15 consejos para mantener tu PC libre de virus

Instituto Superior Leonardo Da Vinci

Dirección de TI | Soporte Técnico

15 CONSEJOS PARA MANTENER TU PC LIBRE DE VIRUS

1

Utiliza un buen antivirus y actualízalo frecuentemente

La mejor manera de estar protegido contra los virus es instalar un buen antivirus en tu ordenador.

Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Porque los conoce, sabe cómo actúan y también sabe cómo eliminarlos.

Sin embargo, cada día aparecen más de 20 nuevos virus que los antivirus no son capaces de reconocer. Para la detección y eliminación de estos virus es necesario actualizar frecuentemente nuestro antivirus.

Por lo tanto, la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización, preferentemente diaria.

Comprueba que tu antivirus incluye soporte técnico, resolución urgente de nuevos virus y servicio de alerta

Si bien un antivirus perfectamente actualizado es la mejor arma para luchar contra los virus, es aconsejable contar con servicios adicionales.

El servicio de soporte técnico, bien a través de correo electrónico o por teléfono, es de gran ayuda ante cualquier problema o duda que pueda surgir relacionado con virus o con el funcionamiento del antivirus.

En el supuesto de verse afectado por algún virus de reciente creación, se debe contar con un servicio de resolución urgente de nuevos virus capaz de eliminarlos en el menor tiempo posible.

Otro servicio fundamental son las alertas sobre nuevos virus peligrosos, por ejemplo, a través de listas de correo.

Asegúrate de que tu antivirus esté siempre activo.

Un antivirus está activo cuando dispone de una protección permanente capaz de vigilar constantemente todas las operaciones realizadas en el ordenador.

Existen dos maneras para comprobar que esta protección permanente está activa; a través de un icono fijo en la barra de tareas, junto a la información horaria, o en la propia configuración del programa antivirus.

Estar protegido contra los virus requiere una protección permanente, tanto de archivos como de correo electrónico.

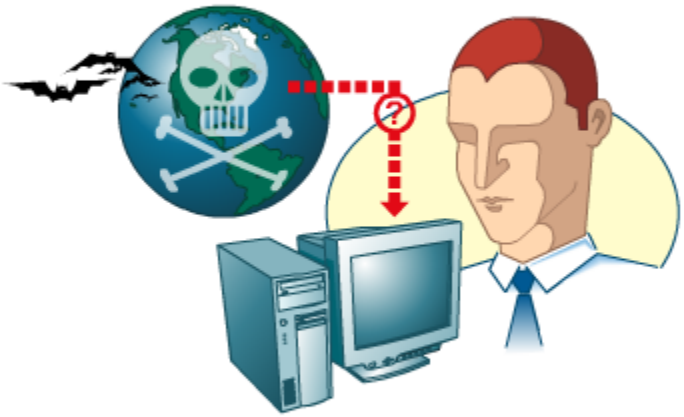
Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido.

El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.

Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip"). Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado; en algunos sistemas basta únicamente con abrir el mensaje, o visualizarlo mediante la 'vista previa'.

Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente al utilizado normalmente por el remitente.

Evita la descarga de programas de lugares no seguros en Internet.



Muchas páginas de Internet permiten la descarga de programas y archivos a los ordenadores de los internautas. Cabe la posibilidad de que estos archivos estén infectados con virus.

Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de programas desde sitios web que no nos ofrezcan garantías. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.

Rechaza archivos que no hayas solicitado cuando estés en chats o grupos de noticias (news).

Gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los grupos de noticias y los chats, respectivamente.

Los grupos de noticias o "news", como no son listas de correo y usan su propio sistema de transmisión por Internet (NNTP), también necesitan de una protección eficaz y constante.

Ambos sistemas, además de permitir la comunicación con otras personas, también facilitan la transferencia de archivos. Aquí es donde hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.

Actualiza el software que tienes instalado con los parches aconsejados por el fabricante de ese programa.

Con el objetivo de propagarse al mayor número de equipos posible, los virus aprovechan vulnerabilidades o problemas de seguridad existentes en los programas más utilizados por los usuarios (correo electrónico, navegadores de Internet, sistemas operativos, etc.).
Por tal motivo, es aconsejable estar informado e instalar las actualizaciones que, periódicamente, ofrecen los fabricantes de software para corregir los problemas descubiertos en los programas. De esta manera, contaremos con aplicaciones que no podrán ser utilizadas por los virus para difundirse, al tiempo que optimizaremos su rendimiento.

Retira los disquetes al apagar o reiniciar tu ordenador.

A pesar de que Internet es uno de los medios de propagación de virus más habituales, cabe resaltar que los disquetes siguen siendo una vía de infección de gran magnitud.

Además de analizar con un antivirus todos los disquetes utilizados, una forma de evitar que se activen los ya clásicos virus de boot o de arranque consiste en retirar los disquetes de las disqueteras al apagar o reiniciar el ordenador.

Por si se nos olvida hacerlo, es conveniente contar con un antivirus capaz de comprobar en tales circunstancias la existencia de disquetes infectados.

Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido.

Los archivos comprimidos, muy útiles por contener en su interior múltiples archivos y ocupar menos espacio, son un caldo de cultivo para los virus.

En primer lugar, hay que demandar a nuestro antivirus que detecte el mayor número de formatos comprimidos posible.

Antes de abrir directamente uno de estos archivos, como los de formato ZIP, es aconsejable guardarlos en carpetas temporales -creadas por los usuarios y cuyos ficheros pueden ser posteriormente borrados- en lugar de abrirlos sobre directorios de trabajo, por ejemplo, la carpeta Windows, Mis Documentos, el Escritorio, etc.

10

Mantente alerta ante acciones sospechosas de posibles virus.

Mediante el simple uso del ordenador, hay numerosos síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los archivos, avisos de macros en documentos Word o Excel que en principio no deberían contenerlas, recepción por parte de otras personas de mensajes nuestros de correo que no hemos enviado…

Como solución más completa a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de nuestra compañía antivirus.

11

Añade las opciones de seguridad de las aplicaciones que usas normalmente a tu política de protección antivirus.

Los programas informáticos más utilizados se convierten, precisamente por esa razón, en blanco de los autores de virus. Sus fabricantes suelen incluir en ellos opciones de seguridad contra virus.

Tal es el caso de los navegadores de Internet, procesadores de texto, programas de correo, etc., que disponen de características para asegurar un poco más la información.
Si no estamos familiarizados con ellas, podemos acudir a la ayuda del propio programa y realizar una búsqueda del término 'seguridad' para saber cómo utilizarlas.

Es conveniente aprovechar estas opciones específicas de seguridad, además de contar con un antivirus constantemente actualizado.

12

Realiza periódicamente copias de seguridad.

Una muy buena forma de minimizar el impacto de un virus, tanto a nivel corporativo como particular, es restaurar las copias de seguridad de nuestra información.

Realizar copias periódicas y frecuentes de nuestra información más importante es una magnífica política de seguridad. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

13

Mantente informado.

Una buena manera de protegerse contra los nuevos virus es estar continuamente informado sobre lo que acontece en el sector de la Seguridad Informática.

Sin embargo, ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos: compañías antivirus, empresas consultoras de seguridad, organismos que informan de alertas tempranas, organismos gubernamentales, universidades, etc.

14

Utiliza siempre software legal.

A la hora de instalar nuevos programas en el ordenador, el riesgo de infección es menor si se trata de software legal.

Sin embargo, si el software nos ha llegado en CDs piratas, o se trata de software legal manipulado posteriormente para "saltarse" la protección de los propios fabricantes, nadie nos puede asegurar que esté libre de virus.

Además, si se trata de software antivirus, su legalidad nos permite disfrutar de todos los servicios adicionales que garantizan su eficacia y seguridad.

15

Exige a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus.

En la lucha contra los virus se precisa la participación de todos los agentes implicados en el sector informático: empresas, usuarios finales, compañías antivirus, medios de comunicación, etc.

Como Internet es el medio más utilizado por los virus para su propagación, la colaboración de los proveedores de acceso a Internet es muy importante.

Así mismo, es aconsejable que los fabricantes de software y las publicaciones que ofrecen CD-ROMs adopten medidas para no difundir virus.

La contribución de todos ellos ayudará a minimizar el problema de las infecciones provocadas por virus.