Manual de privacidad y seguridad en internet

Diego Chiquero Mena

01 febrero 2021

Privacidad & **Seguridad** en internet

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

Índice general

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. Y ha sido escrito en R-Markdown empleando el paquete `bookdown` cuya guia encontrarás en (Xie, 2021).

Imagen portada (Katemangostar - Freepik, 2021)


BY NC SA

Sobre el autor

Hola, mi nombre en 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 marcan 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

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 abrierto 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 públicadas 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, 2021b).

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).

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 1and1, 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 1and1, 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

Este es otro ejemplo de índice[1].

2.2 Datos personales sensibles

Hiperlink de ejemplo Google

2.3 Oversharing

Esto es un texto normal que contiene una nota[2]. Puedes escribir tanto como necesites.

2.4 Privacidad en tus cuentas

Cuentas

2.5 Navegación privada

La navegación

2.6 Cookies

La cookies son ...

[1] Esta es la explicación sin más
[2] Aquí irá el texto de tu nota.

2.7 La nube

Que pasa en la nube

Incluso crear varios párrafos, ya que la nota siempre irá al final del documento. En este caso, si haces click serás dirigido al final del artículo (pero puedes volver al punto de lectura fácilmente, ¡haz la prueba!)

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 compartida.

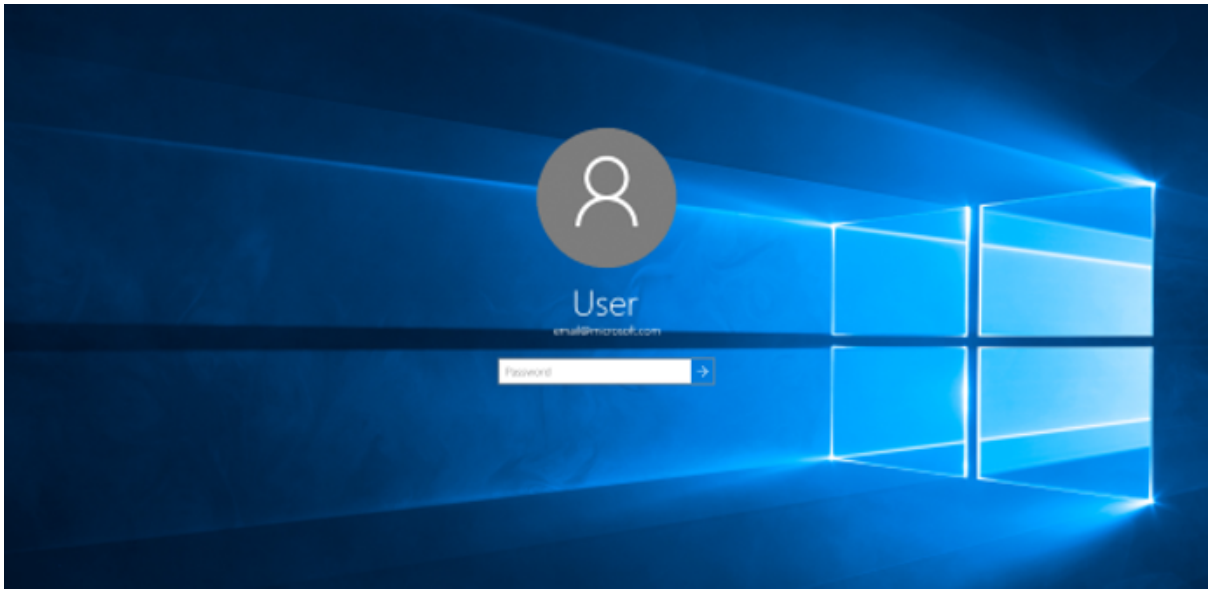

Figura 3.1: Cuenta de usuario windows 10.

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, entendiendo 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 d 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 filtra 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 podras 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 actulizaciones 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, Antimalware.

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, 2021a).

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

span

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 conocewr

Esta es la última unidad

6.2 Metadatos

For example, we are using the **bookdown** package (Xie, 2021) in this sample book

6.3 Huella digital o reputación online

huella

6.4 Eliminar el historial de busquedas

eliminar

6.5 Constastar 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

Enetic (2021). Diferencias entre firewall, antivirus, antispyware y antimalware. *Enetic Soluciones Tenológicas*.

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*.

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). Copias de seguridad. *Wikipedia.org*.

Wikipedia (2021b). Reglamento general de protección de datos. *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.