

# Manual de privacidad y seguridad en internet

Diego Chiquero Mena

03 febrero 2021



# Privacidad & Seguridad en internet

---

UN MANUAL DE LECTURA RECOMENDADO PARA  
CONOCER Y PROTEGERNOS DE LOS **CIBERATAQUES**

# Índice general

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>Prólogo</b>                                                          | <b>6</b>  |
| <b>Sobre el autor</b>                                                   | <b>8</b>  |
| <b>1 Privacidad y Seguridad en Internet</b>                             | <b>9</b>  |
| 1.1 Introducción . . . . .                                              | 9         |
| 1.2 Privacidad . . . . .                                                | 10        |
| 1.3 Seguridad . . . . .                                                 | 10        |
| 1.4 RGPD (Reglamento general de protección de datos) . . . . .          | 11        |
| 1.5 Aviso legal, política de privacidad y política de cookies . . . . . | 11        |
| <b>2 Gestión de la privacidad</b>                                       | <b>13</b> |
| 2.1 Gestionando la privacidad . . . . .                                 | 13        |
| 2.2 Datos personales sensibles . . . . .                                | 13        |
| 2.3 Oversharing o sobreexposición . . . . .                             | 14        |
| 2.4 Privacidad en tus cuentas . . . . .                                 | 14        |
| 2.5 Navegación privada . . . . .                                        | 14        |
| 2.6 Cookies . . . . .                                                   | 16        |
| 2.7 La nube . . . . .                                                   | 17        |
| <b>3 Gestión de la seguridad en equipos físicos</b>                     | <b>18</b> |
| 3.1 Gestionando la seguridad en los equipos . . . . .                   | 18        |
| 3.2 Equipo local y dispositivos móviles . . . . .                       | 18        |
| 3.3 Router . . . . .                                                    | 19        |
| 3.4 Actualizaciones . . . . .                                           | 20        |
| 3.5 Antivirus, antimalware, antispyware y firewall . . . . .            | 20        |
| 3.6 Copias de seguridad . . . . .                                       | 21        |

|          |                                               |           |
|----------|-----------------------------------------------|-----------|
| <b>4</b> | <b>Gestión de la seguridad en la red</b>      | <b>22</b> |
| 4.1      | Gestionando la seguridad en la red . . . . .  | 22        |
| 4.2      | Contraseñas . . . . .                         | 22        |
| 4.3      | Protocolo https . . . . .                     | 22        |
| 4.4      | Compras y transacciones . . . . .             | 22        |
| 4.5      | Wi-Fi . . . . .                               | 22        |
| 4.6      | Plugins o extensiones . . . . .               | 22        |
| 4.7      | Descargas . . . . .                           | 23        |
| 4.8      | Cierre de sesiones . . . . .                  | 23        |
| <b>5</b> | <b>Amenazas</b>                               | <b>24</b> |
| 5.1      | Principales amenazas . . . . .                | 24        |
| 5.2      | Virus . . . . .                               | 24        |
| 5.3      | Gusanos informáticos . . . . .                | 24        |
| 5.4      | Troyanos . . . . .                            | 24        |
| 5.5      | Spyware o software espía . . . . .            | 24        |
| 5.6      | Phishing / pharming / typosquatting . . . . . | 24        |
| 5.7      | Vishing . . . . .                             | 25        |
| 5.8      | Smishing . . . . .                            | 25        |
| 5.9      | Spam o correo malicioso . . . . .             | 25        |
| 5.10     | Toolbars . . . . .                            | 25        |
| 5.11     | Usurpación de identidad . . . . .             | 25        |
| 5.12     | Vulnerabilidades . . . . .                    | 25        |
| 5.13     | Cryptohacking . . . . .                       | 25        |
| 5.14     | Plugins maliciosos . . . . .                  | 25        |
| 5.15     | SIM Swaping . . . . .                         | 25        |
| 5.16     | Shoulder surfing . . . . .                    | 26        |
| <b>6</b> | <b>Otros conceptos relacionados</b>           | <b>27</b> |
| 6.1      | Otros conceptos que debemos conocer . . . . . | 27        |
| 6.2      | Metadatos . . . . .                           | 27        |
| 6.3      | Huella digital o reputación online . . . . .  | 27        |
| 6.4      | Eliminar el historial de búsquedas . . . . .  | 27        |

|     |                                                         |    |
|-----|---------------------------------------------------------|----|
| 6.5 | Constatar la información . . . . .                      | 27 |
| 6.6 | Otras utilidades . . . . .                              | 27 |
| 6.7 | INCIBE (Instituto nacional de ciberseguridad) . . . . . | 28 |
| 6.8 | OSI (Oficina de seguridad del internauta) . . . . .     | 28 |

# Prólogo

Este manual aglutina de manera filtrada y tamizada una amplia y detallada parte del conocimiento e información de relevancia que puedes encontrar en la web sobre privacidad y seguridad en internet, de forma ordenada y estructura. Además encontrarás en la bibliografía todas las fuentes que han hecho posible la elaboración y documentación de este manual, para que puedas contrastar por ti mismo dichas fuentes.

Entenderás las diferencias entre los conceptos de privacidad y seguridad en internet, para que de este modo puedas hacer una buena configuración y uso de éstas.

Aprenderás buenas prácticas en la gestión de la privacidad, así como la manera más adecuada de gestionar la seguridad tanto en los equipos (PC, tables, smartphones, etc.), como en la red de datos.

Conocerás las principales amenazas que existen en el uso de las tecnologías y el mundo digital.

Y por último, pero no por ello menos importante, se abordarán otros conceptos relacionados con los ciberdelitos, la huella digital, la importancia de ser selectivos con la información online y otros aspectos más.

Para concluir, también encontrarás a lo largo del manual multitud de enlaces que te llevarán a más información ampliada sobre las temáticas, así como una extensa lista de recursos y herramientas para que puedas llevar tu privacidad y seguridad en internet al siguiente nivel.

Si quieres contribuir y ayudar a nutrir de más contenido de valor este manual, por favor, no lo dudes y ponte en contacto conmigo, estaré encantado que colaboremos. Encontrarás mis datos de contacto en el siguiente apartado *sobre el autor*.

Este manual está disponible en el repositorio Github: [diegochiquero/manual-de-privacidad-y-seguridad-en-internet](https://github.com/diegochiquero/manual-de-privacidad-y-seguridad-en-internet). Y ha sido escrito en R-Markdown empleando el paquete [bookdown](#) cuya guía encontrarás en (Xie, 2021).

Imagen portada (Katemangostar - Freepik, 2021)

Esta obra está bajo la [licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](#).



# Sobre el autor



Hola, mi nombre es Diego.

Y lo primero que me gustaría hacer, es agradecerte que hayas decidido leer este manual. Ya que éste hecho, hace que las horas de dedicación, esfuerzo, documentación y contrastación de fuentes hayan merecido la pena.

El propósito de este manual es hacerte consciente de los peligros de navegar por internet, de lo vulnerable y expuesto que puedes llegar a estar en el uso de las tecnologías y a su vez dotarte de conocimientos, consejos y herramientas para poder hacer una buena gestión de la web de manera segura y privada.

De formación académica Técnico superior en desarrollo de aplicaciones web. Para concluir y a modo de breve presentación, haré referencia a mi extracto de LinkedIn:

Apasionado de las tecnologías, el espíritu empresarial y la programación.

Plenamente convencido que las competencias transversales pueden marcar la diferencia, que el derecho nos asiste a todos y que un mundo mejor es posible.

En continuo proceso de crecimiento personal y profesional.

Diego Chiquero Mena

Puedes contactar conmigo en [chiquerodiego@yahoo.es](mailto:chiquerodiego@yahoo.es)

Más sobre mí [Diego Chiquero Mena](#)



# Capítulo 1

## Privacidad y Seguridad en Internet

### 1.1 Introducción

En estos últimos años hemos podido ver como la evolución de las IT (Tecnologías de la información) y el paso de la Web1.0. a la Web 2.0., nos ha permitido a muchos de nosotros como usuarios interactuar los unos con los otros subiendo y compartiendo todo tipo de contenidos. La aparición de las Redes sociales ha traído con ellas, la posibilidad de publicar fotos, videos, información, comentarios, reseñas, etc. a través de cualquier dispositivo, ya sea un PC, tablet o smartphone. Y no solo eso, sino que además, también nos ha abierto un amplio abanico de posibilidades con las que podemos gestionar cuentas bancarias, hacer compras online, trámites telemáticos y un sinfín de gestiones que hasta hace tan solo unos años atrás eran difíciles de imaginar.

Como consecuencia de ello, el enorme conglomerado de información sensible que se encuentra disponible en internet, hace que nosotros como usuarios estemos en el punto de mira de ciberdelincuentes y expuestos a todo tipo de ciberataques. En esta línea, este manual contribuye a enseñarte, aconsejarte y proveerte de herramientas necesarias para prevenir, evitar y paliar en la medida de lo posible todos los riesgos y peligros a los que estamos expuestos en nuestro uso diario de las tecnologías.

Por lo tanto, en lo sucesivo iras viendo el porqué de la importancia de velar de manera activa por tu privacidad y seguridad en internet haciendo una buena gestión de éstas. También te ayudará a conocer y reconocer la amplia lista de ciberdelitos que actualmente están más extendidos.

En estás [estadísticas](#) publicadas por el Obsevatorio Español de Delitos informáticos ([OEDI, 2021](#)) puedes ver el porqué de cuidar tu privacidad y seguridad en internet. En ellas se expone una exhaustiva lista de ciberdelitos y sus recurrencias cronológicas.

## 1.2 Privacidad

La privacidad es aquello que se lleva a cabo en un ámbito reservado; en Internet podría entenderse como el control que ejercemos sobre nuestra información para limitar la cantidad de personas autorizadas a verla, así como la cantidad de contenido expuesto. Esto incluye datos personales, fotografías, documentos, etc.

Internet es una herramienta que nos permite la interacción entre dos o más personas. Siendo ejemplo de los anteriores sitios como Facebook y Twitter, Redes Sociales en donde las personas pueden compartir públicamente opiniones, noticias, sentimientos, ideas, fotografías, videos, etc. Por ello es necesario considerar que Internet es un espacio abierto al mundo, por lo tanto, cualquier acción que se haga va a tener un impacto global y permanente. Por ejemplo, imagina una publicación de la cual puedas arrepentirte (como una fotografía u opinión) no solo podrá ser vista por millones de usuarios, sino que también será prácticamente imposible de borrar completamente de la red.

También puede resultar peligroso publicar datos que puedan identificarte, como la dirección, teléfonos, lugar de estudio o trabajo, días de vacaciones, etc. Esto puede resultar todavía más complicado si posees una gran lista de amigos a los que no conoces personalmente.

Por todo lo que se ha mencionado en éstas últimas líneas, es de suma importancia que antes de publicar algo, pienses en las consecuencias que puede conllevar divulgar información sensible en sitios públicos y de los cuales no siempre se tiene un control directo ([ESET, 2021](#)).

## 1.3 Seguridad

La seguridad en internet son todas aquellas precauciones que son tomadas para proteger todos los dispositivos informáticos, así como la red de internet que pueden ser afectados por delincuentes cibernéticos. Además de ser una rama de la seguridad informática que se dedica a identificar y prevenir todas las amenazas que afectan a la red de redes, siendo una de las herramientas más conocidas los antivirus ([GCFGlobal, 2021](#)).

Entre los peligros más habituales de no hacer un buen uso de la seguridad en la red, nos encontramos, robo de datos bancarios o personales, virus informáticos, phishing, spam, etc. Una lista amplia y exhaustiva será vista la [unidad 5](#) Amenazas.

## 1.4 RGPD (Reglamento general de protección de datos)

El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones han debido ir adaptándose para su cumplimiento. Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo deberán acogerse a la misma ([Wikipedia, 2021c](#)).

En el pasado el uso de datos eran obtenido por omisión, en estos momentos para estar seguros de cumplir con el RGPD se ha de obtener el consentimiento inequívoco o expreso por parte del usuario.

Paralela a la RGPD europea existe una a nivel de España llamada LOPD (Ley orgánica de protección de datos) y cuyo objeto es también garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas y en especial, su honor e integridad personal y familiar.

## 1.5 Aviso legal, política de privacidad y política de cookies

Si una web va a realizar transacciones comerciales de la naturaleza que sea, va a gestionar datos de usuarios o hacer uso de cookies, ha de tener a disposición del usuario la siguiente información de manera detallada. Todas estas políticas están recogidas en el RGPD del apartado anterior. Sin embargo para documentarlo con terminología más cotidiana, en este apartado nos hemos apoyado en la sección de derecho digital de la compañía IONOS by 1&1 en su división IONOS Guía Digital,

- **Aviso Legal:** Se trata de un documento donde se recogen tanto el cumplimiento por parte de la entidad o empresa, conforme a las leyes vigentes en el desarrollo de su actividad, así como los datos referentes a los administradores de la misma.

Todo proyecto de base digital u online con ánimo de lucro, ya sea a través de modelos de patrocinio, publicitarios o compra-venta de productos o servicios, requieren de un aviso legal visiblemente expuesto y a disposición de todos los usuarios. Este requerimiento está recogido en la legislación española en la Ley 34/2002 de Servicios de la Sociedad de la Información y el Comercio Electrónico ([IONOS by 1and1, 2021a](#)).

- **Política de privacidad:** El reglamento general de Protección de Datos de carácter personal, establece que cualquier página web que incluya

un formulario de carácter personal que deban rellenar los usuarios, que incluya un correo de contacto o utilice las redes sociales desde las cuales se puede obtener información de los usuarios, está obligada a disponer de una política de privacidad (IONOS by land1, 2021c).

La política de privacidad se creó con la finalidad de proteger y preservar los derechos del espacio privado de las personas.

- Política de cookies: Una cookie es una pequeña información enviada por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Su propósito principal es identificar al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos (IONOS by land1, 2021b).

Toda web que haga uso de cookies está obligada ponerlo en conocimiento de los usuarios y a solicitar su aceptación.

## Capítulo 2

# Gestión de la privacidad

### 2.1 Gestionando la privacidad

La privacidad en Internet se refiere al control de la información personal que posee un determinado usuario que se conecta a Internet, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación. Por ello en esta unidad vas a tratar de aprender a gestionar la privacidad de manera inteligente para así evitar males mayores ([Wikipedia, 2021a](#)).

### 2.2 Datos personales sensibles

Cuando se habla de datos personales sensibles en la red, se refiere a aquellos datos, que están revelando información privada, como, por ejemplo, el domicilio, o cualquier otra información de carácter privado, costumbres o hábitos. Así como acciones que ubican o determinan a una persona en posibles situaciones futuras que pudiesen abrir una brecha de vulnerabilidad en la vida privada de ésta. Ejemplo: subir a la red que te vas de vacaciones, de manera que estás diciendo a los ciberdelincuentes que tu casa está vacía.

Entrando en un terreno más técnico los datos sensibles son aquellos que, de difundirse indebidamente, podrían afectar la esfera más íntima del ser humano. Ejemplos de este tipo de datos son: el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y las preferencias sexuales.

Por ello, aporta solo los datos necesarios y no te expongas.

## 2.3 Oversharing o sobreexposición

El Oversharing es la sobreexposición de información personal en internet y en su mayoría en los Medios Sociales a través de tus perfiles sociales. Este hecho se presenta continuamente en la actualidad, donde los jóvenes y no tan jóvenes, publican constantemente imágenes o información personal.

De esta manera, tu vida quedan totalmente expuesta y, aunque el propósito de ello sea totalmente lícito e incluso plausible, estos datos, imágenes o información pueden volverse en tu contra por un uso indebido o ilícito por parte de terceros.

Este exceso de información que se puede facilitar en internet, sumado al comportamiento malicioso de otros usuarios, supone un grave riesgo que se corre cada día al señalar tu ubicación, comentar información personal o privada, colgar una imagen o video comprometedores, etc.

Esto no supone un delito en cuestión, pero puede dar lugar al chantaje, ciberacoso o robo de información personal a través de algún tipo de técnica. Además de exponerte al riesgo de un posible robo y/o suplantación de identidad ([Agencia española protección de datos, 2021](#)).

## 2.4 Privacidad en tus cuentas

Prácticamente todo el mundo en menor o mayor medida dispone de cuentas de usuarios en todas sus aplicaciones o servicios en la red. Una de las más conocidas es la cuenta de [Google](#), entre otras, así como la de [Microsoft](#).

En lo que respecta a las redes sociales como, [Facebook](#), [Twitter](#) o [Instagram](#), entre otras muchas más, no debes olvidar que también disponen opciones de privacidad y que en este escenario está en juego tus datos más personales, luego el mejor consejo es establecer una configuración privada en lugar de pública. Ya que estas redes sociales no tienen, por defecto, los niveles más elevados en cuanto a la protección y a la seguridad.

Con referencia a todo lo expuesto, puedes dejar la configuración de privacidad que la cuenta trae por defecto o acomodarla a tus necesidades o preferencias. Dentro de cada cuenta se encuentran todas las opciones de privacidad, como, por ejemplo, historial de búsquedas, actividad de ubicación entre otras.

## 2.5 Navegación privada

La navegación privada es una función de privacidad que conocerás como modo incógnito o modo privado. Su principal característica es que permite

a los navegadores web no almacenar información sobre la página en que navegamos.

La navegación privada te ofrece una sesión temporal que no comparte datos con el navegador, que no guarda información sobre páginas web, ni historial de navegación, caché web, contraseñas, información de formularios, cookies u otros datos de sitios web, borrando éstas y otros archivos temporales cuando finalizamos la sesión ([Muy computer, 2021](#)).

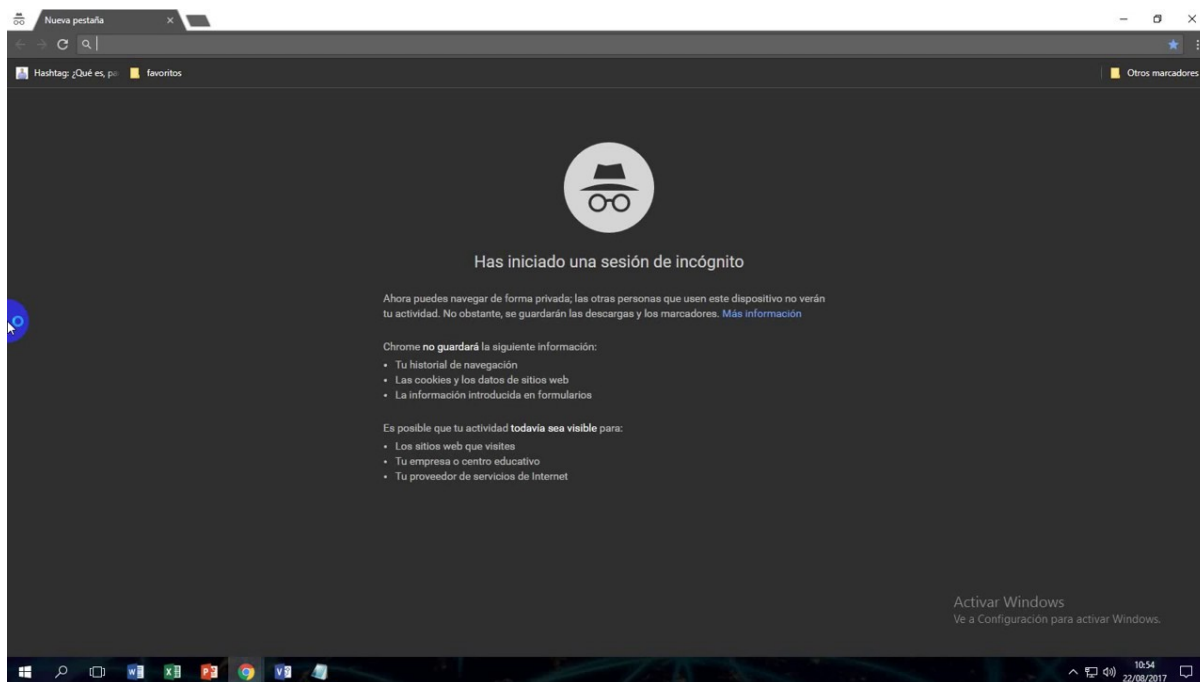


Figura 2.1: Navegación privada navegar Google Chrome.

Ten en cuenta que no es lo mismo navegar privadamente que navegar de forma anónima por Internet, lo que requiere de otras herramientas como [TOR](#).

El uso de la navegación privada resulta conveniente en los siguientes supuestos:

- Transacciones económicas.
- Utilización de un ordenador de terceros.
- Resultados “puros” del motor de búsquedas.

También existen navegadores que protegen tu privacidad sin necesidad de activar la navegación privada, como por ejemplo, [Epic](#), [Brave](#) e incluso buscadores como [DuckDuckGo](#).

Dentro de la navegación tienes además otra herramienta para proteger tu privacidad y se trata de un VPN (son las siglas de Virtual Private Network) ([Wikipedia, 2021d](#)).

Las VPN, son una tecnología de red que permiten una extensión de tu conexión local o LAN, permitiendo conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar. Entre sus ventajas está la de ofrecer una mayor privacidad al ocultar tu localización, pero también, y este el caso que nos compete, el que parezca que tu conexión esté realizándose en otro país concreto, con lo que uno se puede saltar censuras o acceder a contenidos de servicios locales.

Las VPN suelen ser aplicaciones o extensiones de terceros, aunque el navegador [OPERA](#) lo trae por defecto, lo único que tendrás que hacer es activarla desde sus opciones, y se creará una conexión cifrada entre tu dispositivo y un servidor VPN para esconder tu ubicación real.

## 2.6 Cookies

Una cookie es una pequeña información enviada por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

Su propósito principal es identificar al usuario almacenando su historial de actividad de un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos. Esto quiere decir que cada vez que visitas una página web por primera vez, se guarda una cookie en el navegador con un poco de información. Luego, cuando visitas nuevamente la misma página, el servidor pide la misma cookie para arreglar la configuración del sitio y hacer la visita del usuario tan personalizada como sea posible ([Blogthinkbig by telefónica, 2021](#)).

Existe la opción de navegar sin cookies gracias a las sesiones privadas que tienen los distintos navegadores, como has podido ver en el apartado anterior. De esta forma no se almacenará ningún tipo de información en tu ordenador cuando navegues en una web y del mismo modo tampoco recordará nada después al volver a navegar de nuevo.

Es importante que con frecuencia elimines las cookies, ya que como ya sabes manejan información privada y además ocupan espacio en tu dispositivo. Esto lo puedes hacer de dos maneras. Manualmente desde el menú de opciones del navegador o con software específico para tal cometido, como por ejemplo [Ccleaner](#).

Por otro lado si quieres deshacerte de la incómoda notificación de cookies de las web, puedes instalar en el navegador el plugin [I don't care about cookies](#).



## 2.7 La nube

Como ya sabrás el almacenamiento en la nube, es el almacenamiento de datos basado en redes de computadoras, donde los datos están alojados en espacios de almacenamiento virtualizados, también conocidos como servidores y por lo general aportados por terceros. Algunos de estos servicios más conocidos son [Google drive](#), [One drive](#) o [Dropbox](#) entre otros.

Con respecto a ésto, debes tener en cuenta que solo es recomendable compartirlo con personas de confianza, ya que de lo contrario podrían hacer un mal uso de ello, o simplemente una mala gestión que provoque la pérdida de la información.

## Capítulo 3

# Gestión de la seguridad en equipos físicos

### 3.1 Gestionando la seguridad en los equipos

Para poder tener la tranquilidad de que tus equipos tales, como el ordenador, la tablet, el smartphone, el router, etc., estén a salvo de ataques o pérdidas de datos, entre otras, debes mantener una seguridad robusta y confiable en tus equipos.

A lo largo de esta unidad veras que debes hacer y las precauciones que debes tomar para que tus equipos e información estén seguros y a salvo de ciberataques.

### 3.2 Equipo local y dispositivos móviles

Una cuenta de usuario es el conjunto de información perteneciente a un usuario concreto. De esta forma indica al sistema operativo los archivos y carpetas a los que dicho usuario tiene acceso así como la posibilidad de realizar cambios y configuraciones personales ([OSI, 2021b](#)).

Las pautas de seguridad que vas a ver a continuación te van a ser útil, tanto para ordenadores como cualquier tipo de dispositivo móvil, smartwatch y demás.

Todos los equipos informáticos funcionan con una cuenta de usuario, única y personal. Luego una vez, hayas creado la tuya, solo tú debes hacer uso y disfrute de ella. En los ordenadores personales existe la posibilidad de crear varias cuentas de usuarios. Una vez éstas están creadas solo son accesibles mediante contraseña y aunque solo sirva para no olvidarlo, nunca debes de compartirla.

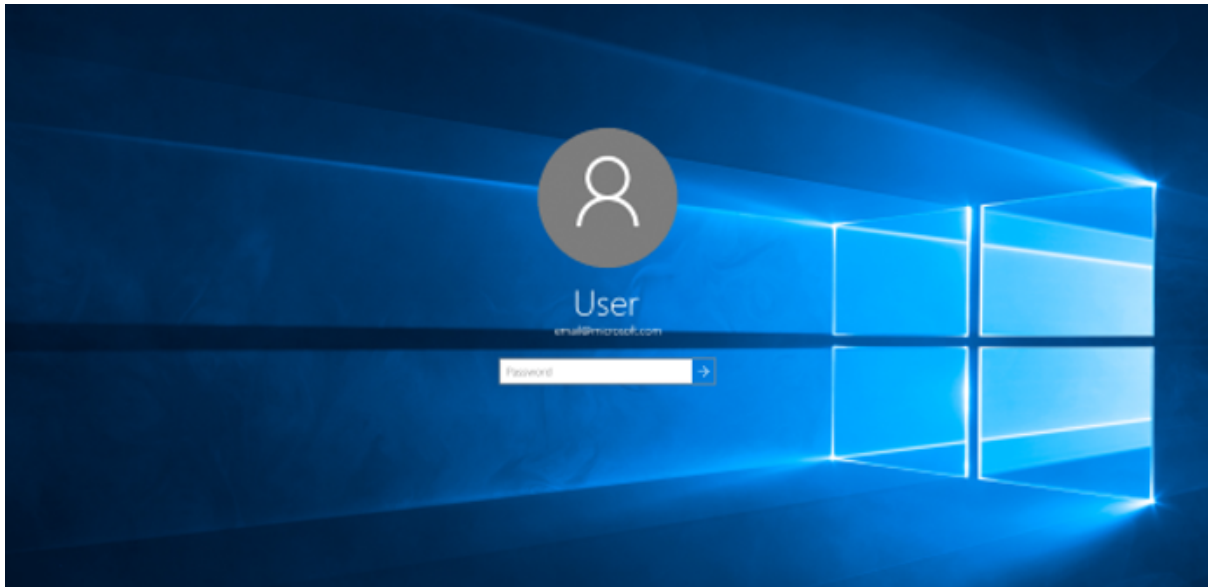


Figura 3.1: Cuenta de usuario windows 10.

### 3.3 Router

Un router es un dispositivo que proporciona conectividad a nivel de red. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiéndose por subred un conjunto de máquinas IP que se pueden comunicar. Además de ser el dispositivo que nos proporciona un punto de acceso Wi-Fi

Dispone de varios niveles de seguridad y estándares de cifrado, para que nadie pueda acceder a nuestra red y poder alcanzar cualquier dispositivo a través de la Wi-Fi.

Ordenados de menor a mayor grado de cifrado:

- [WEP](#) (Wired Equivalent Privacy)
- [WPA](#) (Wi-Fi Protected Access)
- [WPA2](#) (Wi-Fi Protected Access 2)
- [WPA3](#) (Wi-Fi Protected Access 3)

Es importante que cambies la clave que el router trae por defecto y uses el nivel de seguridad WPA2 con el que vas a poder establecer una contraseña de hasta 63 caracteres en lugar de los máximos 29 de la WEP.

Para establecer una capa más de seguridad puedes realizar un [filtrado MAC](#) (Media Access Control). Un filtro MAC consiste en la creación de una lista de dispositivos que tienen permiso para acceder al router, a pesar de que un tercero haya podido obtener la clave wifi.

Este enlace te llevará a un [generador de claves Wi-Fi](#) donde podrás crear de forma automática una clave Wi-Fi segura y robusta.

### 3.4 Actualizaciones

Las actualizaciones de seguridad o parches son elaboradas por los desarrolladores y fabricantes de productos informáticos. Estos pueden tardar desde un día hasta meses para publicar un parche, en función del tipo de vulnerabilidad, dispositivos a los que afecte y otros criterios. Aunque también se realizan para mejoras de otras naturalezas, como, rendimiento, productividad, etc.

Tener actualizados los dispositivos es una medida más de seguridad. Para ello debes actualizarlos cada vez que el dispositivo lo solicita o en su defecto buscar una actualización disponible.

Las actualizaciones no solo corresponden al Hardware (ordenadores, smartphones, etc.), sino que también han de ser realizados en el software (programas), navegadores, antivirus, etc.

La principal función de las actualizaciones son las de mejorar tanto la funcionalidad como la seguridad de los dispositivos o software (OSI, 2021a).

### 3.5 Antivirus, antimalware, antispyware y firewall

Aunque a priori pudiese parecer lo mismo, los antivirus, antimalware, antispyware y firewall, cumple funciones diferentes, pero con un mismo fin, mantener la seguridad de nuestros equipos. La mayoría de estos tipos de software los puedes encontrar en dos modalidades: gratuita y de pago (Enetic, 2021).

- **Antivirus:** Es un programa que detecta la presencia de virus informáticos (software malicioso que altera el funcionamiento normal del ordenador sin que el usuario lo sepa o consienta) y los elimina o repara. Algunos ejemplos de antivirus son: [Avira](#), [Avast](#), [AVG](#), [Virus Total](#) (online), entre muchos más.
- **Firewall o cortafuegos:** Es una parte de la red o el sistema que se realiza para bloquear accesos no autorizados y permitiendo los que sí lo están. Se pueden hacer por medio de software o hardware, y permiten una mayor protección a las redes, especialmente importante en empresas que cuentan con datos que han de ser bien protegidos. El [firewall](#) más conocido es el Windows.
- **Antispyware:** Es un conjunto de herramientas que sirven para prevenir y eliminar Spywares (espías o programas que recopilan información del ordenador para transmitirla a otras personas sin el consentimiento ni conocimiento del propietario del ordenador). Algunos ejemplos de antispyware son: [SpyBot](#), [SuperAntiSpyware](#), [SpywareBlaster](#).

- Antimalware: Es un software encargado de eliminar el software malicioso (malicious-software, malware) del ordenador tras un minucioso análisis del sistema. Algunos ejemplos de antimalware son: [HiJackThis](#), [Anti-malware](#).

Dependiendo de las necesidades pueden ser usados uno o varios, ya que son complementarios entre sí.

### 3.6 Copias de seguridad

Una copia de seguridad o backup en informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas ([Wikipedia, 2021b](#)).

Simplificando el sistema de copias de seguridad que en algunas ocasiones puede llegar a ser complejo, están los siguiente:

- Completas: Del sistema operativo completo, de esta forma al restaurar la copia, dispondremos de nuevo de toda la configuración a nivel de S.O., software instalado, carpetas y archivos. Para este cometido vamos a necesitar de programas de terceros, algunos de ellos con versiones gratuitas y de pago, ejemplo de estos son: [Acronis](#), [AOMEI](#), [EaseUS](#).
- Parciales: En este escenario lo que se hace es salvaguardar las carpetas y archivos personales. Como por ejemplo, carpetas con fotografías, documentos personales y demás.

Y las copias pueden ser mantenidas:

- En almacenamientos externos: Tales como disco duros externos, DVD, entre otros. De esta forma podemos custodiarlos a buen recaudo.
- En la nube: Estos son servicios de terceros accesibles online, ejemplo de ello son: [BackBlaze](#), [Carbonite](#), siendo estos especializados en backups. Pero si tus copias de seguridad se limitan a tus carpetas y archivos personales puedes usar un servicio en la nube, como [Google Drive](#), [Onedrive](#) o [Dropbox](#).

Las copias de seguridad debes realizarlas con la frecuencia que sea necesaria para garantizar tu nivel de seguridad ([Media Cloud, 2021](#)).

## Capítulo 4

# Gestión de la seguridad en la red

### 4.1 Gestionando la seguridad en la red

Some *significant* applications are demonstrated in this chapter.

### 4.2 Contraseñas

Segundo nivel

### 4.3 Protocolo https

Tercer nivel

### 4.4 Compras y transacciones

Cuarto nivel

### 4.5 Wi-Fi

hola

### 4.6 Plugins o extensiones

hola

## 4.7 Descargas

descargas

## 4.8 Cierre de sesiones

cierre

## Capítulo 5

# Amenazas

### 5.1 Principales amenazas

We have finished a nice book.

### 5.2 Virus

virus

### 5.3 Gusanos informáticos

gusanos

### 5.4 Troyanos

troyanos

### 5.5 Spyware o software espía

sypeware

### 5.6 Phishing / pharming / typosquatting

phishing



## **5.7 Vishing**

vishing

## **5.8 Smishing**

smishing

## **5.9 Spam o correo malicioso**

spam

## **5.10 Toolbars**

tool

## **5.11 Usurpación de identidad**

usurpación

## **5.12 Vulnerabilidades**

vulnerabilidades

## **5.13 Cryptohacking**

crypto

## **5.14 Plugins maliciosos**

plugins

## **5.15 SIM Swaping**

sim

## **5.16 Shoulder surfing**

Shoulder

## Capítulo 6

# Otros conceptos relacionados

### 6.1 Otros conceptos que debemos conocer

Esta es la última unidad

### 6.2 Metadatos

For example, we are using the

### 6.3 Huella digital o reputación online

huella

### 6.4 Eliminar el historial de búsquedas

eliminar

### 6.5 Constatar la información

Y en Linux

### 6.6 Otras utilidades

otras

## **6.7 INCIBE (Instituto nacional de ciberseguridad)**

incibe

## **6.8 OSI (Oficina de seguridad del internauta)**

osi

# Bibliografía

- Agencia española protección de datos (2021). *Oversharing o sobreexposición*.
- Blogthinkbig by telefónica (2021). ¿qué son las cookies? *blogthinkbig.com*.
- Enetic (2021). Diferencias entre firewall, antivirus, antispyware y antimalware. *Enetic Soluciones Tecnológicas*.
- ESET (2021). *Guia de privacidad en internet*.
- GCFGlobal (2021). Seguridad en internet. *Goodwill Community Foundation*.
- IONOS by 1and1 (2021a). Aviso legal. *IONOS Guía digital*.
- IONOS by 1and1 (2021b). Política de cookies. *IONOS Guía digital*.
- IONOS by 1and1 (2021c). Política de privacidad. *IONOS Guía digital*.
- Katemangostar - Freepik (2021). Imagen portada.
- Media Cloud (2021). Diferentes tipos de copias de seguridad. *Mediapro*.
- Muy computer (2021). Navegación privada. *muycomputer.com*.
- OEDI (2021). Estadísticas ciberataques. *Obsevatorio Español de Delitos informáticos*.
- OSI (2021a). Actualizaciones. *Oficina de seguridad del internauta*.
- OSI (2021b). Cuentas de usuario. *Oficina de seguridad del internauta*.
- Wikipedia (2021a). Concepto de privacidad. *Wikipedia.org*.
- Wikipedia (2021b). Copias de seguridad. *Wikipedia.org*.
- Wikipedia (2021c). Reglamento general de protección de datos. *Wikipedia.org*.
- Wikipedia (2021d). Vpn. *Wikipedia.org*.
- Xie, Y. (2021). *Bookdown: Authoring Books and Technical Documents with R Markdown*. Chapman and Hall/CRC, Boca Raton, Florida, 2nd edition. ISBN 978-1138700109.