Antivirus

Que es un Antivirus?

- Constituyen una herramienta básica de la seguridad informática, que garantiza en principios la protección final de una estación de trabajo contra la infección por programas malignos.

Surgimiento

- Surgen de la necesidad de mantener los sistemas operativos en optimas condiciones, como vigilante seguro.
- Ningun antivirus es 100% seguro, ya que a medida que avanza la tecnología se perfeccionan los programas malignos
- Los antivirus se han convertido en compañeros inseparables del trabajo diario. Hoy en día no se concibe ningún equipo conectado a Internet que carezca de una buena protección contra programas malignos

Clasificacion de los Antivirus

Antivirus Preventores

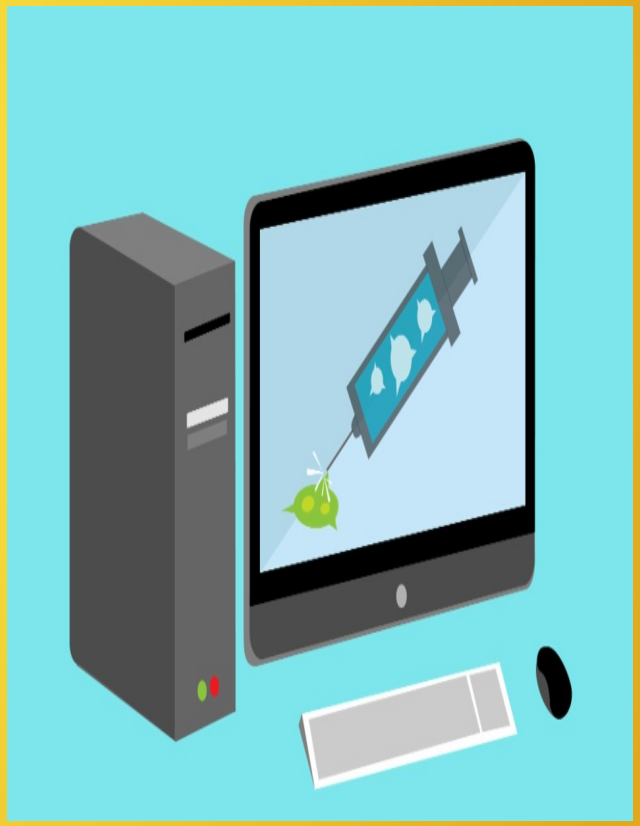
Los programas que previenen la infección, quedan residentes en la memoria de la computadora todo el tiempo y monitorean algunas funciones del sistema

Antivirus Identificadores

Estos productos antivirus identifican programas malignos específicos que infectan al sistema. Los mismos trabajan con las características de un programas malignos o sus variantes, o exploran el sistema buscando cadenas (secuencias de bytes) de códigos particulares o patrones característicos de los mismos para identificarlos

Antivirus Descontaminadores

Sus características son similares a los productos identificadores, con la diferencia que su principal función es descontaminar a un sistema que ha sido infectado, eliminando
el programas malignos y retomando el sistema a su estado original por lo que tiene que ser muy
preciso en la identificación de los programas malignos contra los que descontaminan.



Funcionamiento Antivirus

Capacidad de detectar programas malignos que no están en su base de datos, a través del sondeo del sistema en busca de síntomas clásicos de infección.

Principales Antivirus

- Dentro de las principales antivirus, se encuentran:
  - Symantec
  - Panda
  - McAfee
  - Kaspersky
  - Avast
  - Nod_32
  - Avg

Que significa Heuristica

Es el arte para resolver Problemas.

Symantec

- **Symantec Corporation** es una corporación internacional que desarrolla software para computadoras.
- Symantec es también un líder de industria en la seguridad electrónica completa de mensajería, ofreciendo las soluciones para antispam y antivirus.
- La organización Symantec Security Response es uno de los principales antivirus y grupos de investigación en la industria.
- **Productos:**
  - Norton AntiVirusNorton AntiVirus
  - Norton Internet Security
  - Norton 360
  - Norton 360 MultiDevice

Panda

Centrada inicialmente en la producción de software antivirus.
Ademas incluye los siguientes software:

- Cortafuegos
- Deteccion de Spam y Spyware.
- Prevencion CyberCrimen
- Tipo de Malware.
- Deteccion de intrusos en redes Wifi.
- Sus herramientas son patentadas por TruePrevent.
- En 2009 lanzo Panda Cloud Antivirus.
- Permite analisis automatico de las amenazas, lo que le permite ser mas rapido y eficiente.

McAfee

- Es una compañía de software relacionada con la seguridad informática.
- Su producto más conocido es el antivirus McAfee VirusScan
- La empresa fue fundada en 1987 con el nombre de McAfee Associates.
- McAfee compro Trusted Information Systems.
- Trusted Information Systems se encargó del desarrollo del Firewall Toolkit.
- 2010 Intel compro McAfee por 7.680 millones de dólares.

Kaspersky

- Es un grupo internacional activo en, aproximadamente, 200 países del mundo. Su sede central se encuentra en Moscú, Rusia.
- El grupo engloba 31 oficinas ubicadas en treinta países diferentes.
- Kaspersky Lab es la empresa privada más grande del mundo y uno de los proveedores de protección TI con mayor crecimiento.
- La línea actual de productos Kaspersky ofrece los siguientes productos:
  - Kaspersky Pure
  - Kaspersky Internet Security
  - Kaspersky AntiVirus
  - Kaspersky Mobile Security
  - Kaspersky AntiVirus para Mac
  - Kaspersky Password Manager y Kaspersky Small Office.

Avast

- Es un *software* antivirus y suite de seguridad de la firma checa AVAST Software.
- Desarrollada a principios de la década de 1990.
- Su cuota del mercado de 21,4% es el software antivirus gratuito más utilizado en el mundo.
- Avast incluyó su propio sistema de recomendación de compras en línea, SafePrice, el cual se activaba automáticamente por defecto, añadido en su extensión Online Security.
- Existen varias versiones:
  - **avast! Free.**
  - **avast! Pro.**
  - **Motor de heurística**
  - **avast! Internet Security.**

Nod 32

- Es un programa antivirus desarrollado por la empresa ESET.
- Es de origen eslovaco.
- El producto está disponible para Windows, Linux, FreeBSD,
- Solaris, Novell y Mac OS X.
- Tiene versiones para estaciones de trabajo, dispositivos móviles, servidores de archivos, servidores de correo electrónico, servidores gateway.
- También cuenta con un producto integrado llamado ESET Smart Security que además de todas las características de ESET NOD32, incluye un cortafuegos y un antispam.
- La primera versión de ESET NOD32 se publicó a principios de los años 90.

Motor

Utiliza un motor unificado llamado *ThreatSense* que permite la detección en tiempo real de nuevas amenazas o virus nuevos aún no catalogados, analizando el código de ejecución en busca de las intenciones malignas de alguna aplicación de malware.

Módulos

En las versiones previas a la 3.0, ESET NOD32 Antivirus contaba con un modelo modularizado, con
componentes tales como:

- **AMON** (**A**ntivirus **Mon**itor)
- DMON (**D**ocument **Mon**itor)
- EMON (**E**mail
- **Mon**itor)
- IMON (**I**nternet **Mon**itor), etc.

Avg

Es un software antivirus desarrollado por la empresa checa AVG Technologies.
Disponible para sistemas operativos Windows, Linux, Android, iOS, Windows Phone, entre otros.
Technologies es una empresa privada checa formada en enero de 1991.
2006, el software AVG también ha sido
usado como un componente opcional de Seguridad de Correo.
AVG destaca la mayor parte de las funciones comunes disponibles en el antivirus moderno y programas de
seguridad de Internet, incluyendo escaneos periódicos, escaneos de correos electrónicos enviados y recibidos.
La capacidad de reparar algunos archivos infectados por virus, y una bóveda de virus donde los archivos infectados son guardados, un símil a una zona de cuarentena.

Para elegir un buen antivirus hay que tomar en cuenta lo siguiente:

- Actualizar firmas al menos una vez por semana.
- La empresa que lo promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta que no excedan de 48 horas, el cual pueda orientarlo en caso de que contenga una infección.
- Se debe contar con distintos métodos de verificación y análisis de posibles códigos maliciosos
- Se debe poder adaptar a las necesidades de diferentes usuarios.

- Debe permitir la creación de discos de emergencia o de rescate.
- No debe afectar el rendimiento o desempeño normal del equipo.
- El programa residente en memoria debe ser lo mas pequeño posible.
- El número de pasos positivos que se den, tanto en el rastreo normal com en el heurístico, debe ser el mínimo posible.
- Su mecanismo de auto protección debe poder alertar sobre una posible infección por medio de las distintas vías de entrada, Internet, e–mail, red, discos flexibles etc.
- Debe tener posibilidad de chequear el arranque y los posibles cambios en el registro de las aplicaciones.