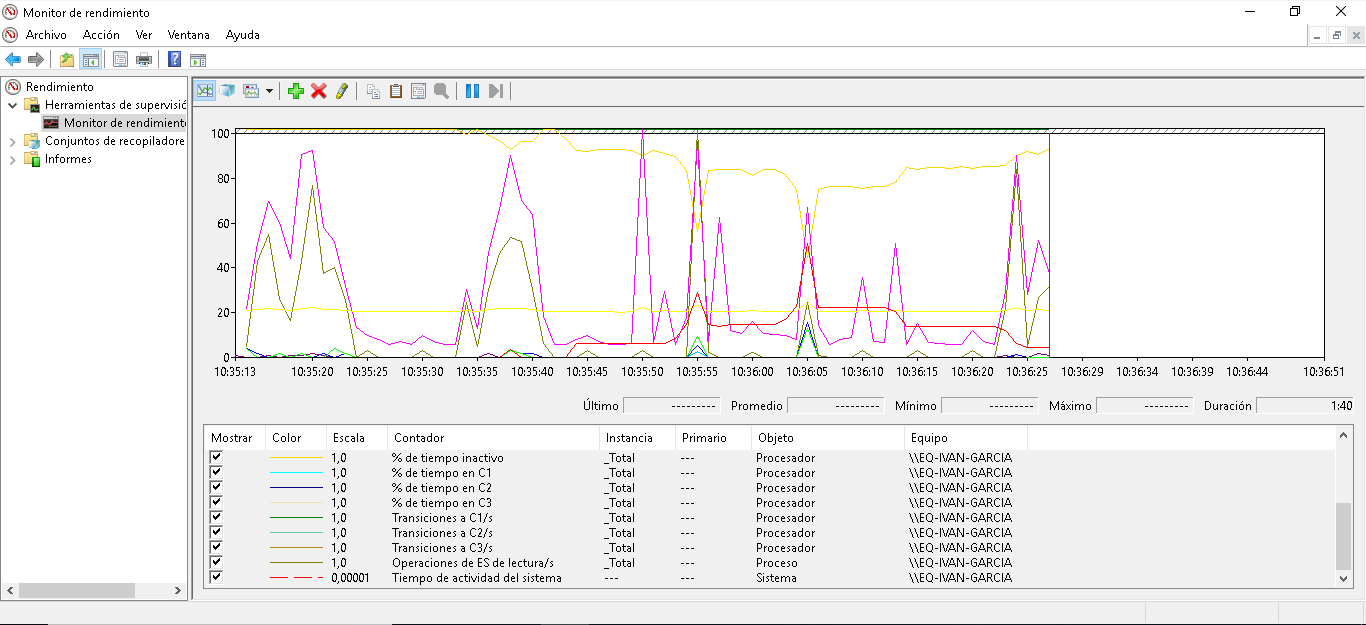
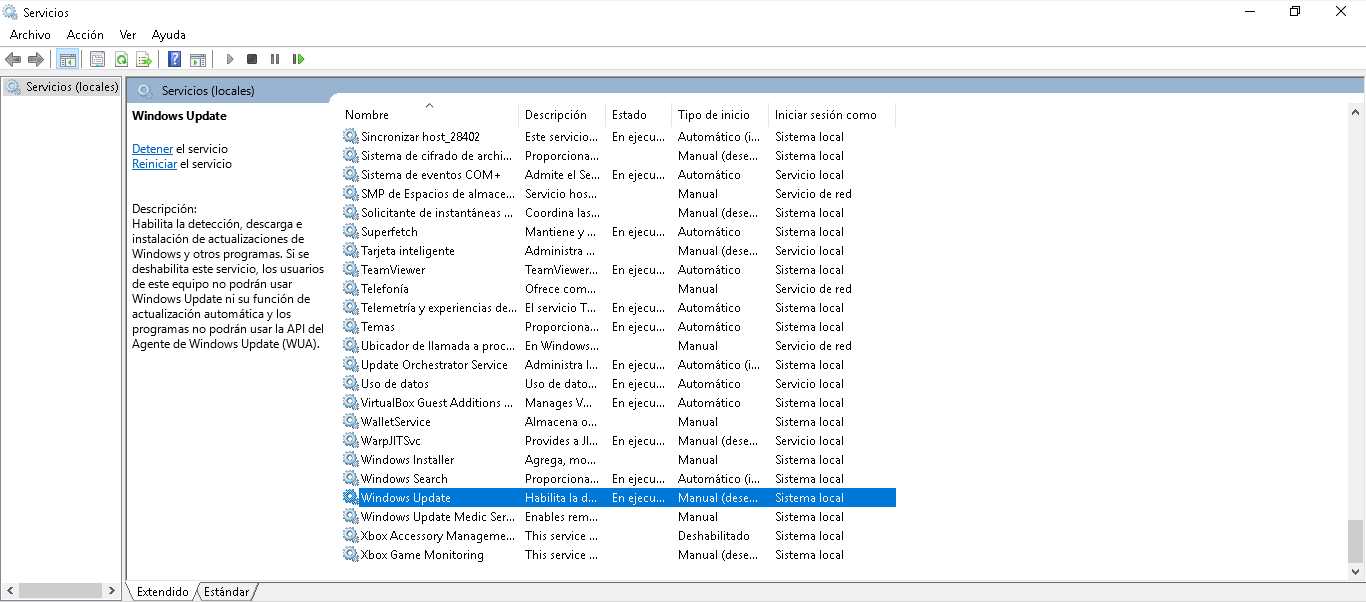
Monitor del Sistema, Servicios, Windows Defender y GPO

***Práctica: Monitor del Sistema y Servicios***

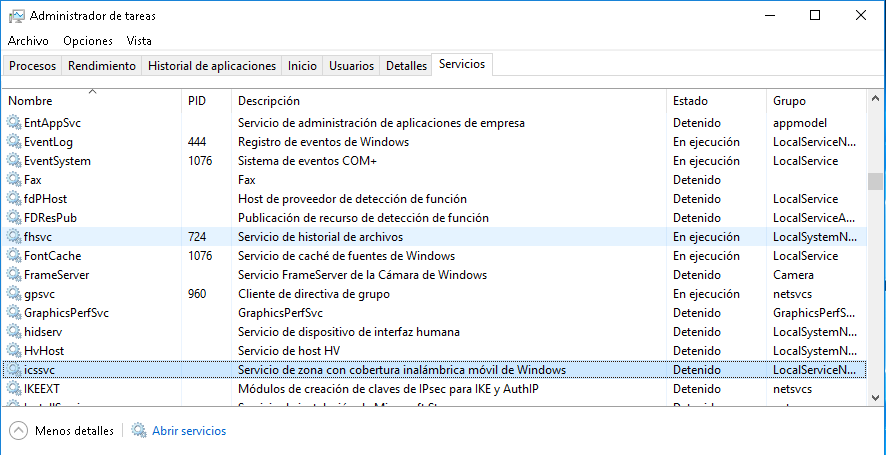
Abre el monitor de rendimiento de Windows, agrega los componentes Procesador, %tiempo inactivo sistema y procesos y operaciones de lectura de archivos. Para realizar su seguimiento observa la gráfica

Inicio 🡪 Monitor de rendimiento 🡪 Monitor de rendimiento🡪 Botón verde 🡪 Buscamos los componentes a añadir 🡪 Agregar 🡪 Aceptar

Abre la consola de servicios y detén, inicia, pausa y reanuda el servicio de Windows Update.

Inicio 🡪 Servicios 🡪 Buscamos Windows Update 🡪 Detener 🡪 Iniciar 🡪 Pausar 🡪 Reanudar

Desde el administrador de tareas, localiza el servicio de Google Update (comprueba que lo tienes) y deshabilita su inicio.

Inicio 🡪 Administrador de tareas 🡪 Servicios 🡪 Google Update (No lo tengo)

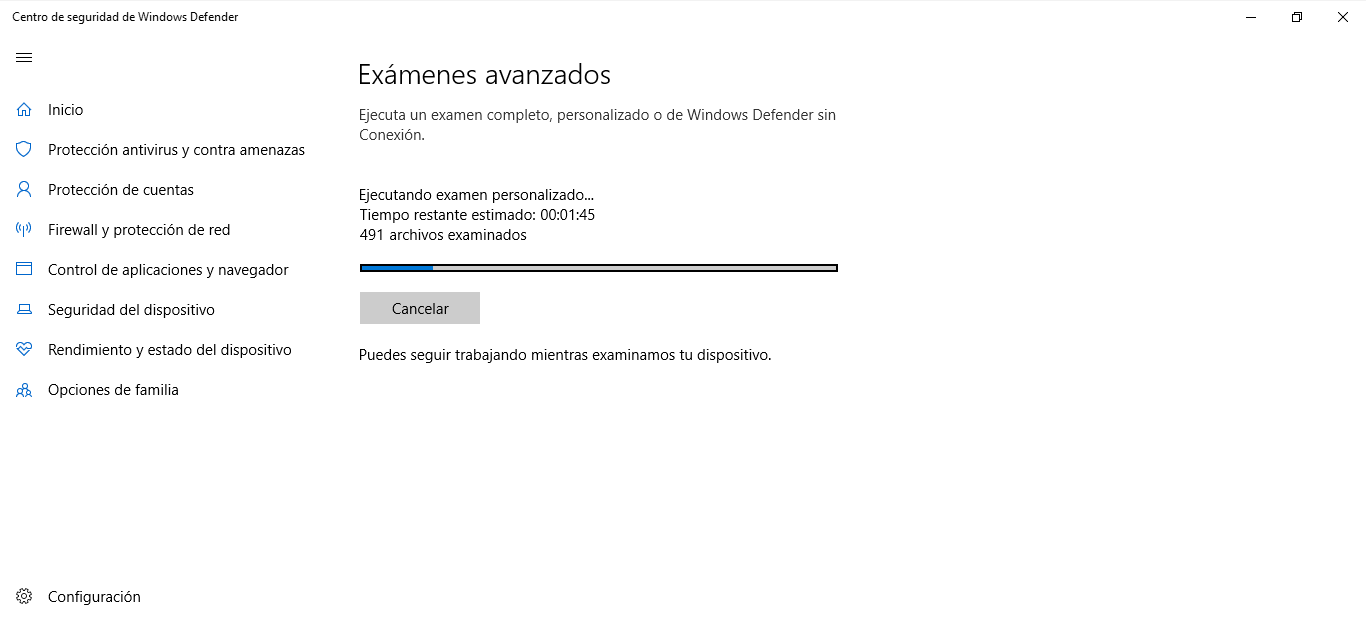
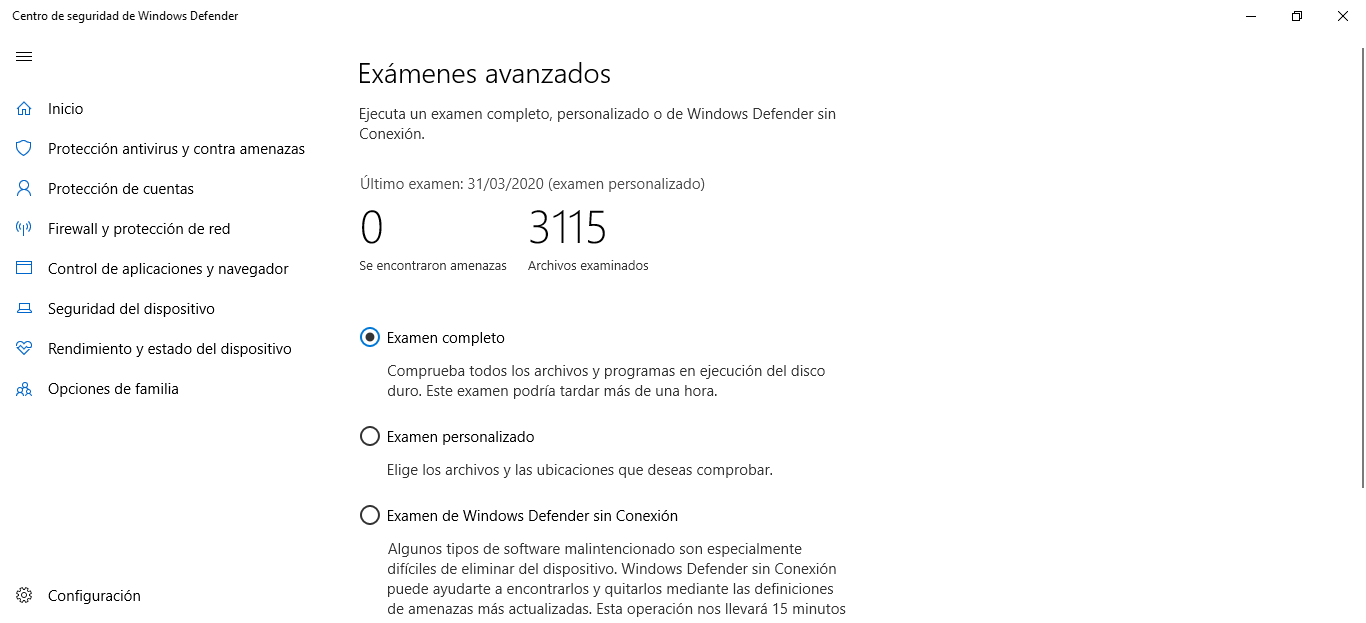
Prueba otras opciones de servicios

✔

***Práctica: Windows Defender***

Realizar un análisis de una unidad extraíble que tengas conectada al ordenador y una captura de pantalla del proceso y otra del resultado del análisis. ¿Se ha detectado alguna amenaza? En caso afirmativo, ¿de qué tipo? ¿qué acciones has tomado (¿eliminar, ignorar alerta, poner en cuarentena el archivo? Razona tu respuesta.

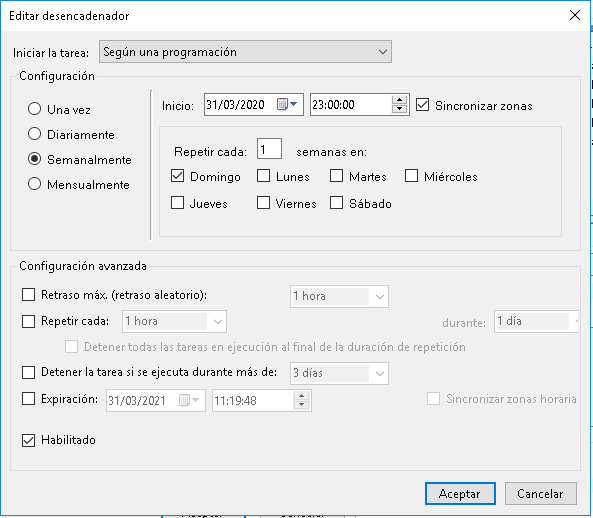
Inicio 🡪 Equipo 🡪 Unidad extraíble (Clic derecho) 🡪 Examinar con Windows Defender

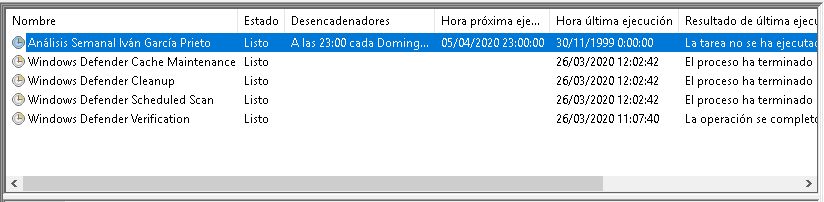
 

No he tomado ninguna acción dado que no tengo amenazas en mi unidad extraíble.

Utilizaremos la acción de eliminar cuando no queramos analizar más detenediamente el archivo infectado o no queramos recuperar información contenida en dicho archivo.  
Moveremos el archivo en cuarentena por defecto, de esta manera el archivo no podrá hacer daños a nuestro equipo, podrá ser analizado más detenidamente, y en caso de ser una falsa alarma podremos recuperar el archivo.  
Solo ignoraremos la alerta en caso de que estemos completamente seguros de que se trate de una falsa alarma.

A continuación, configura un análisis programado para que se ejecute semanalmente a las 23:00 horas y que revise todos las unidades de disco y la memoria. Nombra la tarea como 'ANÁLISIS SEMANAL <Tu Nombre y Apellidos>'. Realiza una captura de pantalla de la configuración de la programación.

Inicio 🡪 Programador de tareas 🡪 Biblioteca 🡪 Microsoft 🡪 Windows 🡪 Windows Defender 🡪 Crear tarea 🡪 Desencadenadores 🡪 Nuevo 🡪 Semanalmente a las 23:00 🡪 Aceptar 🡪 Acciones 🡪 Nueva 🡪 Iniciar un programa 🡪 Programa: “C:\Program Files\Windows Defender\MpCmdRun.exe” 🡪 Agregar argumentos 🡪 “Scan -ScheduleJob -ScanTrigger 55”🡪 No 🡪 Aceptar 🡪 Aceptar



***Práctica: GPOs Directivas de seguridad local y Directivas de grupo local.***

Habilita las directivas de contraseña correspondientes para que el sistema

Inicio 🡪 Ejecutar 🡪 SecPol.msc 🡪 Configuración de seguridad 🡪 Directivas de cuenta 🡪

Guarde registro de las 4 últimas contraseñas de usuario.

Directiva de contraseñas 🡪 Almacenar contraseña con cifrado reversible 🡪 Habilitar 🡪 Aplicar 🡪 Aceptar

Directiva de contraseñas 🡪 Exigir historial de contraseñas 🡪 4 🡪 Aplicar 🡪 Aceptar

Deben de ser complejas

Directiva de contraseñas 🡪 Las contraseñas deben cumplir los requerimientos de complejidad 🡪 Habilitar 🡪 Aplicar 🡪 Aceptar

Tener una vigencia máxima de 1 mes

Directiva de contraseñas 🡪 Vigencia máxima de la contraseña.🡪 10 🡪 Aplicar 🡪 Aceptar

Longitud mínima de 10 caracteres.

Directiva de contraseñas 🡪 Longitud minina de la contraseña 🡪 10 🡪 Aplicar 🡪 Aceptar

Permitir hasta 3 equivocaciones del usuario al iniciar sesión.

Directiva de bloqueo de cuenta 🡪 Umbral de bloqueo de la cuenta 🡪 3 🡪 Aplicar 🡪 Aceptar

Denegar el inicio de sesión local a un usuario de tu sistema (el que tú quieras).

Inicio 🡪 Ejecutar 🡪 SecPol.msc 🡪 Configuración de seguridad 🡪 Directivas locales 🡪 Asignación de derechos de usuario 🡪 Denegar el inicio de sesión local 🡪 Agregar usuario o grupo 🡪 Opciones avanzadas 🡪 Buscar ahora 🡪 Seleccionamos el usuario 🡪 Aceptar 🡪 Aceptar 🡪 Aplicar🡪 Aceptar

Cambiar el nombre de las cuentas de invitado y administrador desde aquí, configurando la correspondiente GPO, y habilita/deshabilita las mismas.

Inicio 🡪 Ejecutar 🡪 SecPol.msc 🡪 Configuración de seguridad 🡪 Directivas locales 🡪 Cuentas: cambiar el nombre de la cuenta de invitado/administrador 🡪 Aplicar 🡪 Aceptar