

# Introducción a la Ciberseguridad

Módulo 4



# Software antivirus

## Software antivirus


Un antivirus es un software que posee la función de **detectar códigos maliciosos**. Aunque su nombre está relacionado con los virus informáticos, actualmente estos programas son soluciones antimalware que poseen protección contra gusanos, troyanos, rootkit, spyware y otros elementos dañinos; es decir, **todo tipo de códigos maliciosos**.

Además, un antivirus tiene como función **identificar una amenaza**. Esto se refiere a la capacidad de la aplicación no sólo de detectar un malware, sino también de **describir de qué amenaza se trata**, tanto por su tipo (virus, troyano, gusano, etc.) como su nombre (como *Michelangelo*, *Conficker*, *QHost*, *Nuwar*, etc.).

Finalmente, una vez detectada e identificada cierta amenaza, un antivirus debe **prevenir o eliminar la misma del sistema**.

En el primer caso se trata de un código malicioso que es detectado al momento de intentar infectar un sistema, por lo tanto el antivirus bloqueará su acceso y prevendrá la infección.

En el otro caso, cuando se descubre el malware en un sistema que ya está infectado, el antivirus debe eliminar (o desinfectar) la amenaza.



Sin embargo, tal como se describe en este sencillo proceso de funcionamiento de un antivirus, **el primer paso es la detección de un código malicioso**. Para este fin el antivirus analiza los archivos (puede ser en tiempo real o a petición del usuario) en búsqueda de malware. En su visión simplificada, el antivirus examina cada archivo respondiendo a la pregunta: *¿es un código malicioso?*

A continuación, analizaremos los dos métodos de detección más habituales con los que suelen contar todos los antivirus del mercado.

## Detección reactiva: base de firmas

Desde sus orígenes, los antivirus cuentan con un **método de detección basado en firmas** (también llamadas ***vacunas***). Este emplea una base de datos generada por el fabricante que permite determinar al software si un archivo es o no una amenaza.

El sistema es sencillo: se coteja cada archivo a analizar con la base de datos y, si existe coincidencia (es decir, existe en la base una firma que se corresponde con el archivo), se identifica el archivo como código malicioso.

El proceso de generación de firmas se compone de los siguientes pasos:

1. Aparece un **nuevo código malicioso**.
2. El laboratorio de **la empresa antivirus recibe una muestra de ese código**.
3. **Se crea la firma** para el nuevo código malicioso.
4. **El antivirus comienza a detectar el malware cuando actualiza su base de firmas**.

Recién, a partir del último paso, el sistema estará protegido contra esta amenaza. Aquí radica **la importancia de tener actualizado el antivirus**: si la firma ya ha sido creada por el fabricante, pero no ha sido descargada en el sistema del usuario, el mismo no estará protegido contra esa amenaza en particular.

Además de la necesidad de mantener actualizada la base de datos, **este método posee otras dos desventajas**:

- El programa no puede detectar malware que no se encuentre en la base de datos.
- Se debe contar con una firma por cada variante de un mismo malware.

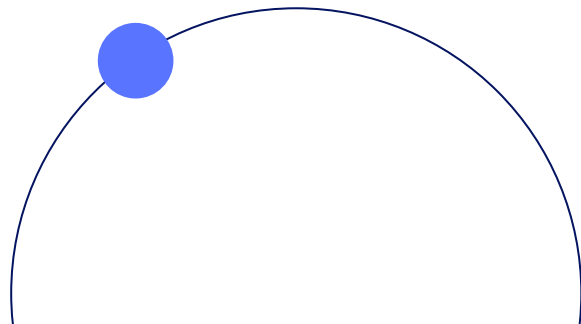
La demora necesaria para generar una firma es variable, y depende del tiempo que tarde el malware en ser descubierto por el laboratorio, de las características del código malicioso y de la dificultad para generar la firma. De una u otra forma, se puede considerar que la demora puede oscilar entre las 2 y las 10 horas; aunque existen casos y excepciones que se escapan de este rango en ambos límites.

En conclusión, **la detección por firmas es un método de protección reactivo: primero se debe conocer el malware para que luego sea detectado.**

Sin embargo, debido a la alta velocidad de propagación de nuevos códigos maliciosos, y la gran cantidad de nuevas variantes que aparecen día a día, **este método se volvió, con el pasar de los años, lento e insuficiente.**

De manera similar a lo que sucede durante las epidemias del campo biológico, en el caso del malware también existen probabilidades de que se produzca una infección antes de que aparezca la cura para dicha amenaza (la firma).

Un antivirus que utilice sólo métodos reactivos de detección estará protegiendo a sus usuarios sólo de aquellos códigos maliciosos que han sido incorporados a la base de datos, dejando siempre desprotegido al usuario frente a todas las variantes que sean desconocidas por el laboratorio del fabricante, o que aún no posean una firma.



## Detección proactiva: heurística

Para dar solución a esta problemática aparecen los **métodos de detección proactivos basados en heurística**, como complemento de la detección basada en firmas. Esto quiere decir que la detección proactiva es un agregado a la detección por firmas y **para una óptima protección son necesarios ambos métodos**, tal como trabajan las soluciones antimalware en la actualidad.

El objetivo esencial de los algoritmos heurísticos es dar respuestas en aquellas situaciones en donde los métodos reactivos no pueden darla: la capacidad de **detectar un archivo malicioso aunque una muestra de éste no haya llegado al laboratorio antivirus, y que aún no se posea la firma correspondiente**.



Por lo general, la programación heurística es considerada como una de las aplicaciones de la inteligencia artificial y como herramienta para la resolución de problemas. Tal como es utilizada en sistemas expertos, **la heurística se construye bajo reglas extraídas de la experiencia**, y las respuestas generadas por tal sistema mejoran en la medida en que “aprende” a través del uso y aumenta su base de conocimiento.

La heurística siempre es aplicada cuando no puedan satisfacerse demandas de completitud que permitan obtener una solución por métodos más específicos (por ejemplo, la creación de una firma para un malware determinado).

A manera de ejemplo, puede suponerse que un responsable de Recursos Humanos desea contratar un graduado de cierta carrera y se conecta con la universidad. La institución le ofrece un listado de 300 alumnos que se graduaron en los últimos años y él debe seleccionar a uno para su contratación. Su capacidad para realizar entrevistas es de 20 personas, por lo que debe tomar alguna decisión que le permita encontrar al candidato indicado. Una decisión heurística podría ser que se seleccione a los 20 alumnos con mejor promedio, lo cual probablemente le permita acercarse a los mejores candidatos.

## Funcionamiento

Los algoritmos heurísticos son la base de la mayor parte de métodos de detección de malware proactivos.

**El análisis heurístico posee un comportamiento basado en reglas para diagnosticar si un archivo es potencialmente ofensivo.** El motor analítico trabaja a través de su base de reglas, comparando el contenido del archivo con criterios que indican un posible malware, y se asigna cierto puntaje cuando se localiza una semejanza. Si el puntaje iguala o supera un umbral determinado, el archivo es señalado como amenaza y procesado de acuerdo con ello.

De igual modo que un analista de malware intentaría determinar, trabajando en el laboratorio, la peligrosidad de un determinado programa, analizando sus acciones y características (por ej.: modifica el registro, se carga al inicio de sesión, elimina archivos, etc.), el análisis heurístico realiza el mismo proceso de toma de decisiones inteligentes, actuando como un investigador virtual de malware.



Mientras que la identificación de una amenaza realizada por medio de una detección reactiva basada en firmas posee la previa legitimación de una persona del laboratorio, **la detección proactiva a través de métodos heurísticos no incluye la intervención humana**, y en la detección posee un suficiente grado de certeza al respecto como para afirmar que un archivo es una amenaza. A pesar de esta aparente “desventaja”, los algoritmos heurísticos ofrecen protección donde la exploración por firmas no puede darla.

Aunque la detección proactiva no depende de la actualización de la base de firmas, sí **debe mantenerse actualizado el programas antivirus, a fin de contar con los últimos algoritmos de detección heurística.**



## Tipos de heurística

*“Los algoritmos heurísticos, como su pluralidad lo indica, son distintas metodologías de análisis proactivo de amenazas”.*

Se definen a continuación las tres variantes más comunes en este tipo de análisis:

- **Heurística genérica:** se analiza cuán similar es un objeto a otro, que ya se conoce como malicioso. Si un archivo es suficientemente similar a un código malicioso previamente identificado, este será detectado como *“una variante de...”*.
- **Heurística pasiva:** *“se explora el archivo tratando de determinar qué es lo que el programa intentará hacer. Si se observan acciones sospechosas, éste se detecta como malicioso”.*
- **Heurística activa:** se trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código. Otros nombres para la misma técnica son *“sandbox”, “virtualización”* o *“emulación”*.

Asimismo, los algoritmos de detección proactiva de amenazas contienen instrucciones que le permiten sortear diversos mecanismos que poseen los códigos maliciosos para ocultar su comportamiento, especialmente el empaquetamiento y el cifrado.

Encuentra más información [aquí](#)



## Precauciones

Al estar basados los algoritmos heurísticos en inteligencia artificial, poseen dos relativas desventajas, que deben ser eliminadas para hacer su funcionamiento más eficiente.

En primer lugar, al utilizar algoritmos inteligentes complejos, la carga de trabajo que posee el antivirus puede ser mayor que cuando se emplea el método basado en firmas (una simple exploración en una base de datos).

Por lo tanto, **es importante que los algoritmos de detección proactiva basados en heurística estén optimizados, a fin de que el rendimiento de la solución sea el máximo posible.**

En tal caso, incluso pueden ser más rápidos que una exploración por firma a medida que la base de datos del método reactivo vaya creciendo.

El otro factor de riesgo para los algoritmos de detección proactiva está constituido por los **falsos positivos**: archivos que no son códigos maliciosos, y son detectados como tales.

Así como un antivirus trabaja para minimizar los falsos negativos (es decir, amenazas que no son detectadas), en el caso de la heurística es necesario minimizar también los falsos positivos.

El motivo de tal calificación incorrecta resulta comprensible: al trabajar estos algoritmos con grados de certeza, y análisis inteligente, puede ocurrir que se haga una detección errónea de un archivo. Con la base de firmas esto ocurre en un nivel muy bajo, porque sólo se detectan amenazas

conocidas que ya han sido catalogadas como tales por el laboratorio.

Es indispensable, entonces, que los algoritmos de detección proactiva posean optimización, para minimizar la tasa de falsos positivos, ya que estos son altamente perjudiciales para los usuarios.

Por lo tanto, los algoritmos heurísticos de los antivirus deben ser evaluados, no sólo por sus capacidades de detección, sino también por su rendimiento y la cantidad de falsos positivos detectados. **La mejor heurística es aquella que combina los niveles de detección con bajos (o nulos) falsos positivos.**

# VirusTotal

[VirusTotal](https://www.virustotal.com) es un servicio web que ofrece analizar archivos o URLs utilizando cerca de 45 motores de análisis diferentes ofrecidos por varios fabricantes de software antivirus.

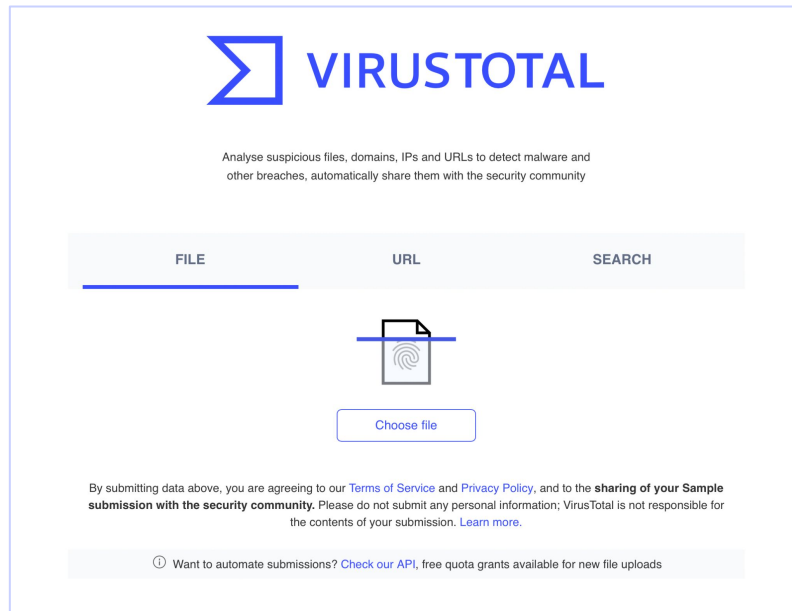




En la imagen podemos ver el formulario de la página principal de VirusTotal desde donde puedes analizar un archivo o una dirección URL.

El máximo tamaño de archivo que se puede analizar es de 64 MB.

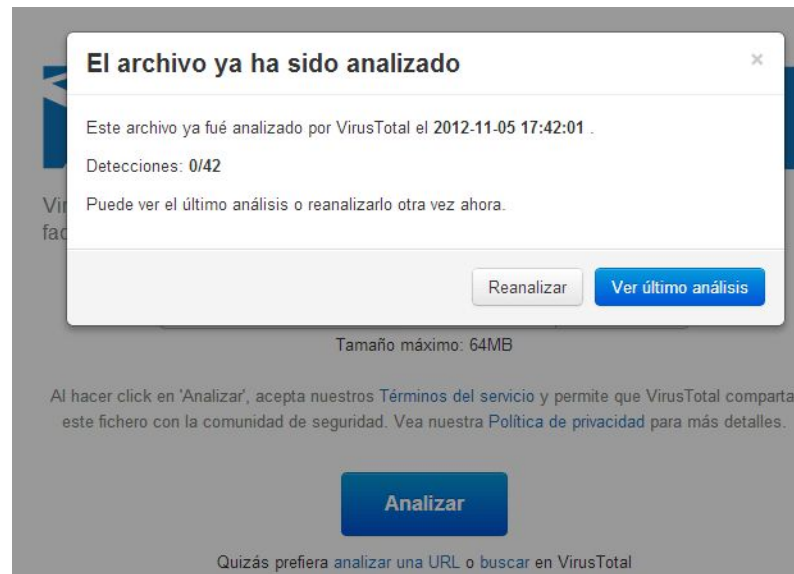
Si el archivo que vamos a analizar ya ha sido analizado anteriormente por otro usuario, tendremos acceso al informe guardado en VirusTotal sin tener que volver a subir el archivo, claro que también podemos volver a subir el archivo y volver a analizarlo.



The image shows the VirusTotal homepage. At the top, there is the VirusTotal logo and a tagline: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community". Below this, there are three tabs: "FILE", "URL", and "SEARCH". The "FILE" tab is selected. In the center, there is a large icon of a document with a fingerprint, representing a file upload. Below this icon is a button labeled "Choose file". At the bottom, there is a disclaimer: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#)." At the very bottom, there is a link: "Want to automate submissions? [Check our API](#), free quota grants available for new file uploads".

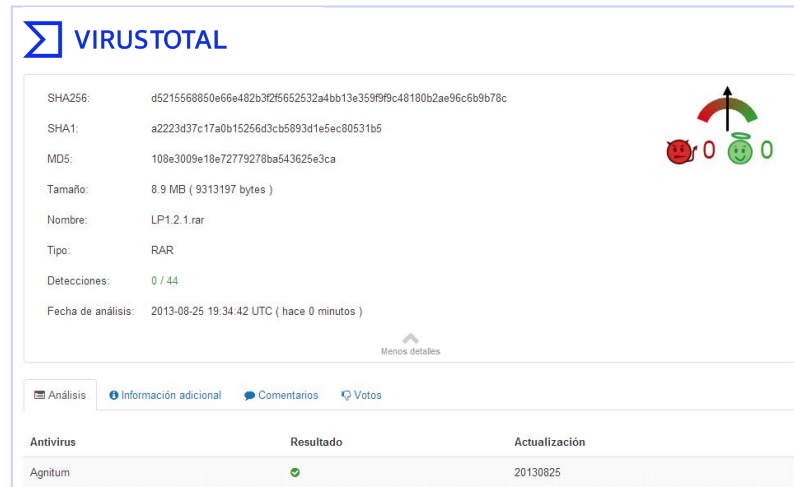
Después de subir el archivo el informe de VirusTotal es bastante completo, incluye el análisis de antivirus tan conocidos como *Avast*, *AVG*, *BitDefender*, *ClamAV*, *Comodo Antivirus*, *DrWeb*, *ESET NOD32*, *GData*, *Karspersky*, *McAfee*, *Microsoft Security Essentials*, *Panda*, *Malwarebytes*, *Norton* y muchos más, para luchar contra diferentes tipos de software: virus, spywares, troyanos, etc...

Es capaz de detectar cualquier código malicioso, incluso cuando los archivos se encuentran comprimidos (aunque no deben estar cifrados).



Para identificar los archivos, VirusTotal se guía por los hash MD5, SHA1, SHA256 y ssdeep de forma que cada archivo es único aunque su nombre sea el mismo o diferente.

VirusTotal también detecta lenguajes de programación, compiladores, compresores y otros tipos de código.



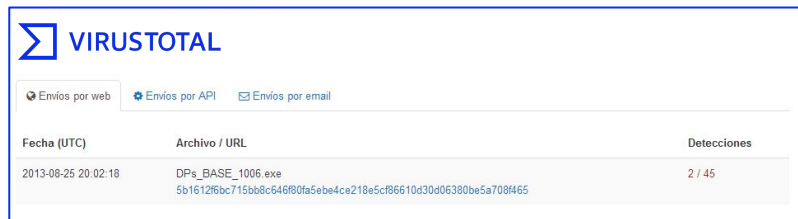
The screenshot shows the VirusTotal interface for a file analysis. The file name is LP1.2.1.rar, which is a RAR archive of size 8.9 MB. It has been analyzed on 2013-08-25 at 19:34:42 UTC. The analysis shows 0 detections out of 44 engines. The interface includes tabs for 'Análisis', 'Información adicional', 'Comentarios', and 'Votos'. Below the analysis details is a table showing the results from various antivirus engines.

Antivirus	Resultado	Actualización
Agnitum	✓	20130825

Los usuarios pueden comentar en los informes de análisis de los archivos e incluso votar positivo o negativo en los análisis de malware, aunque para eso debemos estar autenticados con una cuenta VirusTotal.

**La principal ventaja de tener una cuenta en VirusTotal es que se guardaran en ella todos los análisis realizados y podremos acceder a los informes posteriormente.**

Análisis	
Información adicional	
Comentarios	
Votos	
File identification	
MD5	108e3009e18e72779278ba543625e3ca
SHA1	a2223d37c17a0b15256d3cb5893d1e5ec80531b5
SHA256	d5215568850e66e482b3f2f5652532a4bb13e359f9f9c48180b2ae96c6b9b78c
ssdeep	196608:Hc74VIU2VIGXhBBx4l11+J5hB4nJPkdAWzazTz:8UAvRZo1yZgJMdAVTz
File size	8.9 MB ( 9313197 bytes )
File type	RAR
Magic literal	RAR archive data, v14, os: Win32
TrID	RAR Archive (83.3%) REALbasic Project (16.6%)



The screenshot shows the VirusTotal website interface. At the top, there is a navigation bar with the VirusTotal logo and three tabs: 'Envíos por web', 'Envíos por API', and 'Envíos por email'. Below the navigation bar, there is a table with three columns: 'Fecha (UTC)', 'Archivo / URL', and 'Detecciones'. The table contains one row of data.

Fecha (UTC)	Archivo / URL	Detecciones
2013-08-25 20:02:18	DPs_BASE_1006.exe 5b1612f6bc715bb8c646f0fa5ebe4ca218e5cf86610d30d06380be5a708f465	2 / 45

En cuanto al análisis de direcciones URL y sitios web, **VirusTotal utiliza cerca de 32 motores de análisis antimalware** para detectar cualquier tipo de malware en el código del sitio web. Algunos de los más conocidos y utilizados son los de *Google*, *NetCraft*, *Opera*, *Kaspersky*.

- Podemos confirmar la seguridad que ofrece VirusTotal a sus usuarios revisando sus estadísticas en la siguiente dirección URL: <https://www.virustotal.com/es/statistics/>
- Si queremos obtener más información acerca de VirusTotal o utilizar el servicio puedes acceder a la siguiente dirección URL: <https://www.virustotal.com/es/>
- VirusTotal dispone de una API que puedes integrar en tus propios programas para analizar los archivos. Si quieres acceder a ella podemos hacerlo a través de la siguiente URL: <https://www.virustotal.com/es/documentation/>

## Desinfección

**El primer paso siempre es desconectar el sistema de internet.** De este modo romperemos la conexión que el atacante pudiera tener con nosotros, lo cual disminuye los riesgos. Seguido a esto, nos ponemos a desinfectar el equipo.

Matar el proceso del malware no es suficiente. Si sólo hacemos eso, es muy probable que al reiniciar el equipo se vuelva a ejecutar el código malicioso y seguiremos infectados.

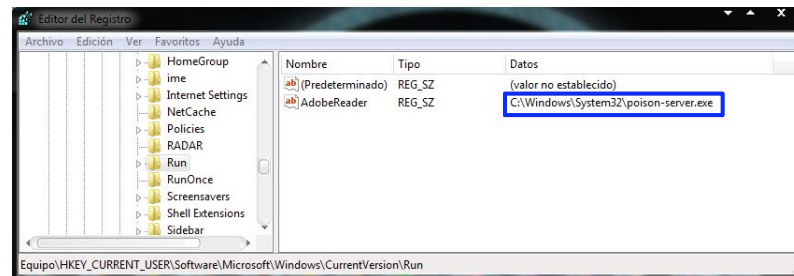
La desinfección es todo un proceso, que podemos llevar a cabo manualmente o con la ayuda de herramientas especializadas.



## Desinfección manual

Al realizar las técnicas de detección, obtuvimos información sobre el malware que se aloja en el sistema (por ejemplo el proceso que utiliza o vimos el nombre del ejecutable en las conexiones y el registro). Utilizaremos estos datos para **encontrar la ubicación exacta del malware en nuestro equipo**; por lo general se copian a la carpeta **System32, Windows, Users, AppData o Temp**. Una vez localizado, si hemos matado su proceso, **podremos eliminar el ejecutable sin problemas**.

También tenemos que **eliminar la entrada del malware en el registro**, algo que podemos hacer desde el mismo **Regedit**: click derecho del mouse sobre la entrada **Eliminar**.



**La entrada del malware en el registro delata su ubicación.**

*“Una vez hecho esto **reiniciamos el equipo** y, cuando arranque nuevamente, **volvemos a revisar los procesos, las conexiones y las entradas en el registro** para asegurarnos de que el malware definitivamente quedó erradicado de nuestro sistema”.*

En el caso de que vuelva a aparecer el proceso del malware, tendremos que analizar su ejecutable con herramientas más complejas que nos ayudarán a determinar qué componentes le permiten seguir ejecutándose en nuestro sistema.

Este análisis más profundo lo dejaremos para el próximo módulo, donde haremos uso de la suite **SysInternals**.



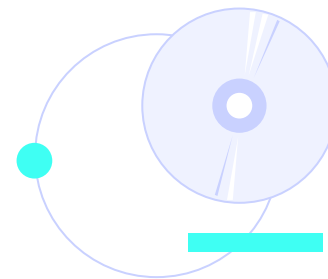


## Desinfección automatizada

Podemos utilizar, además del antivirus estándar que deberíamos tener instalado en cada uno de los dispositivos, **un CD de arranque para realizar un análisis “externo” del malware.** Estos CD de arranque tienen la ventaja de correr sobre un sistema operativo totalmente diferente del original (generalmente utilizan GNU/Linux).

Varios de los fabricantes antimalware reconocidos brindan este tipo de CD de forma totalmente gratuita. Algunos de ellos son:

- Kaspersky.
- ESET (Nod32).
- Avast.
- F-Secure.



**¡Sigamos  
trabajando!**