4.2.- Configuración de antivirus (I).

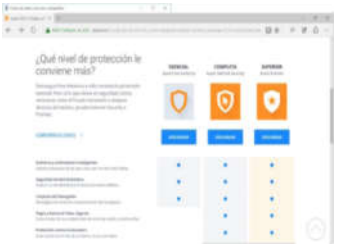
Como vimos en la anterior unidad los antivirus se encargan de detectar, bloquear y eliminar virus y otros programas malintencionados. Para ello monitorizan las aplicaciones que se ejecutan y la entrada y salida de archivos en el ordenador para evitar que alguno de ellos pueda llevar a cabo una acción malintencionada.

Actualmente, los antivirus consumen una cantidad moderada de recursos con lo que no afectan tanto al rendimiento del equipo. Además, nos permiten programar análisis periódicos según nuestras necesidades y pueden observar patrones de comportamiento potencialmente peligrosos en procesos, y detectar así nuevo software malintencionado no recogido en la lista de definiciones de virus. La base de datos de virus contiene todo el software malintencionado que es capaz de reconocer el antivirus. En ella el antivirus tiene el código de cada virus conocido, incluidas sus actualizaciones y cuando revisa los archivos lo que hace es comparar esos códigos. La base de datos de virus se actualiza periódicamente con nuevas amenazas detectadas. La predicción de amenazas no reconocidas se realiza mediante técnicas heurísticas.

En este apartado vamos a ver qué opciones tiene y cómo configurar un programa antivirus concreto. Hoy en día, contamos con una amplia oferta para elegir entre antivirus comerciales y gratuitos de gran calidad. En nuestro caso, tomamos como alternativa un antivirus gratuito, Avast! Free Antivirus, debido a su accesibilidad, amplio uso y eficacia. Seguiremos los siguientes pasos:

- **Descarga e instalación.**
- **Navegar por las opciones del menú.**
- **Protección con sandbox o caja de arena.**
- **Uso de la heurística.**
- **Mejorar el rendimiento.**
- **Planificar análisis periódicos.**

Descarga e instalación.



Para comenzar accedemos a la web de Avast para descargar el antivirus:

Sitio de descarga de Avast! Free Antivirus.

Haremos clic en el enlace correspondiente para descargar Avast! Free Antivirus. Avast! Además de su antivirus gratuito ofrece otros productos comerciales que incluyen opciones adicionales (protección contra el spam, cortafuegos, compras y banca online más seguras, etc.).

Terminada la descarga, haremos doble clic sobre el fichero de instalación, **setup_av_free.exe**, para iniciar la instalación. El proceso de instalación es sencillo y lo primero que realiza es un punto de restauración, para que en caso de algún problema, se pueda volver al estado anterior a la instalación del antivirus.

Es importante asegurarnos al iniciar la instalación de que no están activos otros antivirus en el sistema, pues esto puede hacer que el ordenador funcione bastante lento.

Navegar por las opciones del menú

Ya hemos finalizado la instalación y vamos a conocer la interfaz del programa. Ésta es bastante intuitiva y clara, está organizada por bloques situados a la izquierda de la pantalla principal. Estos bloques son:

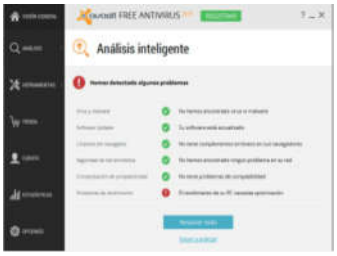
- Visión General.
- Análisis.
- Tienda.
- Cuenta.
- Estadísticas.
- Opciones.

En el bloque Visión General podemos ver el estado actual del equipo. Nos da ofrece varias opciones , el análisis inteligente que realiza una búsqueda rápida de virus y malwares, Software que necesitan actualizarse, Ajustes de la red domestica y en busca de "basura" que se puede acumular en el PC con el paso del tiempo.

Con el análisis rápido realizamos como su propio nombre indica un análisis rápido del ordenador, que puede no ser tan eficiente como un análisis completo.

Este antivirus proporciona protección para el sistema de archivos, el correo electrónico, servicio de mensajería instantánea, la web, las conexiones P2P, además de tener un escudo de scripts de red y para el comportamiento de las aplicaciones.

La opción de limpieza del navegador también es importante, podemos tener bastantes vulnerabilidades a través de sus complementos, los cuales nos analiza avast y nos informa sobre posibles problemas.



4.2.1.- Configuración de antivirus (II).

Tipos de análisis, configuración y programación de los mismos

El antiviruas Avast! nos da la posibilidad de realizar distintos tipos de análisis, todos ellos configurables:

- Análisis rápidos: Analiza la unidad del sistema, rootkits, programas de inicio automático, se pueden incluir programas potencialmente peligrosos (PDD). Podemos modificar las opciones por defecto para este tipo de análisis y adaptarlo a nuestras necesidades.
- Análisis completo del sistema: Realiza un análisis exhaustivo del sistema, es más lento que el anterior. Incluye el análisis de todos los discos duros, rootkits, programas de inicio automático y módulos cargados en memoria. La prioridad del análisis y sensibilidad heurística (ampliaremos este concepto posteriormente) son mayores que en el análisis rápido.
- Análisis de unidades extraíbles.
- Análisis de carpeta seleccionada.
- Crear análisis personalizado: Permite seleccionar los elementos que se quieren analizar (todos los discos duros, la unidad del sistema, la memoria, rootkits, programas de inicio automático, ...) y escoger otras opciones de análisis (sensibilidad heurística, archivos que deben descomprimirse para analizarlos, posibles exclusiones, activar la generación de informes, la programación de tareas, etc.).
- Análisis durante el arranque.

Estos tipos de análisis se pueden adaptar a las necesidades del usuario en aspectos tales como el nivel de sensibilidad heurística, las extensiones de archivos que debe descomprimir para analizar, posibles exclusiones, activación de la generación de informes, la programación de tareas, etc.

Un punto importante es la **programación de tareas de análisis**, con ello evaluaremos el estado de seguridad de nuestro equipo y podremos despreocuparnos de tener que hacerlo manualmente cada cierto tiempo. En Avast! Programamos el análisis desde la opción: Más detalles - Opciones – Programar. En la pantalla de Programar podemos fijar la periodicidad del análisis (una vez, diaria, semanal, mensual), la hora de comienzo, el día de inicio, etc.

Protección con autosandbox.

Avast!, en sus versines de pago, nos da la posibilidad de ejecutar cualquier aplicación sospechosa en un entorno seguro de pruebas o sandbox (caja de arena). Cualquier operación que hagamos con un programa o archivo dentro del sandbox no afectará al sistema con lo que podremos estar seguros de probarlo. Para acceder a la opción de configuración de este entorno seguro de ejecución nos dirigiremos a la opción Herramientas -> SandBOX.

Por defecto esta característica está activada en modo 'Preguntar', con lo que consultará previamente al usuario si quiere transferir la ejecución de una aplicación sospechosa al entorno seguro de pruebas. Para una mayor seguridad, puede ser útil activar el modo 'Auto' y evitar continuas preguntas. Así se aplicará a todos los programas que se ejecuten, por lo que es aconsejable excluir de Sandbox las aplicaciones que utilicemos con

frecuencia y sobre las que tengamos confianza para no ralentizar el uso de las mismas. Esto puede hacerse desde el botón 'Examinar' del apartado de 'Archivos que serán excluidos del Sandbox automático'.

Rescue Disk:

En herramientas nos encontramos con otra opción muy interesante, "Rescue Disc" .

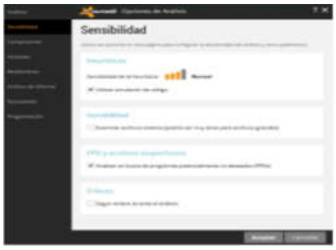
Con ella, podremos crear una unidad de arranque con las definiciones de Avast más recientes. Las definiciones quedan anticuadas con rapidez, por ello es importante crear habitualmente el Rescue Disc, para tenerlas actualizadas si hace falta usarlas.

Gracias a esta herramienta, si tenemos problemas con algún virus, tal que no nos deja iniciar el Sistema Operativo, o inicia pero va mal, podremos resolverlos iniciando con ella el equipo y haciendo el análisis sin arrancar el sistema.

4.2.2.- Configuración de antivirus (III).

Uso de la heurística.

Las técnicas heurísticas se utilizan para poder detectar amenazas no registradas en la lista de virus conocidos por el antivirus. Consiste en una comparación de patrones de código sospechosos y ciertos comportamientos con los programas o archivos del equipo. El empleo de estas técnicas consume bastantes recursos por lo que el rendimiento del equipo puede verse afectado, por esta razón el antivirus permite ajustar el nivel de sensibilidad de la heurística. Podemos adaptar la heurística en Análisis completo del sistema -> Opciones -> Sensibilidad.



Mejora del uso de los recursos.

Los desarrolladores de antivirus han realizado un esfuerzo considerable para conseguir que los programas antivirus consuman la menor cantidad de recursos posible. Avast! nos permite configurar ciertas opciones que nos ayudarán a mejorar el rendimiento del antivirus. Para acceder a ellas accedemos a Análisis completo del sistema -> Opciones.

Podemos indicarle que analice archivos comprimidos y que tipos. Si queremos que analice los archivos muuy grandes o que analice en busca de programas potencialmente no deseados (PPDs).

En el apartado Rendimiento nos encontramos con la posibilidad de utilizar la memoria caché transitoria en la que se guardan los archivos ya analizados durante la actual sesión de trabajo para evitar que vuelvan a ser comprobados hasta que el equipo se reinicie, o la base de datos de virus sea actualiza. Por último, si se activa la caché persistente, conseguiremos almacenar los identificadores de los archivo “seguros” vigentes siempre para que sean analizados sólo una vez, incluso si reiniciamos o se actualiza la base de datos de virus.

Mantenimiento

Desde opciones > Actualización podemos actualizar la base de datos de virus y el programa, de forma automática – el programa detecta por sí sólo las actualizaciones, se las descarga y avisa al usuario – o también podremos hacerlo manualmente. Además, otro módulo útil es el baúl de virus, consistente en una ruta a la que se mueven los archivos detectados como peligrosos o infectados (archivos en cuarentena). Si durante el análisis se encuentra alguno de estos archivos puede darse la opción al usuario de desinfectar, eliminar, ignorar o mover al baúl.