

Los mejores antivirus de rescate contra el malware en PCs

Los antivirus de rescate tienen ventajas notables a la hora de descubrir esos virus, troyanos, gusanos y especímenes maliciosos de todo tipo campan a sus anchas por Internet y terminan colándose en las computadoras. Los creadores de malware van por delante con desarrollos cada vez más sofisticados y ciberataques avanzados que aprovechan el despiste o la desidia de los usuarios y las vulnerabilidades de software no parcheadas a tiempo. **Es hora de pasar a la acción.**

Los sucesivos listados de [peores incidentes en ciberseguridad](#) confirman que nos queda mucho por hacer. Y es difícil mantenerse a salvo por sí mismo. Puedes pensar que no te va a tocar, hasta que te toca por muy prudente que seas y hay que serlo, indudablemente. En el mundo actual, 100% conectado y con decenas de dispositivos en uso en cada hogar, las soluciones de seguridad informática son una buena herramienta en la que apoyarse.

Contar al menos con una solución básica es altamente recomendable, especialmente en sistemas operativos Windows, los más usados y atacados y a los que nos vamos a enfocar especialmente en una semana donde se ha celebrado el [Día Europeo de la Protección de datos 2026](#) un mayor conocimiento sobre los derechos y responsabilidades en esta materia y en general **concienciar de la necesidad de mantener un grado de seguridad personal y empresarial efectiva** en este complicado mundo virtual.

Antivirus de rescate, ¿por qué son tan útiles?

Entre el gran grupo de soluciones de seguridad destacan los llamados de 'rescate', los que desde una unidad externa se inician antes de que arranque el sistema operativo y por ello tienen **ventajas notables** sobre los típicos antivirus instalados.

Conviene recordar aquí que hay especímenes maliciosos que se cargan en la memoria **antes del arranque del sistema** y antes del inicio del antivirus instalado, por lo que éste no es capaz de detectarlo o eliminarlo. Otra ventaja es que los antivirus de este grupo no necesitan instalarse en el equipo ni estar

ejecutándose permanentemente con lo que se reduce el consumo de recursos de los instalados y no se penaliza el rendimiento.

Si detectas un funcionamiento anómalo de algún componente de tu PC; tienes errores aleatorios; te faltan archivos; te han cambiado las contraseñas: las aplicaciones por defecto han cambiado y, en general, si notas cosas 'raras', es hora de comprobar tu ordenador personal.

Creación y manejo

Los antivirus de rescate **se crean en unidades externas en formatos «Live»** que tienen capacidad de autoarranque y funcionamiento independiente al sistema operativo. Se pueden usar medios ópticos o mejor pendrives más seguros y extendidos hoy. Prácticamente todos tienen como base alguna distribución GNU/Linux y los proveedores que veremos más abajo ofrecen la posibilidad de crearlos desde su página web o una imagen .ISO o .IMG descargable que se puede manejar con las aplicaciones especializadas tipo Rufus, UNetbootin o similar.



Una vez creado, su uso es similar al de otras herramientas de rescate. Simplemente reinicias tu máquina con el medio insertado en su localización para arrancar desde el mismo y si no lo has hecho anteriormente, situándolo como primer dispositivo de arranque, antes de la unidad de almacenamiento de tu PC.

Una vez iniciado verás interfaces distintas, alguna en modo texto y otras visuales con bastantes funciones, aunque todas tienen (casi) lo que podemos encontrar en los antivirus instalados incluyendo las necesarias actualizaciones de la base de datos de virus, escaneo y desinfección del sector de arranque y de los archivos y carpetas de discos internos o externos. Tiene acceso directo al disco y al sistema de archivos y son capaces de eliminar las amenazas persistentes a las que a veces no llegan los instalados.

Selección de antivirus de rescate gratuitos

Todos los grandes especialistas en seguridad informática ofrecen algún tipo de solución gratuita de este tipo. Lamentablemente, no todos se mantienen actualizados en términos de interfaces y funciones, aunque para esta tareas tampoco es vital y es más importante la actualización de las definiciones de los últimos virus detectados y **su capacidad de escaneo y desinfección.**

Como decíamos arriba, algunos proveedores ofrecen la posibilidad de crear el medio directamente desde su página web, con propio tutorial de creación que es muy similar para todos ellos, o una imagen ISO o IMG que se puede usar para crear el medio. Te dejamos con algunos de los disponibles gratuitos.

[ESET SysRescue Live](#)

De los mejor mantenidos y actualizados con soporte para todos los Windows, cliente y servidor. Se puede usar desde un CD, DVD o USB, y como el resto de manera independiente del sistema operativo. Cuenta con varios modos de funcionamiento, «Exploración bajo demanda», «Exploración inteligente» o «Exploración personalizada».



[AVG Rescue CD](#)

Ofrece dos imágenes distintas para creación en CD o USB. Su interfaz es bastante espartana basada en texto pero que no te asustes, cumple su función, y como el resto, actualiza previamente la base de virus a las últimas disponibles.

[Kaspersky Rescue Disk](#)

Kaspersky hace tiempo que no actualiza la interfaz pero su disco de rescate basada en Gentoo tiene la gran potencia del líder de soluciones de seguridad en consumo. Descargas la imagen ISO, la grabas en un medio de arranque y la utilizas.



[Norton Bootable Recovery Tool](#)

Ofrece la creación del disco de arranque con un asistente que facilita su creación sin aplicaciones externas una vez que hayas descargado la herramienta. Una vez arrancado con él, verás una interfaz gráfica pero minimalista sin opciones de personalización, con dos opciones principales: escanear y limpiar.

[Panda SafeDisk](#)

Otra desactualizada en interfaz, pero muy sencilla de utilizar porque no tiene demasiadas opciones de personalización. Carga un asistente que busca automáticamente las definiciones de antivirus disponibles y, cuando se pulsa start, comienza a analizar todo el sistema en la búsqueda de archivos maliciosos.



[Trend Micro Rescue Disk](#)

Creación muy sencilla del medio de rescate a golpe de clic desde su página web y con la opción de elegir CD/DVD o disco/pendrive USB. Su interfaz es la más espartana de todo el listado, en un modo texto minimalista con unas cuantas opciones básicas.

[Avira Rescue System](#)

Ofrece la descarga de una imagen para creación del medio. Interfaz gráfica con pocas funciones pero sencilla de utilizar. Como otras que hemos visto de interfaz simple, su potencia está en el motor de búsqueda y desinfección y su capacidad de actualización de la base de virus, algo que todas hacen.

[Bitdefender Rescue CD](#)

Personalmente es de las que más me gustan. O me gustaban porque fue desactualizada a cambio de ofrecer un Modo de Rescate Bitdefender. Utiliza un Linux basado en Xubuntu que permite mayores posibilidades además de eliminación de virus. Descargas la ISO desde el enlace y quemas en el medio. Te dejamos enlace de web.archive donde todavía está disponible. Como el resto, aunque la versión no se esté actualizada, sí descarga las últimas definiciones y cumple su función.



[F-Secure Rescue CD](#)

Un super clásico que nos ha librado de virus más de una vez... Hace mucho tiempo que no se actualiza, pero es otro de los que se pueden utilizar. Con una base Knoppix, no hay ninguna interfaz de usuario real a excepción de un diálogo basado en texto, donde se te preguntará si deseas iniciar el análisis.

[Avast](#)

No ofrece descarga directa de una imagen y la única manera es crear el disco de rescate desde una solución de Avast ya instalada. Lo bueno es que se puede hacer desde la versión de escritorio gratuita. Creas el medio y después si quieres la eliminas.



Ten alguno de estos a mano porque a veces son **imprescindibles para acabar con malware persistente** que una vez cargado en la

memoria e iniciado el sistema operativo es difícil de erradicar e incluso de detectar. Además, este tipo de soluciones no penalizan el rendimiento al funcionar de manera independiente al sistema operativo del PC. Muy útiles para ejecutarlos de vez en cuando y comprobar el estado del equipo y eliminar las amenazas de seguridad que nos acechan.

* Imagen de portada generada por IA

Con información de Muy Computer