INTERNET SEGURO (IFCT057PO)

Hispamérica

Internet seguro (IFCT057PO)

Telef. (00 34) 91 028 28 51

Madrid, España

ISBN **978-84-17958-66-4**

Impreso en Madrid (España) – Printed in Madrid (Spain)

Deposito legal: M-30002-2023

ÍNDICE

Módulo 1

Introducción y antivirus

1. Introducción y antivirus

1.1 Introducción a la seguridad

Podemos definir la **seguridad en Internet** como el conjunto de medidas que los internautas deben tomar para navegar con ciertas garantías por la Red, mantener a salvo su privacidad y la integridad de sus PCs.

Una **navegación segura** no sería concebible si nuestros PCs estuviesen infectados por algún tipo de **malware o software malicioso** que, a su vez, abriera puertas traseras (backdoors) que permitieran a los intrusos acceder a nuestros PCs a su antojo.

Por todo ello, entendemos que la seguridad en Internet está estrechamente ligada, entre otros aspectos, a la ausencia de software malicioso en los PCs. Por supuesto, además de contar con un **antivirus residente, programas antispyware y un cortafuegos**, también son necesarias ciertas dosis de prudencia, precaución y sentido común por parte de los internautas cuando navegan por la Red, realizan compras con tarjeta de crédito, acceden a webs de entidades bancarias o descargan software, además de mantener los sistemas operativos actualizados.

1.2 Antivirus. Definición de virus. Tipos de virus

Un **virus o virus informático** es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr **fines maliciosos** sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Además, pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos que solo producen molestias o imprevistos.

Existen multitud de virus informáticos entre los cuales podemos destacar los siguientes:

- **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 pulsan), para luego enviarla al ciberdelincuente.

- **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.

- **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.

- **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.

- **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.

- **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, etc.

1.3 Previo a instalar algún programa

Cuando un equipo es **conectado a la red, se encuentra en potencia de ser atacado** por una inmensa cantidad de **virus** intentado explotar las vulnerabilidades de este. Debido a esto, es imprescindible contar con medidas de protección antes de proceder a la interconexión con otros equipos.

No obstante, a pesar de que el equipo no esté conectado a Internet también corre peligro de ser infectado. Acciones como instalar una memoria externa infectada resulta una brecha de seguridad importante.

Por lo tanto, una de las primeras acciones que tenemos que llevar a cabo cuando tenemos ante nosotros un equipo con instalación limpia es **instalar un antivirus actualizado** desde una fuente segura.

Idealmente, realizaremos la instalación desde un dispositivo de almacenamiento externo que nos garantice que el contenido de este es realmente un antivirus.

1.4 Antivirus. Descarga e instalación

Como hemos mencionado en el punto anterior, es muy aconsejable realizar la instalación desde un dispositivo de almacenaje externo que no se encuentre infectado. Para ello, se debe realizar la descarga desde un equipo que ya se encuentre protegido y grabarlo en la memoria externa. Dicha memoria debe ser analizada antes de ser extraída.

Previo a la introducción de la memoria externa en nuestro ordenador, debemos cerciorarnos de que este no se encuentra conectado a internet. Una vez hecho esto, conectaremos la memoria externa y procederemos a la instalación del antivirus.

A continuación, presentamos como ejemplo el proceso de instalación del antivirus gratuito Avast:

1. Accedemos a su página web www.avast.com

2. Hacemos clic con el botón izquierdo de nuestro ratón en la opción ¨**DESCARGA PROTECCIÓN GRATUITA**¨

3. El archivo se descarga automáticamente y lo copiamos en nuestra memoria externa.

4. Analizamos la memoria externa y, una vez hecho esto, podemos introducirla en el ordenador que queremos proteger.

5. Nos aseguramos de que el equipo no se encuentra conectado a Internet y ejecutamos el archivo.

6. Le concedemos los permisos y pulsamos el botón de instalación.

7. Finalmente, el antivirus se encarga de hacer el resto.

1.5 Otros programas recomendados

Además de los antivirus, existen otros programas que contribuyen a la desinfección y limpieza de nuestros equipos como, por ejemplo:

Anteriormente conocido como ¨**TuneUp Utilities**¨, es un paquete de aplicaciones para optimizar, personalizar y corregir fallos del sistema. Entre otros propósitos, permite desfragmentar el disco duro, eliminar archivos temporales, realizar ajustes automáticos para incrementar la velocidad de navegación en Internet y desfragmentar y corregir errores del registro de Windows.

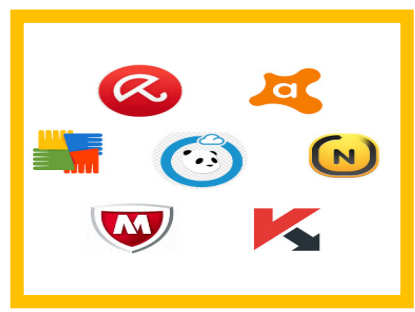
Anteriormente ¨**Crap Cleaner**¨, es una herramienta de software utilizada para limpiar archivos potencialmente no deseados y entradas invalidas del registro de Windows de un computador. Es una de las aplicaciones de limpieza más antiguas existentes, siendo lanzada originalmente en 2003.

Proporciona el acceso a una red privada virtual (VPN) que añade una capa de seguridad adicional al tráfico que se envía y recibe en la red.

1.6 Herramientas de desinfección gratuitas

A continuación, presentamos una lista de herramientas de desinfección con licencia gratuita:

- **Avast Free Antivirus.**
- **Avira Free Security.**
- **McAfee.**
- **Norton.**
- **AVG.**
- **Panda Free Antivirus.**
- **Kaspersky.**



1.7 Técnico. Ejemplo de infección por virus

En este punto, tomaremos como ejemplo un equipo infectado por un virus **Spyware**, mostrando cuales son los síntomas más comunes y cómo eliminarlo.

1. **¿Cómo sé si tengo un software espía?**

   Los programas espía infectan nuestro ordenador, instalándose en el disco duro y consumiendo el rendimiento de nuestra memoria RAM y nuestro procesador. Sin embargo, a diferencia de un virus, no se propagan en todos los ordenadores de una red, de modo que actúa como un parásito.

   Para averiguar si tenemos un software espía, podemos notar los síntomas a través de una reducción considerable de la velocidad de la red al navegar por Internet, o bien bloqueos repentinos del sistema operativo.

   También podemos conocerlo porque Windows Defender o nuestro antivirus nos manda un mensaje de alerta, o también utilizando algún tipo de software *anti-spyware*, aunque conviene siempre que conozcamos el programa, ya que existen algunos programas *anti-spyware* que dan falsos positivos y podríamos calificar como *fakes*.

2. **¿Qué hago para eliminar el spyware?**

   Hay varias formas de eliminar un software espía que hay en nuestro ordenador. Windows, en su página oficial, nos recomienda que utilicemos una herramienta anti-spyware para proceder a la búsqueda y eliminación del programa espía.

   Otra de las opciones es intentar eliminar el programa espía manualmente. Se trataría de entrar en nuestro panel de control y averiguar si alguno de los programas que vemos instalado es un software no deseado y que no recordamos haber instalado, ni que viniera con Windows al inicio.