Configuración de Kaspersky Endpoint Security 10 SP1

El antivirus, versión para casa, está configurado para que lo adaptemos según nuestras necesidades y según los recursos de nuestro equipo doméstico.

Está versión sólo está permitida para ordenadores de uso doméstico, no debemos utilizarla en equipos que pertenezcan a la Universidad.

Se distribuye con todos los módulos, excepto el cifrado por temas de gestión de licencias con la empresa. Al distribuirse con todos los módulos activos, el ordenador si no dispone de recursos necesarios, se verá afectado en el rendimiento. Es aconsejable adaptar los módulos a nuestras necesidades.

Requisitos de Hardware y Software

Para garantizar el funcionamiento adecuado el equipo debe cumplir:

- 2 Gb de espacio libre en el disco duro
- Microsoft Internet Explorer 7.0
- Microsoft Windows Installer 3.0
- Conexión a Internet para activar la aplicación y actualizar las bases de datos y módulos de la aplicación.

Requisitos hardware mínimos:

- Ms Windows XP Pro x86 Edition SP3
  - Procesador Intel Pentium a 1 GHz o equivalente compatible
  - 512 Mb de RAM, se recomienda 1 Gb
- Ms Windows Vista SP2, Windows 7 Pro / Enterprise / Ultimate SP1, Windows 8 Pro / Enterprise, Windows 8.1 Enterprise
  - Procesador Intel Pentium a 1 GHz o equivalente para 32 bits
  - Procesador Intel Pentium a 2 GHz o equivalente para 64 bits
  - 1 Gb de RAM libre

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

Componentes del cliente KES 10 SP1

Los componentes que incluye el cliente Kaspersky 10 SP1 son:

1. Antivirus de archivos

El componente Antivirus de archivos protege el equipo frente a la infección del sistema de archivos. De forma predeterminada, el Antivirus de archivos se inicia con Kaspersky Endpoint Security, permanece activo todo el tiempo en la memoria del equipo y analiza todos los archivos que se abren, guardan o ejecutan en el equipo y en todas las unidades que se incorporan a él en busca de virus y otro software malicioso (malware).

2. Antivirus del correo

Analiza los mensajes de correo entrantes y salientes en busca de virus y otro software malicioso (malware). Analiza tráfico POP3, SMTP, IMAP, MAPI y NNTP.

Este componente interactúa con las aplicaciones de correo electrónico instaladas en el equipo. En el caso de los clientes de correo electrónico Microsoft Office Outlook® y The Bat!, los módulos de extensión (complementos) le permiten efectuar un ajuste preciso de la configuración del análisis de mensajes de correo electrónico.

3. Antivirus para chat

Analiza el tráfico de clientes de mensajería instantánea; estos pueden contener URL's que intentan descargar código malicioso, direcciones URL's de programas maliciosos y sitios web que los intrusos utilizan para ataques fraudulentos.

Estos ataques persiguen robar datos privados del usuario, números de tarjetas, contraseñas para pagos bancarios y otros servicios en línea, como cuentas de correo-e o credenciales de redes sociales.

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

4. Antivirus Internet

Analiza el tráfico HTTP y FTP, entrante y saliente; también comprueba las direcciones URL por medio de la lista de direcciones web maliciosas o fraudulentas.

Intercepta y analiza virus y otras amenazas en cada página web o archivo a los que el usuario o una aplicación acceden.

5. Firewall

Nunca lo tenemos activado, dejamos por defecto el firewall de windows

6. Control de vulnerabilidades

El componente Control de vulnerabilidades ejecuta un análisis en tiempo real de vulnerabilidades de aplicaciones que están en ejecución en el equipo o iniciadas por el usuario.

7. Prevención de intrusiones

La prevención de intrusiones analiza el tráfico de red entrante en busca de actividad habitual de los ataques de red. Al detectar un intento de ataque de red dirigido a su equipo, Kaspersky Endpoint Security bloquea la actividad de red del equipo atacante. A continuación aparece una advertencia, en la que se comunica que se ha producido un intento de ataque de red y muestra información sobre el equipo atacante.

El tráfico de red del equipo de ataque se bloquea durante una hora.

8. Control de actividad de aplicaciones

El control de actividad de aplicaciones evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos de identidad.

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

Este componente controla la actividad de las aplicaciones, entre las que se incluyen el acceso a recursos protegidos (como archivos, carpetas, claves de registro), mediante el uso de *reglas de control de aplicaciones*. Las reglas de control de aplicaciones son un conjunto de restricciones que se aplican a varias acciones de aplicaciones del sistema operativo y a los derechos de acceso a los recursos del equipo.

9. Control Web

Permite que los usuarios de la LAN controlen acciones restringiendo o bloqueando el acceso a los recursos web. Los recursos web son una página web, varias, un sitio web o varios que cuentan con una característica común.

Puede restringir o bloquear el acceso a categorías específicas de recursos web p.e. bloquear el acceso a sitios que pertenecen a la categoría "Redes Sociales"

10.Control de dispositivos

El control de dispositivos garantiza la seguridad de los datos privados gracias a una restricción del acceso de usuarios a dispositivos que se instalan en el equipo o se conectan a él:

Dispositivos de almacenamiento de datos (discos duros, unidades extraíbles, unidades de cinta, unidades de CD/DVD)

Herramientas de transferencia de datos (módems y tarjetas de red externas)

Dispositivos diseñados para convertir datos en copias impresas (impresoras)

Buses de conexión (conocidos también como "buses"), que corresponden a interfaces para conectar dispositivos a equipos (como USB, FireWire e infrarrojos)

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

11.System Watcher [Análisis heurístico]

Recopila datos sobre las acciones de las aplicaciones de su equipo y pasa esta información a otros componentes para proporcionar una protección más fiable.

No se recomienda activar este módulo a menos que sea absolutamente necesario, ya que afecta al rendimiento de los componentes de protección.

Propuesta de configuración

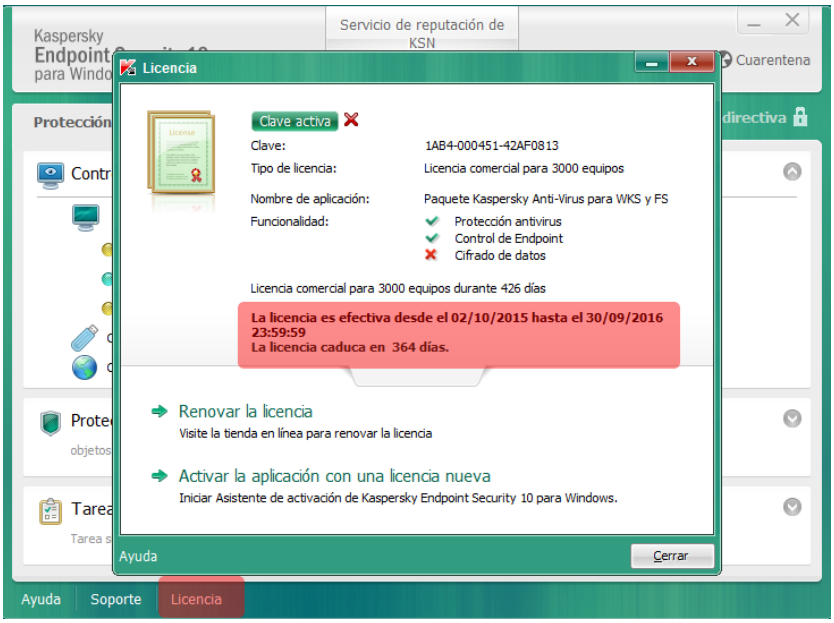
Para facilitarles la tarea, hemos creado la siguiente propuesta de configuración, no obstante serán ustedes los que deberían adaptarlas a sus necesidades y recursos.

Licencia y Versión de mi cliente

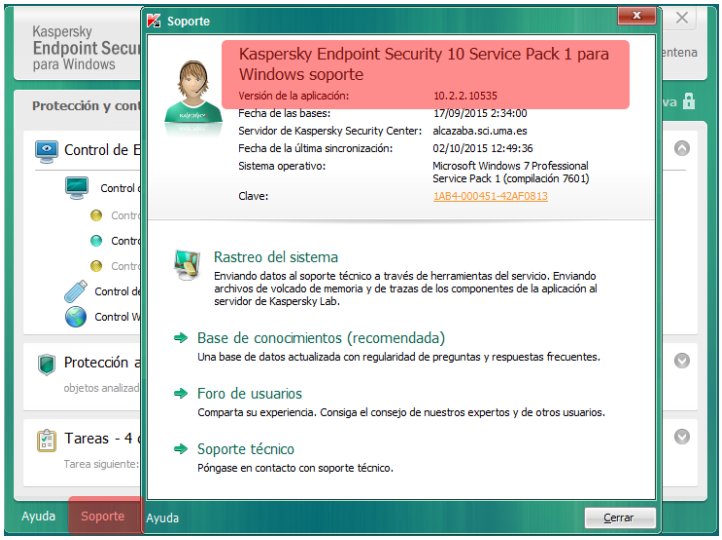
Lo primero que deberemos reconocer será nuestra versión de cliente y si la licencia está vigente. Lo podemos ver abriendo la consola del antivirus, que está junto al reloj de Windows, una K mayúscula.

Haciendo click, sobre **licencia** en la parte inferior de la ventana de la consola, aparecerá la ventana de licencia.

Observamos los paquetes que integran la licencia y el intervalo de vigencia.



Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es



Si pulsamos sobre **Soporte** podemos ver la versión del cliente instalado.

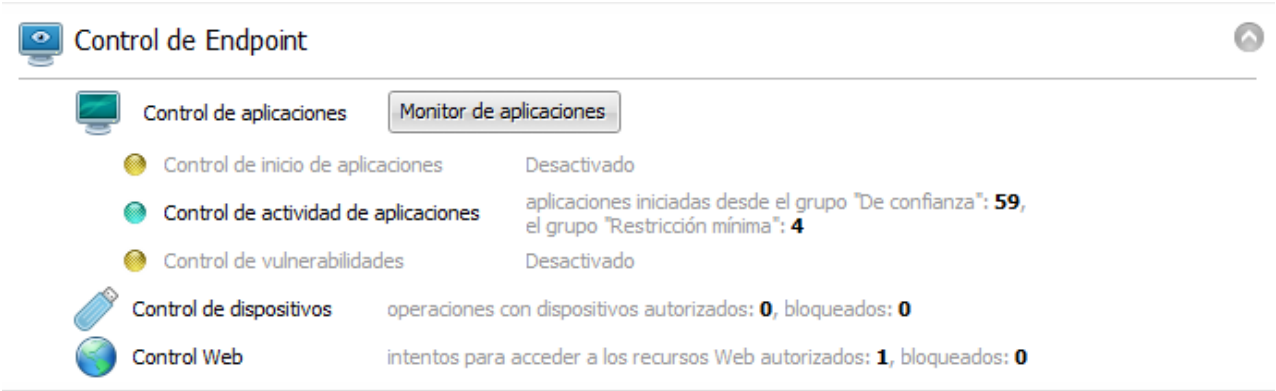
En el momento de hacer esta guía, la última versión es la que aparece en la captura.

Sobre esta versión está hecha la guía y esta será la versión que deberíamos tener instalada. No importa que el ordenador no tenga suficientes recursos, eso lo solucionaremos quitando módulos para no sobrecargar los recursos de la máquina.

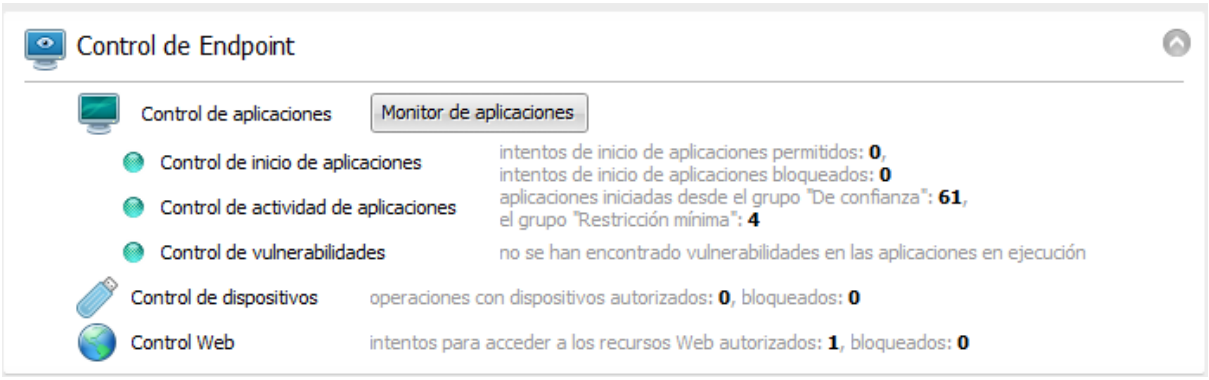
Sección Control de Endpoint

La primera sección del cliente, si está recién instalado, debería ser parecida a lo que se ve en esta captura:

Los controles que está amarillos no están activados, pulsamos sobre ellos para activarlos o desactivarlos.



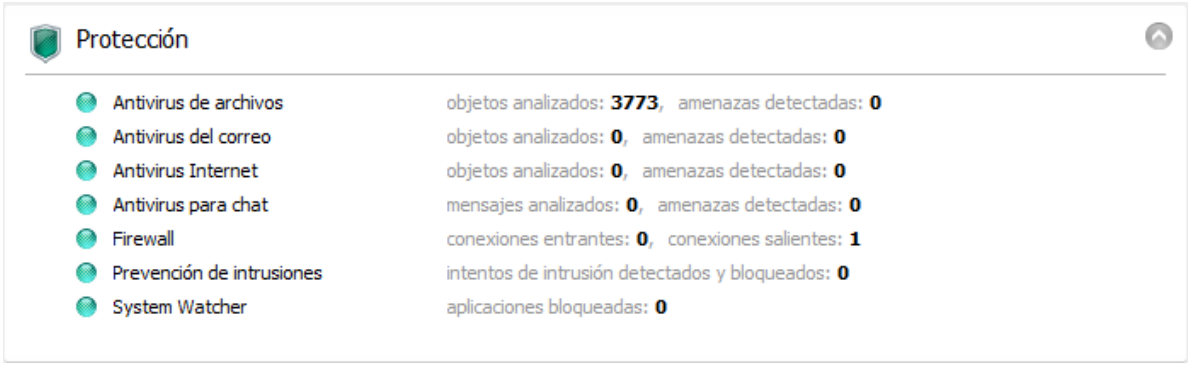
Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es



Aconsejamos tenerlo todo activado, si acaso podemos desactivar el **control web** caso que no queramos controlar las web a las que accederemos.

Sección de protección

Es la segunda sección según el orden del interfaz y es donde más tendremos que afinar para conseguir un equilibrio entre protección y recursos.

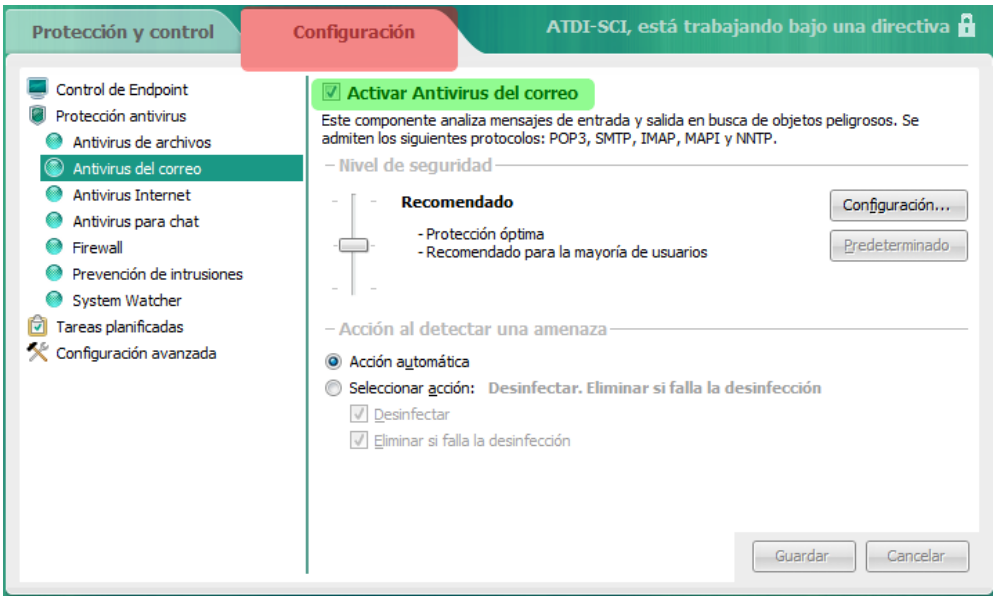


Por defecto están todos los módulos activos, en verde, pero algunos podríamos desactivarlos dependiendo de nuestro uso del ordenador.

Por ejemplo, si el correo lo leemos por webmail podemos desactivar el **antivirus de correo**, también caso que no utilicemos programas de chat, el de **antivirus para chat**. Podemos utilizar el **firewall** de windows y el análisis heurístico que siempre consume muchos recursos, **system watcher**, también podemos desactivarlo.

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

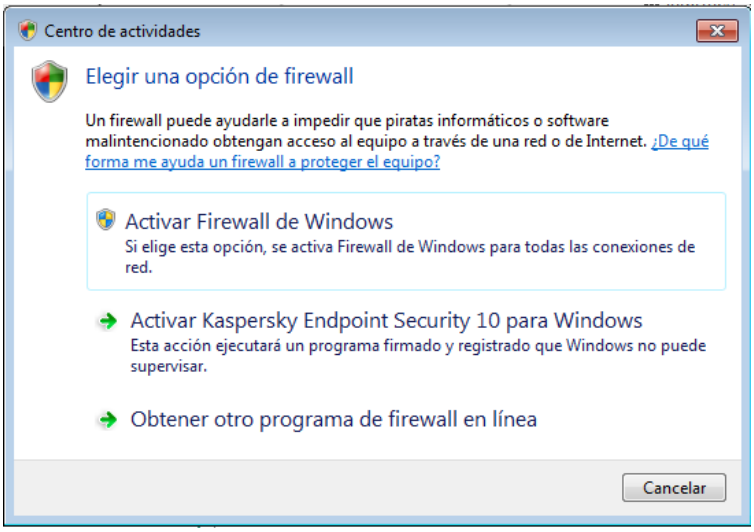
Para desactivar los módulos pulsamos sobre la pestaña **configuración** y luego desmarcamos la casilla de verificación del módulo a desactivar.



Si desactivamos el **firewall** no deberíamos olvidar activar el de windows.

Al desactivar el de Kaspersky, Windows nos alerta por si queremos activar el de Windows.

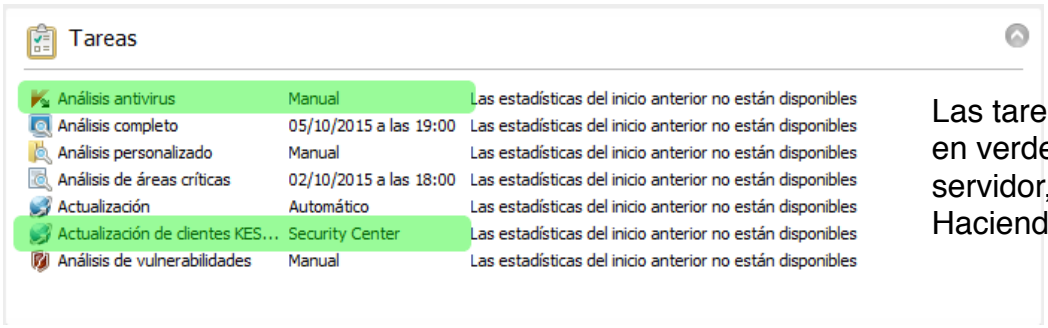
El firewall también se puede activar desde el panel de control de Windows.



Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

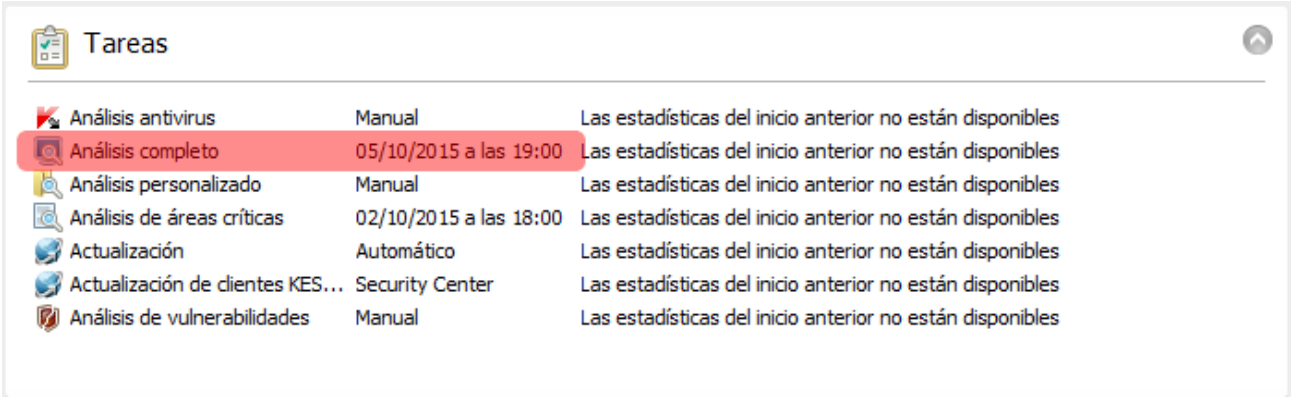
Sección de Tareas

La última sección es la que corresponde a las tareas, actualización, análisis, etc.



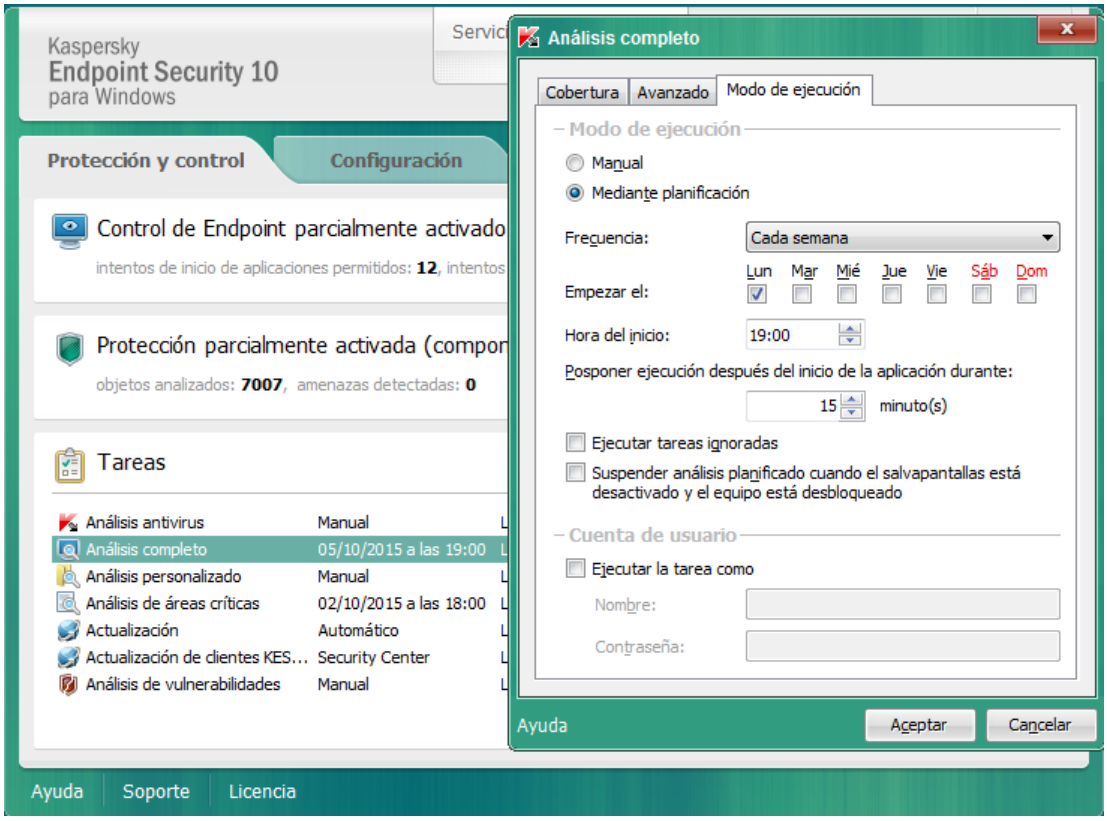
Las tareas configuradas y marcadas en verde, están programadas en el servidor, el resto se puede manipular. Haciendo click sobre ellas.

Viene configurada una tarea por defecto que te hace un análisis completo del ordenador los Lunes a las 19:00h, siempre; esto lo podemos modificar si hacemos click sobre esa tarea.



Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es

Podemos desactivarla y ponerla de forma manual o programarla para otro día, según nuestras necesidades.



Contacto:

Boulevard Louis Pasteur, 33 - 29071 MÁLAGA. Tel.: 952131466 /67 Fax: 952131492
E-mail- sci@uma.es www.sci.uma.es