**Práctica 2. Amenazas.**

1. **Propón medidas preventivas básicas de seguridad a adoptar ante:**

**Ataque de ingeniería social, donde empleados del departamento de informática han  
conseguido las claves del personal de contabilidad.**

Para prevenir este ataque considero que lo mejor sería dar una formación de lo importante que es mantener las claves, no facilitárselas a nadie, ya que si el informático necesita la contraseña de un empleado lo más probable es que la tenga él.

**Ataque de un virus que se ha colado por el correo de la oficina y se propaga por la red.**

Habría que instalar antivirus en los ordenadores para proteger los correos y demás archivos, ya que un buen antivirus evita que se descarguen correos desde el correo.

**Ataque de denegación de servicios, donde los routers de la red están siendo saturados  
por una denegación de servicios, donde la información ni entra ni sale.**

Existen firewalls que te protegen de ataques DDoS, que lo que hacen es al recibir x conexiones de una IP la bloquean. En algunos routeres es posible bloquear IP´s cuando hacen muchas conexiones/peticiones en poco tiempo.

**Ataque de un troyano que amenaza con hacerse con el control de un ordenador y  
sacar información confidencial de la empresa.**

Con un antivirus se podrían proteger los ordenadores. Incluso, para determinados virus, troyanos, etc. Existen formas de quitarlos manualmente aunque es algo más laborioso.

**Ataque de un hacker que intenta hacerse con información de la empresa.**

Habría que controlar los puertos, ver que están correctamente en el firewall, comprobar que no hay ninguna puerta trasera ni ningún programa intrusivo en nuestro sistema.

1. **Caso Ronnie**

Santiago Garrido, conocido como Ronnie, fue expulsado de una red de chat de IRC-Hispano por quejarse de que los adminsitradores avasallasen a la gente, debido a esto actúo en caliente e inicio el ataque DDoS.

Fue el mayor caso documentado de DDoS en España, se realizó afecto al 30% de la población española.

El hacker conocido como Ronnie creo un gusano y lo propago en las redes que tenían un gran ancho de banda, infectando a miles de ordenadores para sincronizarlos en ataques DDoS contra la infraestructura de IRC.

Lanzo ataques periódicos con sus servidores, usando miles de máquinas infectadas, las empresas infectadas más importantes fueron Wannado, Intelideas y Ono.

1. **Noticia de amenaza informática.**

Un incendio en Telvent provocó un apagón en la prensa digital. Se produjo una explosión en el sistema eléctrico en el edificio, se produjo uno de los dos sistemas de Backup. Tras la explosión el primer sistema quedo inutilizado y dejo fuera de servicio parte del cableado eléctrico del edificio. Esto produjo que el segundo sistema de Backuo no pudiera con todo y debido al daño de la red eléctrica apagaron el aire acondicionado del CPD y a continuación los ordenadores.

<http://www.elconfidencial.com/comunicacion/2008-09-23/un-incendio-en-telvent-abengoa-provoca-un-apagon-en-la-prensa-digital_432248/>

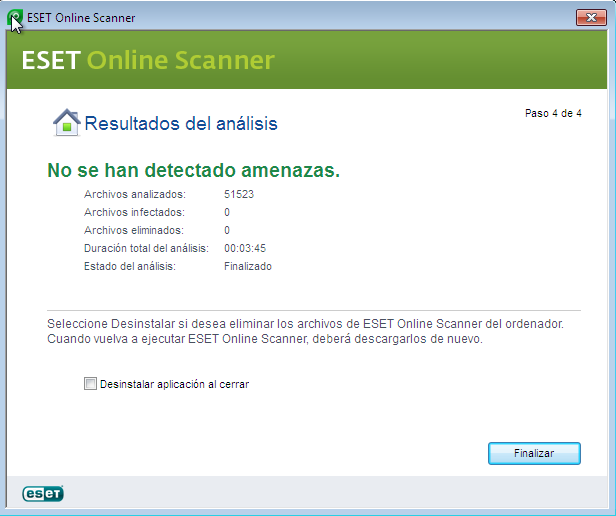
1. **Noticia de amenaza lógica.**

La NASA sufrió en 2011 un ataque por parte de hackers que les dio el control total sobre los ordenadores permitiéndoles el acceso a material confidencial, los atacantes actuaron desde China y tuvieron acceso a material que podría haber supuesto grandes pérdidas de dinero.

<http://www.clarin.com/internet/NASA-sufrio-ciberataque_0_659334164.html>

1. **Antivirus On-line.**

ESET Online Scanner



Ha analizado 51523 archivos, el pico más alto de Ram ha sido de 1GB, consumía el 50% de la CPU. Solo permite analizar el sistema, no implementa firewall ni nada más.

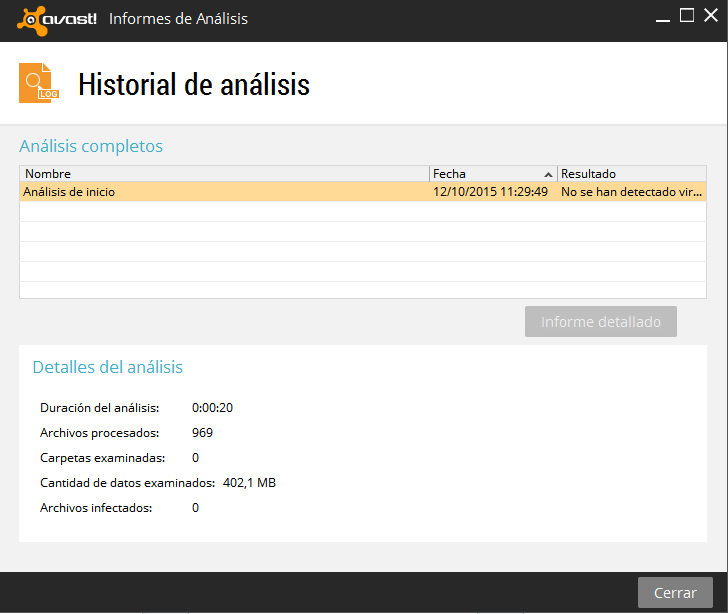
Bitdefender



Apenas consume RAM o CPU, no especifica cuantos archivos ha analizado.

1. **Antivirus local.**

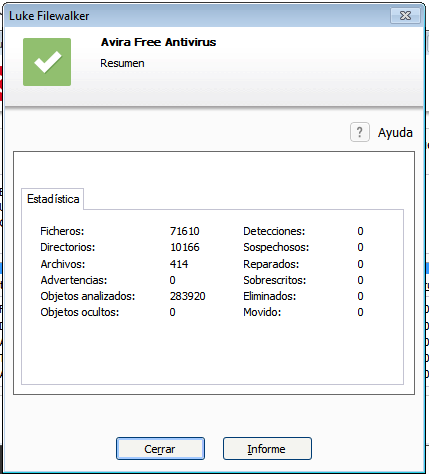
Avast



Las principales opciones del Avast son:

* Analizar en busca de virus: Busca posibles virus todo el disco duro o determinadas carpetas.
* Analizar en busca de complementos en el navegador: Localiza complementos tales como ‘Hola Search’, ‘Webget’, etc.
* Analizar en busca de software obsoleto: Nos informa de que programas tenemos desactualizados.
* Analizar en busca de amenazas en red: Comprueba que el router está bien configurado y los dispositivos no son visibles desde internet.
* Analizar en busca de problemas de rendimiento: Hace un escáner con Grime Fighter para ver si todos los programas funcionan correctamente y no consumen de más.

Avira

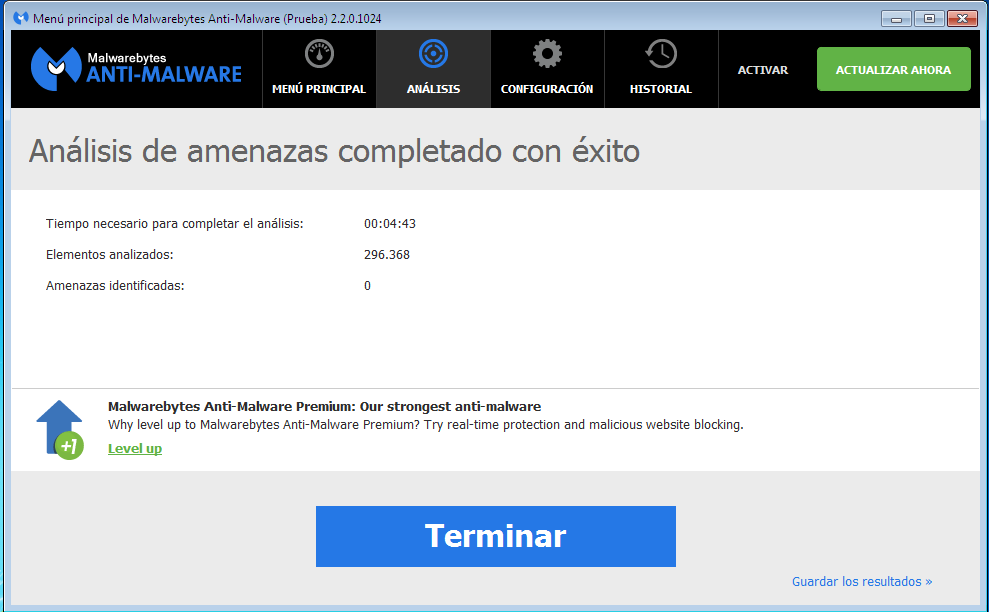


Las principales funciones de Avira son:

* Analizar el sistema: Analiza el sistema para localizar posibles virus, troyanos, etc.
* Firewall: Implementa un firewall para proteger los puertos.

1. **Antimalware.**

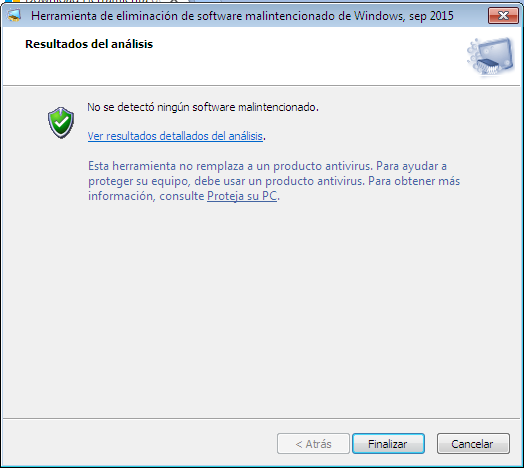
Malwarebytes



Funciones:

* Este antimalware solo permite analizar el sistema, no incluye ningún tipo de firewall.

Herramienta de software malintencionado de Windows



* Su única función es analizar el sistema en busca de malware, no trae más opciones.