puerta a otros tipos de malware que infectan el PC.



Figura 6.2. Troyano.

- **Spyware:** con ejemplos como los registradores de pulsaciones, este tipo de malware tiene el objeto de espiar a los usuarios, guardar sus contraseñas, datos de tarjetas de crédito, otros datos personales y patrones de comportamiento en línea para después enviarlo todo al artífice que lo programó.



Figura 6.3. Spyware.

- **Gusanos:** este tipo de malware ataca redes enteras de dispositivos saltando de un PC a otro.



Figura 6.4. Gusano.

- **Ransomware:** esta variedad de malware secuestra archivos (y, a veces, el disco duro entero), los cifra y exige dinero a la víctima a cambio de una clave de descifrado (que puede funcionar o no, pero lo más probable es que no).



Figura 6.5. Ransomware.

- **Adware:** este tipo de malware, increíblemente irritante, inunda las pantallas de las víctimas de anuncios no deseados y crea vulnerabilidades de seguridad para que otra clase de malware se pueda introducir subrepticamente.



Figura 6.6. Adware.

Resumiendo, los virus son tan solo uno de los varios tipos de malware que existen. En sentido estricto, los troyanos, el ransomware, etc., no son virus informáticos, aunque muchas personas utilizan el término «virus» para simplificar al referirse al malware en general³.

La siguiente información complementa y amplía la anterior:

Los virus, técnicamente conocidos como malware, son códigos informáticos creados para infectar nuestros equipos, provocar problemas en el funcionamiento de los mismos o robar información. Aunque se encuentran en constante evolución y cada cierto tiempo aparecen nuevos tipos, vamos a analizar los principales virus y la mejor forma de protegernos frente a ellos.

Según el comportamiento del virus y su forma de actuar, se le denomina de una forma u otra y existen una gran variedad de ellos. Algunos atacan directamente a nuestras defensas y otros buscan activarse y reproducirse, pero, sea cual sea su forma de actuar, su objetivo final es el de causarnos daño para obtener un beneficio económico. Las técnicas que utilizan los ciberdelincuentes para hacernos llegar el malware también son muy diversas, aunque muchas se apoyan en la ingeniería social.

³ <https://www.avg.com/es/signal/what-is-a-computer-virus>

Veamos los principales tipos de virus y malware que podemos encontrarnos:

- **Adware**, es aquel software que ofrece publicidad no deseada o engañosa. Estos anuncios pueden aparecer en el navegador con pop-ups o ventanas con gran contenido visual, e incluso audios.

Se reproducen de manera automática con el fin de generar ganancias económicas a los creadores. En ocasiones este software provoca que el buscador predilecto del usuario sea cambiado por otro, generando errores en las búsquedas deseadas y entorpeciendo la experiencia de navegación del usuario.

¿Cómo nos protegemos? Evitemos abrir enlaces de descarga de páginas poco fiables y, cuando instalemos software, debemos revisar los pasos para que no se nos instale ningún buscador, programa o complemento sin que nos demos cuenta.

- **Spyware**, este tipo de virus se encarga de recopilar de manera fraudulenta la información sobre la navegación del usuario, además de datos personales y bancarios. Un ejemplo de este tipo de virus son los Keyloggers, los cuales monitorizan toda nuestra actividad con el teclado (teclas que se pulsán), para luego enviarla al ciberdelincuente.

¿Cómo nos protegemos? El primer paso y más importante será la instalación y actualización de un buen sistema antivirus. Otra forma de protegernos es evitar conectar dispositivos desconocidos, como USB o discos duros externos.

- **Gusanos**, este virus está creado con la capacidad de replicarse entre ordenadores. A menudo causa errores en la red, como consecuencia de un consumo anormal del ancho de banda ocasionado por este malware.

Los ciberdelincuentes suelen usar nombres llamativos en los enlaces para que este virus sea descargado como, por ejemplo, las palabras: sexo, apuestas, regalo o premio.

¿Cómo nos protegemos? Al igual que para los gusanos y resto de virus detallados, es importante tener actualizado nuestro sistema y sus defensas para estar protegidos y evitar se infectados, así como desactivar la función de «autoejecutar» los discos externos (memorias USB o discos duros). Si el antivirus está actualizado, también identificará y eliminará este tipo de amenazas que intenten colarse en nuestros dispositivos.

- **Troyano**, este tipo de virus se presenta como un software legítimo, pero que, al ejecutarlo, le permite al atacante tomar el control del dispositivo infectado. Como consecuencia, nuestra información personal se encontraría en permanente riesgo, a merced del atacante para robar todo lo que quisiera de nuestros equipos infectados.

¿Cómo nos protegemos? Además de todas las medidas anteriores, como tener actualizado el sistema operativo y el antivirus, y analizar los dispositivos USB que se vayan a conectar a nuestro equipo, debemos tener mucho cuidado cuando navegamos por internet, ya que pueden acabar instalándose algún archivo infectado o al acceder a páginas web fraudulentas.

- **Ransomware**, malware que toma por completo el control del dispositivo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. Este software malicioso se trasmite en el dispositivo, tal y como lo hace un gusano o un troyano. Pueden llegar camuflados en adjuntos de correos electrónicos o en páginas web poco fiables que nos inviten a descargar algún archivo bajo una inofensiva apariencia. También se aprovechan frecuentemente de fallos de seguridad del sistema operativo o incluso de aplicaciones.

¿Cómo nos protegemos? Mucho cuidado con los correos electrónicos maliciosos con algún adjunto. La mayoría de los ataques por ransomware se producen cuando el usuario ejecuta un archivo infectado. También es recomendable realizar copias de seguridad para que, en caso de infección, dispongamos de una copia de nuestros datos en otro lugar de almacenamiento.

- **Botnets**, son redes de dispositivos infectados que los ciberdelincuentes utilizan para lanzar ataques, como el envío masivo de correos spam, ataques de denegación de servicio o DDoS, robos de credenciales, etc. Una vez que un dispositivo está infectado, entrará a formar parte de la red de botnets cuyo objetivo es seguir expandiéndose.

¿Cómo nos protegemos? Lo principal es hacer un buen uso de los dispositivos cuando nos conectamos a la red, teniendo un sistema actualizado con programas antivirus instalados, utilizando credenciales robustas y cambiando las contraseñas regularmente y no entrando en páginas web que puedan ser poco fiables. Otra fuente de infección son los correos maliciosos.

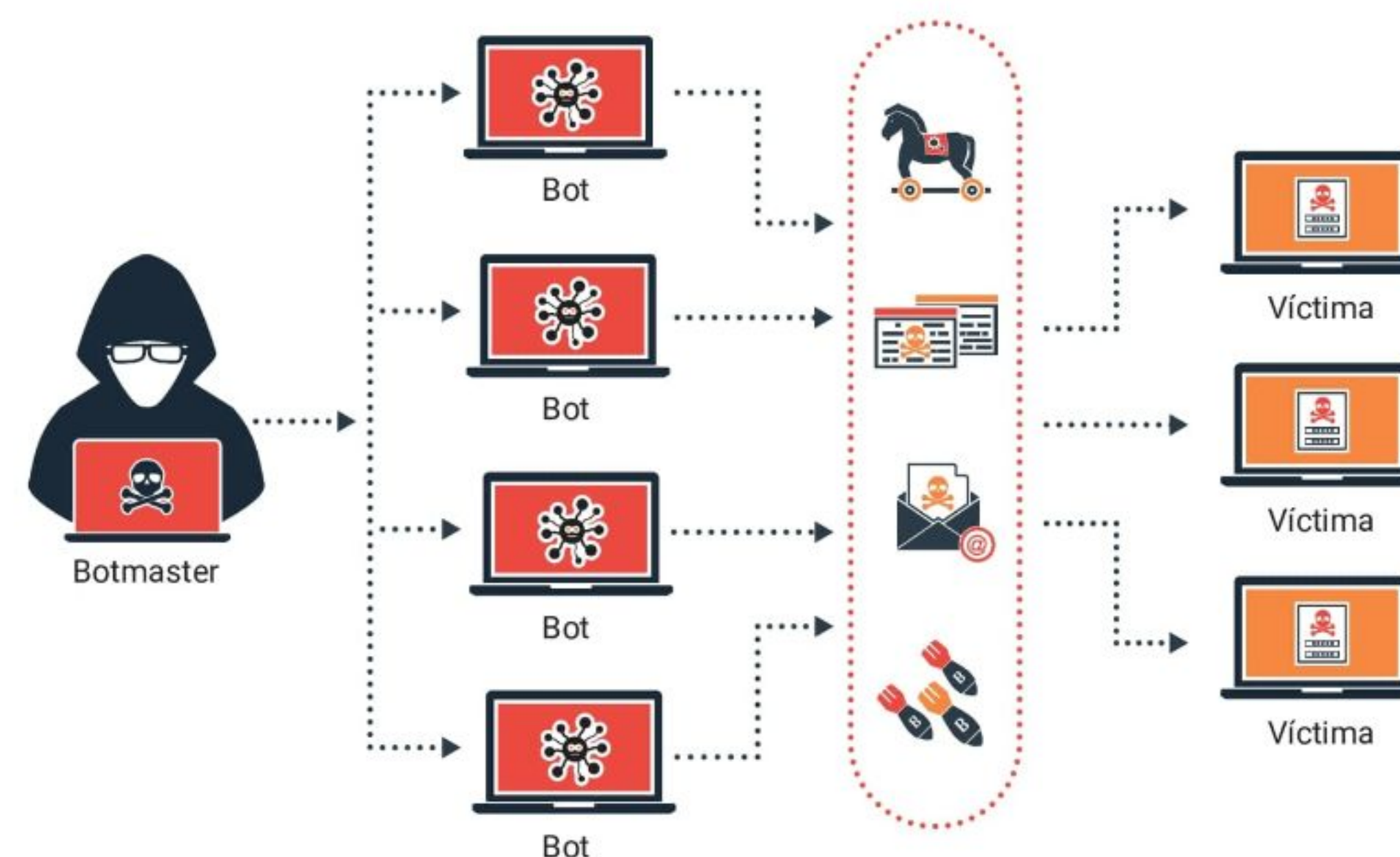


Figura 6.7. Botnets.

- **Apps maliciosas**, cuando instalamos una app en nuestro dispositivo móvil, esta nos pide concederle una serie de permisos. A veces, estos permisos no tienen relación con la funcionalidad de la app o descargamos una app poco fiable que acaba por infectar nuestro dispositivo, tomar control y robar la información que tenemos almacenada en él como contactos, credenciales, imágenes, vídeos, etcétera.

¿Cómo nos protegemos? Cuando se trata de descarga de apps, lo primero que debemos tener en cuenta es utilizar tiendas oficiales. Además, debemos revisar las valoraciones y comentarios de otros usuarios e información del desarrollador. Al instalarla, nos pedirá aceptar una serie de permisos, que no debemos dar a no ser que esté relacionado con la función de la app. Por ejemplo, nunca le daríamos permiso a una app «Linterna» para acceder a nuestros contactos ¿verdad?⁴.



Figura 6.8. Aplicaciones maliciosas.

Aunque los malos no descansan y siguen inventando nuevas formas de fastidiar al prójimo, ya tenemos una idea de los tipos de amenazas más frecuentes, y de cómo protegernos frente a ellas; por cierto, en la página de la OSI se citan casos reales de cada una de las amenazas descritas. Es muy recomendable leerlas para mentalizarnos de que estas cosas ocurren de verdad.

Recordemos: todos disponemos de dos armas muy eficaces frente a este tipo de amenazas, la prudencia y la información. Actuemos sensatamente y mantengámonos informados.

Otro aspecto importante que hay que conocer es cómo se propaga el software malicioso:

¿Cómo se propagan los virus informáticos?

A continuación, describimos algunos de los medios habituales que usan los virus informáticos para infectar a sus víctimas:

⁴ <https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos>

- **Virus de correo electrónico**, el correo electrónico es uno de los medios favoritos para transmitir los virus informáticos a cualquier parte. Estos virus se pueden «contraer» por correo electrónico:

- Abriendo archivos adjuntos. Con nombres habitualmente inofensivos (como «Su itinerario de vuelo»), son tipos de archivos de programa ejecutables (.com, .exe, .zip, .dll, .pif, .vbs, .js o .scr) o archivos de macro (.doc, .dot, .xls, .xlt, .xls, .xlsm, .xsltm...).
- Abriendo un correo con un mensaje infectado. Hoy en día, impulsados por la proliferación de gráficos enriquecidos, colores y ornamentos, algunos virus se transmiten en el cuerpo HTML del propio correo. Muchos servicios de correo electrónico desactivan el HTML de forma predeterminada hasta que el usuario confirma que confía en el remitente.

- **Virus de mensajería instantánea**, los virus también se distribuyen por medio de la mensajería instantánea (MI). Skype, Facebook Messenger, Windows Live Messenger y otros servicios de MI se utilizan inadvertidamente para propagar virus a los contactos a través de vínculos infectados que se reciben en mensajes de chat.

Estos virus de mensajería instantánea y redes sociales se extienden rápidamente por todas partes porque es mucho más fácil conseguir que alguien haga clic en un vínculo incluido en un mensaje procedente de una persona en la que confía que en otro incluido en un correo que envía un desconocido.

- **Virus de intercambio de archivos**, los servicios que se usan para compartir archivos entre pares, como Dropbox, SharePoint o ShareFile, también se pueden utilizar para propagar virus. Estos servicios sincronizan archivos y carpetas con cualquier equipo asociado a una cuenta determinada, de modo que cuando alguien (involuntariamente o por cualquier otra causa) carga un archivo que contiene un virus en una cuenta de intercambio de archivos, dicho virus se descarga en el equipo de todos los usuarios que tengan acceso a esa carpeta compartida.

Algunos servicios de intercambio de archivos, como Google Drive, analizan los archivos cargados en busca de virus (aunque esto solo lo hace con los que pesan menos de 25 MB, lo que deja vía libre a los que propagan virus, que lo único que han de hacer es asegurarse de que los archivos infectados sean de un tamaño superior).

No obstante, casi todos los demás servicios no buscan virus en ningún archivo, así que es responsabilidad tuya garantizar tu protección contra las amenazas potenciales contenidas en el archivo que las otras personas vayan a descargar.

- **Virus de descarga de software**, las infecciones de antivirus falsos son uno de los tipos más comunes de descargas de software que llevan virus. Los estafadores y ciberdelincuentes recurren a ventanas emergentes y anuncios con mensajes intimidatorios a fin de hacer creer a los usuarios que se ha detectado un virus inexistente en el PC, y los conminan a descargar su software «antivirus» para neutralizar la amenaza.



En lugar de quitarle los virus al equipo, este antivirus falso infecta el PC con malware, lo cual, muchas veces, tiene consecuencias devastadoras para los archivos, el disco duro y la información personal de la víctima.

- **Software sin parchear vulnerable**, por último, uno de los medios más comunes (y que más a menudo se pasa por alto) de propagación de virus es el software sin parchear.

Se trata de programas y aplicaciones en los que no se han instalado las últimas actualizaciones de seguridad proporcionadas por el desarrollador con el objeto de tapar brechas de seguridad en el propio software.

El software sin parchear es motivo de grandes quebraderos de cabeza en lo que atañe a la ciberseguridad para negocios y organizaciones, pero dado que los delincuentes explotan vulnerabilidades en versiones desactualizadas de programas tan populares como Adobe Reader, Java, Microsoft Windows o Microsoft Office, los ciudadanos de a pie también corremos mucho riesgo de infección⁵.

Con la información anterior podemos entender los tipos más habituales de software malicioso y cómo se propagan; lo lógico sería, ahora, aprender a identificar los síntomas que permiten saber si los equipos y dispositivos están infectados, para terminar con las indicaciones necesarias para resolver el problema, pero antes es importante entender los siguientes conceptos:

ARGOT TÉCNICO

- **Acción preventiva:** acción tomada para eliminar la causa de una (no conformidad potencial u otra) situación potencial no deseable⁶.
- **Acción correctiva:** acción tomada para eliminar la causa de una (no conformidad detectada u otra) situación no deseable⁷.
- **Corrección:** acción tomada para eliminar una (no conformidad o) situación no deseable detectada⁸.

La acción preventiva se toma para prevenir que algo suceda, mientras que la acción correctiva se toma para evitar que vuelva a producirse.

Hemos extraído estas definiciones de las que figuran en la norma ISO 9000, en su versión online, modificándolas ligeramente para facilitar su comprensión.

⁵ <https://www.avg.com/es/signal/what-is-a-computer-virus>

⁶ <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-3:v1:es>

⁷ <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-3:v1:es>

⁸ <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-3:v1:es>

Hemos recurrido a esta fuente para proporcionar al lector unas definiciones que le permitan entender claramente la diferencia entre corregir, tomar una acción correctiva y prevenir; en el lenguaje de la gestión de calidad se habla de no conformidades, pero en el contexto de la presente obra utilizamos el concepto de situación no deseable, entendiendo que no es deseable que nuestros equipos se infecten con software malicioso, pero hemos preferido dejar entre paréntesis las referencias a las no conformidades, por respeto a la fuente.

Veamos un ejemplo. En una dirección de correo hemos recibido un mensaje con un archivo adjunto que no hemos identificado como malicioso y lo hemos abierto: el equipo se ha infectado con un virus. La corrección es desinfectar el equipo, para lo cual instalamos un antivirus, que sería la acción correctiva; y clasificamos el origen del correo como spam para no volver a abrir sus mensajes, que sería la acción preventiva.

La moraleja es que lo que hay que hacer es prevenir, para eso están los antivirus y los cortafuegos, además de actuar con prudencia y mantenernos informados.

¿Cómo podemos saber si un equipo está infectado?

Recurramos a la OSI, que nos ofrece una lista de síntomas de que un equipo pueda estar infectado por un virus:

- *Lentitud de funcionamiento.*
- *Los programas no funcionan.*
- *El equipo se reinicia o bloquea sin razón.*
- *El antivirus ha desaparecido.*
- *Archivos personales bloqueados.*
- *La impresora no funciona.*
- *Ventanas emergentes cada poco tiempo.*
- *Descargas lentas.*
- *Mis contactos tienen correos míos que yo no he enviado.*
- *Mi navegador hace lo que quiere.*⁹

No siempre lo que causa los problemas citados es un virus, pero el software malicioso puede ser la causa de ello, por lo que conviene actuar en consecuencia.

Recomendamos ir a las páginas citadas en el sitio de la OSI, tienen mucha y muy buena información al respecto, incluido un chat para consultas. No solo tiene información sobre ordenadores también se puede encontrar información sobre móviles, principalmente para Android.

⁹ <https://www.osi.es/es/actualidad/blog/2017/02/23/10-sintomas-de-un-equipo-infectado>



Recordemos el título del apartado, *Detección y eliminación de virus y troyanos*; sabemos lo que son los virus, los troyanos y otros tipos de software malicioso, cómo se propagan y cuáles son algunos de los síntomas de que el equipo está infectado. Ya podemos hablar de la detección y eliminación de estos molestos huéspedes.

Vamos a comentar la detección y eliminación de software malicioso en general, pues en ese grupo están incluidos los virus y los troyanos.



Figura 6.9. Software malicioso.

En primer lugar, vamos a transcribir un texto de la Comisión Federal de Comercio del Gobierno de Estados Unidos (los sitios web de la Administración estadounidense suelen ser muy buenos y cada vez hay más en español), ya que trata el tema de manera sencilla y rigurosa:

¿Cómo reconocer, eliminar y evitar los programas maliciosos?

Los programas maliciosos, también conocidos como malware o software malicioso, son una de las mayores amenazas para la seguridad de su computadora, tableta, teléfono y demás dispositivos. El software malicioso contiene virus, programas espía o spyware y otros programas indeseados que se instalan secretamente en su dispositivo. Una vez que el programa malicioso está instalado en su dispositivo, los delincuentes pueden usarlo para robarle información delicada, enviarle anuncios indeseados o inapropiados, exigirle un pago para decodificar datos encriptados en lo que se conoce como ataque de secuestro de datos o ransomware, y debilitar la seguridad de su dispositivo exponiéndolo a otros ataques de programas maliciosos. A continuación, se describen las maneras de reconocer, eliminar y evitar los programas maliciosos.

¿Cómo puede saber si tiene instalado un programa malicioso?

Fíjese si detecta algo inusual en el funcionamiento de su teléfono, tableta o computadora. Si su dispositivo tiene alguno de los siguientes síntomas, podría estar infectado con un programa malicioso:

- Repentinamente se vuelve más lento, deja de funcionar o muestra mensajes de error.
- No se apaga o no se reinicia.
- No le permite eliminar un programa.
- Muestra muchas ventanas emergentes, anuncios inapropiados o anuncios que interfieren con el contenido de la página.
- Muestra anuncios en lugares donde generalmente no aparecerían, como sitios web del gobierno.
- Aparecen barras de herramientas o iconos nuevos e inesperados en su navegador o en su escritorio.
- Usa un nuevo motor de búsqueda predeterminado o aparecen nuevas pestañas o sitios web que usted no abrió.
- Cambia reiteradas veces la página principal de internet de su computadora.
- Envía emails que usted no escribió.
- Se queda sin batería más rápidamente de lo que debería.

¿Cómo llega a su dispositivo un programa malicioso?

Los delincuentes maniobran para instalar programas maliciosos en sus dispositivos para poder robarle información personal, como sus nombres de usuario y contraseñas, números de cuenta bancaria o su número de Seguro Social. Usan esta información para cometer robo de identidad. Si piensa que alguien pudo haberle robado su información o identidad, visite RododelIdentidad.gov.

- Los programas maliciosos pueden ingresar a su dispositivo cuando usted abre o descarga documentos o archivos adjuntos o cuando visita un sitio web fraudulento. Su dispositivo podría infectarse con un programa malicioso de las siguientes maneras:
- Al descargar cosas gratis de internet, por ejemplo, descargas ilegales de películas, programas de TV o juegos populares.
- Al descargar contenidos disponibles en sitios de archivos compartidos.
- Al descargar archivos en o de dispositivos externos extraíbles como discos duros externos o memorias miniatura.
- Al hacer clic en enlaces de ventanas pop-up enviadas a su computadora por estafadores de soporte técnico.
- Al hacer clic en anuncios publicados por estafadores en los sitios web que usted visita.
- A través de emails tipo phishing que lo engañan para lograr que usted haga clic en un enlace o abra un archivo adjunto.



¿Cómo eliminar un programa malicioso?

Hágalo usted mismo

1. Deje de hacer inmediatamente compras, trámites bancarios y cualquier otra actividad en línea que involucre nombres de usuario, contraseñas o cualquier otra información delicada hasta que elimine todos los rastros del programa malicioso en su dispositivo.
2. Fíjese si su dispositivo tiene un programa de seguridad (antivirus), si no lo tiene, descárguelo. Busque recomendaciones en sitios web de comentarios y opiniones independientes haciendo una búsqueda en internet. También pídale recomendaciones a amigos y familiares. Algunos programas que dicen ser un software de seguridad para protegerlo contra los programas maliciosos son programas maliciosos, así que es importante que investigue.
3. Asegúrese de que su programa esté actualizado. Fíjese que todos los programas estén actualizados, esto incluye el sistema operativo, el software de seguridad, las aplicaciones y demás. Considere habilitar las actualizaciones automáticas para que su programa se mantenga actualizado en todo momento.
4. Haga un escaneo del dispositivo para ver si tiene un programa malicioso. Ejecute un escaneo de seguridad o de detección de programas maliciosos. Elimine todo lo que el programa identifique como un problema. Quizás tenga que reiniciar su dispositivo para que se apliquen los cambios. Vuelva a escanear el dispositivo para asegurarse de que no quede ningún rastro del programa malicioso. Si el resultado del escaneo dice que no hay más problemas, es probable que haya eliminado el programa.

Si no logra reparar su dispositivo siguiendo los pasos 1 a 4, tal vez pueda resolver el problema siguiendo los pasos 5 y 6. Al usar cualquiera de estas opciones, usted se arriesga a perder algunos datos. Si hizo copias de seguridad con regularidad, minimizará esta pérdida de datos

5. Recuperación de su sistema operativo. Para averiguar cómo hacer una recuperación de su sistema operativo (como Windows o macOS), visite el sitio web del fabricante de su dispositivo. Usualmente, hacer una recuperación del sistema le permitirá conservar muchos de los datos almacenados en el dispositivo, así que es una buena alternativa en lugar de reinstalar su sistema operativo (paso 6). Siempre y cuando, elimine el problema del software malicioso. Después de hacer la recuperación de su sistema operativo, le conviene volver a los pasos 2, 3 y 4 para asegurarse de que eliminó el programa malicioso.
6. Reinstalación de su sistema operativo. Para averiguar cómo reinstalar su sistema operativo (como Windows o macOS), visite el sitio web del fabricante de su dispositivo. Reinstalar su sistema es la manera más segura de limpiar un dispositivo infectado, pero perderá todos los datos almacenados en el dispositivo que no haya guardado en una copia de seguridad.



¿Cómo obtener ayuda?

Comuníquese con el fabricante de su dispositivo. Si el aparato está cubierto por una garantía, tal vez pueda obtener soporte técnico gratis, de lo contrario, es posible que tenga que pagar para obtener ayuda. Antes de buscar ayuda, anote el número de modelo y de serie de su dispositivo y el nombre de cualquier software que haya instalado.

Cuando esté buscando ayuda, recuerde que debe tener cuidado con los estafadores de soporte técnico. Estas son dos cosas que hay que saber para evitar a un estafador de soporte técnico:

- Las compañías tecnológicas legítimas no se comunicarán con usted por teléfono, email ni mensaje de texto para decirle que su computadora tiene un problema.
- En las advertencias de seguridad de tipo pop-up de las verdaderas compañías tecnológicas nunca le pedirán que llame a un número de teléfono.

Si detecta cualquiera de estas dos cosas, ya sabe que es una estafa.

¿Cómo evitar los programas maliciosos?

Los estafadores engañan a las personas para lograr que hagan clic en enlaces desde los que descargarán virus, programas espía y otros programas indeseados, y a menudo los agrupan dentro de descargas gratis. A continuación, algunas maneras de evitar los programas maliciosos:

- Instale un programa de seguridad (antivirus) y manténgalo actualizado, también use un firewall. Configure su programa de seguridad, navegador de internet y sistema operativo para que se actualicen automáticamente.
- No debilita los ajustes de seguridad de su navegador. Usted puede minimizar las descargas «drive-by» o agrupadas si mantiene los ajustes de seguridad predeterminados de su navegador.
- Cuando instale un programa nuevo, lea cada una de las pantallas. Si no reconoce un programa, o recibe indicaciones para instalar un programa que viene junto con otros, rechace el o los programas adicionales o salga del proceso de instalación.
- Obtenga programas reconocidos directamente de la fuente. Los sitios web que ofrecen un montón de navegadores diferentes, lectores PDF y otros programas populares gratuitamente tienden a incluir programas maliciosos.
- Preste atención a las advertencias de seguridad de su navegador o explorador. Hay varios navegadores que vienen con un sistema de escaneo de seguridad preinstalado, que lo advierten antes de que visite una página web infectada o descargue un archivo malicioso.
- En lugar de hacer clic en un enlace que le llegue en un email o mensaje de texto, ingrese el URL de un sitio web confiable directamente en su navegador. Los delincuentes envían emails de tipo phishing para engañarlo y lograr que haga clic en un enlace o abra un archivo adjunto que podría descargarle un programa malicioso.



- No haga clic en las ventanas pop-up ni en los anuncios con información sobre el funcionamiento de su computadora. Los estafadores insertan programas indeseados en los mensajes pop-up o en anuncios que le advierten que la seguridad o funcionamiento de su computadora está en riesgo. Evite hacer clic en estos anuncios si desconoce la fuente.
- Escanee los dispositivos USB y otros dispositivos externos antes de usarlos. Estos dispositivos pueden estar infectados con programas maliciosos, especialmente si los usa en lugares con mucho público, como estaciones de impresión de fotos o computadoras públicas.

Reporte los programas maliciosos

Si piensa que su computadora tiene un programa malicioso, reporte el incidente a la FTC en [ReporteFraude.ftc.gov](https://www.ftc.gov/ReportFraud) o ante el Centro de Quejas de Delitos Informáticos del FBI (IC3)¹⁰.

Los sitios citados en los párrafos anteriores corresponden a servicios de la Administración estadounidense; en España podemos recurrir a la Oficina de Seguridad de Internauta (OSI), ya citada, o a los servicios de Guardia Civil y Policía, que tienen unidades especializadas en ciberdelincuencia.

Tengamos en cuenta las advertencias de los profesionales:

Nunca subestimes los peligros del malware

El software malicioso acecha en todos los recodos de internet, puede afectar a cualquiera y producir daños importantes por lo que es necesario tratar el problema a tiempo y tomar las medidas preventivas adecuadas. Además de usar programas especiales y de llevar a cabo un mantenimiento preventivo, no hay que olvidar ser cuidadoso y prudente al acceder a internet, ya sea al navegar por la red, al utilizar aplicaciones web, al descargar archivos o al abrir los archivos adjuntos de los correos electrónicos. A pesar de tener esto en cuenta, no existe una protección 100 % segura e incluso los usuarios más precavidos pueden ocasionar la entrada de programas maliciosos en los sistemas. Eliminar malware requiere esfuerzo, pero tiene su recompensa, pues solo un sistema libre de elementos dañinos puede garantizarte la seguridad y el rendimiento que te corresponden¹¹.

Como hemos podido observar, los consejos de las Administraciones y los de los profesionales del sector van en la misma dirección y recogen muchos de los temas vistos en esta obra y en la de Competencias Digitales Básicas¹².

Hemos aprendido a utilizar nuestro ordenador, tableta o móvil, o hemos mejorado la forma de utilizarlos, y tenemos un buen conocimiento del software y del hardware para uso personal y, en muchos casos, también profesional; todo ello da acceso al maravilloso mundo de internet.

¹⁰ <https://consumidor.ftc.gov/articulos/como-reconocer-eliminar-y-evitar-los-programas-maliciosos#Como%20puede>

¹¹ <https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware>

¹² Mas Alique, P. (2022): *Competencias digitales básicas*. Madrid: Ediciones Paraninfo.

Sí, internet es un mundo maravilloso, pero que no está exento de peligros; conocerlos para saber cómo evitarlos y combatirlos nos permitirá sacar lo mejor de la red.



Figura 6.10. Internet.

Dos comentarios antes de finalizar:

Habrán observado que, a lo largo de la presente obra y de la de Competencias Digitales Básicas hemos utilizado diversas fuentes para tratar temas similares o el mismo tema. Esto es debido a que, como hemos repetido insistentemente, es fundamental mantenernos informados; el mundo de la TIC se mueve muy deprisa, y por eso el autor ha querido ofrecer fuentes distintas para que lector interesado pueda tener un amplio repertorio de sitios a los que acudir en busca de información o de ayuda.

Respecto a la ayuda, hay un recurso que no hemos comentado, pero que conviene conocer: cada vez más seguros del hogar ofrecen, dentro de sus prestaciones, asistencia informática; suele ser telefónica o por internet, con la posibilidad de que un técnico se desplace al domicilio del usuario. Puede que revisando nuestra póliza, puedan sacarnos de algún apuro.

► ACTIVIDAD PROPUESTA 6.1

Información sobre virus

¿Recuerda la clasificación de AV-Test?

- Vaya a su página web y busque los tres mejores antivirus para PC y los tres mejores para Android.
- Vaya a sus páginas web y vea qué información ofrecen sobre virus y malware y si tienen un servicio de noticias que le informe periódicamente sobre este mundillo.
- La recomendación es que se suscriba al que considere mejor; suele ser gratis.

► ACTIVIDAD PROPUESTA 6.2

Información

Busque información sobre delitos informáticos, ciberdelincuencia, etc., en los sitios de la Policía Nacional y de la Guardia Civil.



ACTIVIDADES FINALES

DE COMPROBACIÓN

6.1. Un virus informático es:

- a. Un tipo de software malicioso.
- b. Malware que se replica automáticamente.
- c. Un programa diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de otra forma.
- d. Las tres respuestas anteriores son correctas.

6.2. Los virus son altamente contagiosos:

- a. Solo los que son peligrosos.
- b. Solo en Windows.
- c. Porque se replican automáticamente.
- d. Solo en los Mac.

6.3. Troyano:

- a. Gusano.
- b. Software malicioso que simula ser legítimo para engañar al usuario.
- c. Spyware.
- d. Adware.

6.4. Spyware:

- a. App de noticias indiscretas.
- b. Malware utilizado para espiar y obtener datos de usuarios.
- c. Gusano.
- d. Troyano.

6.5. Los virus pueden propagarse:

- a. Por correo electrónico y mensajería instantánea.
- b. Por intercambio de archivos.
- c. Por descarga de software y por software sin parchear.
- d. Las tres respuestas anteriores son correctas.

6.6. El software malicioso puede causar el funcionamiento anómalo de los equipos:

- a. No, si se trabaja con Windows.
- b. Por lo que, si se detecta mal funcionamiento, hay que revisar el equipo en busca de malware.
- c. No, si se trabaja con Linux.
- d. No, si se trabaja con Google.

6.7. El software malicioso contiene:

- a. Información cada vez más dispersa.
- b. Nada preocupante, el software malicioso es inocuo.
- c. Virus, programas espía o spyware y otros programas indeseados que se instalan secretamente en su dispositivo.
- d. Información para mejorar su forma de usar los equipos, nada malo.

6.8. Adware:

- a. Crea vulnerabilidades.
- b. Inunda las pantallas de anuncios no deseados.
- c. Es muy irritante.
- d. Las tres respuestas anteriores son correctas.

6.9. Para eliminar o neutralizar el malware hay que:

- a. Dejar de comprar o de hacer cualquier tipo de gestión que implique información sensible.
- b. Escanear el dispositivo e instalar un antivirus, si no se tiene.
- c. Actualizar el software.
- d. Las tres respuestas anteriores son correctas.

6.10. Ransomware:

- a. Troyano.
- b. No actúa en Windows.
- c. Software malicioso que secuestra archivos, los cifra y pide rescate.
- d. No es delictivo.

6.11. Nunca subestime los peligros del malware:

- a. No se preocupe, el malware suele ser inocuo.
- b. Basta con verificar los programas normales.
- c. Se evitan con las actualizaciones del software.
- d. El software malicioso acecha en todos los recodos de internet, puede afectar a cualquiera y producir daños importantes, por lo que es necesario tratar el problema a tiempo y tomar las medidas preventivas adecuadas.

6.12. Botnet:

- a. Redes de dispositivos infectados.
- b. Un dispositivo infectado pasa a formar parte de la red de botnets.
- c. La red infectada se utiliza para seguir infectando equipos.
- d. Las tres respuestas anteriores son correctas.

6.13. Hay que ser muy cuidadoso con los permisos que se conceden a las apps que se descargan en los dispositivos:

- a. No hace falta si se bajan de la App Store.
- b. Solo si no son de Google Play.
- c. No, si la recomienda un contacto.
- d. Para evitar ser víctimas de aplicaciones maliciosas.



6.14. El software sin parchear es vulnerable:

- a. Pues al no estar actualizado puede presentar brechas de seguridad.
- b. Solo si se trabaja con Linux.
- c. No, si es de una marca reconocida.
- d. No, si tenemos un antivirus.

6.15. Gusano:

- a. Troyano.
- b. Spyware.
- c. No existe ningún virus ni malware con este nombre.
- d. Software malicioso que ataca a redes de dispositivos saltando de uno a otro.

DE APLICACIÓN

6.16. En la Unidad se han comentado los tipos más habituales de malware (sean o no virus). Busque información sobre más tipos de virus y de software malicioso.

6.17. Busque información sobre troyanos, tipos, ejemplos reales, etcétera.

6.18. Busque información sobre spyware, tipos, ejemplos reales, etcétera.

6.19. Busque información sobre gusanos, tipos, ejemplos reales, etcétera.

6.20. Busque información sobre ransomware, tipos, ejemplos reales, etcétera.

6.21. Busque información sobre adware, tipos, ejemplos reales, etcétera.

6.22. Busque información sobre botnets, tipos, ejemplos reales, etcétera.

6.23. Busque información sobre aplicaciones maliciosas, tipos, ejemplos reales, etcétera.

6.24. Busque información sobre virus de correo electrónico y mensajería instantánea, tipos, ejemplos reales, etcétera.

6.25. Busque información sobre virus de descarga de software, tipos, ejemplos reales, etcétera.

6.26. Busque información sobre la recuperación del SO, para aprender a hacerlo, caso de ser necesario.

6.27. Busque información sobre la reinstalación del SO, para aprender a hacerlo, caso de ser necesario

6.28. Software malicioso y Android. ¿Qué nos puede suceder en el móvil?

6.29. Software malicioso y Linux. ¿Qué nos puede suceder?

6.30. Software malicioso y macOS. ¿Qué nos puede suceder?