

Tarea 5: Administración Básica del Sistema (Windows II)

Francisco Javier Sueza Rodríguez

13 de marzo de 2023

Centro: IES Aguadulce
Ciclo Formativo: Desarrollo Aplicaciones Web (Distancia)
Asignatura: Sistemas Informáticos
Tema: Tema 5 - Administración Básica del Sistema (Windows II)

Índice

1 Caso Práctico	4
2 Actividades	4
2.1 Actividad 1: Estructura Departamental	4
2.1.1 Enunciado	4
2.1.2 Solución	4
2.2 Actividad 2: Cuentas de Usuario Locales	5
2.2.1 Enunciado	5
2.2.2 Solución	6
2.3 Actividad 3: Permisos de Archivos y Carpetas	9
2.3.1 Enunciado	9
2.3.2 Solución	9
2.4 Actividad 4: Directivas de Seguridad y Grupo Local	12
2.4.1 Enunciado	12
2.4.2 Solución	13
2.5 Windows Defender: Programar Análisis	17
2.5.1 Enunciado	17
2.5.2 Solución	17
2.6 Actividad 6: Windows Update	19
2.6.1 Enunciado	19
2.6.2 Solución	19
2.7 Actividad 7: Monitor de Rendimiento	21
2.7.1 Enunciado	21
2.7.2 Solución	21
2.8 Actividad 8: Servicios	23
2.8.1 Enunciado	23
2.8.2 Solución	23
2.9 Actividad 9: Puntos de Restauración	25
2.9.1 Enunciado	25
2.9.2 Solución	25
2.10 Actividad 10: Copia de Seguridad	26
2.10.1 Enunciado	26
2.10.2 Solución	27

Índice de figuras

2.1	Estructura de carpetas a crear	4
2.2	Estructura de directorios creada	4
2.3	Archivos creados es las carpetas Marketing y Gestión	5
2.4	Ventana de creación de usuario	6
2.5	Introducción de datos de usuario	6
2.6	Usuario creados con lusrmgr	7
2.7	Ventana de creación de un nuevo grupo	7
2.8	Introducción de datos del nuevo grupo	8
2.9	Agregación de un usuario al grupo	8
2.10	Grupo Gestión creado	8
2.11	Grupo Marketing creado	9
2.12	Ventana con permisos de la carpeta Gestión	10
2.13	Modificación de los permisos de la carpeta Gestión	10
2.14	Modificación de los permisos de la carpeta Marketing	11
2.15	Acceso a la carpeta Gestión con la usuaria ggongora	11
2.16	Acceso a la carpeta Marketing con la usuaria ggongora	12
2.17	Acceso a las carpetas con el usuario creado en la instalación	12
2.18	Ventana para el cambio de directivas de cuenta	14
2.19	Cambio de la longitud de contraseña requerida	14
2.20	Resumen de las directivas de contraseña	14
2.21	Cambio del umbral de bloque de cuenta	15
2.22	Resumen de la directivas de bloque de cuenta	15
2.23	Ventana de la aplicación gpedit para modificar la directivas de grupo local	16
2.24	Directiva para impedir el acceso al símbolo del sistema	16
2.25	Intento de acceso al símbolo del sistema	17
2.26	Protección antivirus y otras amenazas	18
2.27	Desencadenador creado para la tarea de Windows Defender	18
2.28	Filtro de evento creado en formato XML	19
2.29	Ventana principal de Windows Update	20
2.30	Cambio de rango horario para la ejecución de Windows Update	20
2.31	Activación de notificaciones de Windows Update	21
2.32	Recolector de datos creado en ejecución	22
2.33	Informe del primer análisis de rendimiento	22
2.34	Informe del segundo análisis de rendimiento	23
2.35	Gestor de servicios de Windows 10	24
2.36	Inicialización del Cliente Web	24
2.37	Audio de Windows deshabilitado	24
2.38	Creación de un punto de restauración	25
2.39	Tema cambiado a Windows(claro)	26
2.40	Sistema Restaurado	26
2.41	Nueva unidad formateada en el gestor de discos	27
2.42	Configuración de copias de seguridad	27

1. Caso Práctico

María ya tiene instalado en los equipos de la empresa AguadulSoft el sistema operativo y ahora es el momento de empezar a administrar el sistema para configurarlo y ponerlo en marcha para su utilización. Como es la primera vez, Juan le va a ayudar en el proceso de administración básica del sistema. Ada será la que les dé el visto bueno.

2. Actividades

2.1. Actividad 1: Estructura Departamental

2.1.1. Enunciado

Crea la siguiente estructura departamental de carpetas colgando directamente de la raíz del disco en la que está instalado Windows 10. Crea primero la carpeta `AguadulSoft` dentro de esta las demás:

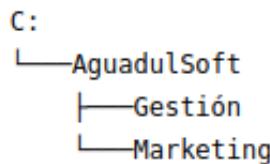


Figura 2.1: Estructura de carpetas a crear

Introduce dos archivos, un documento y una imagen, en la carpeta de cada departamento (Gestión y Marketing) y nómbralos como `tipoArchivo_nombreDepartamento` (por ejemplo, en la carpeta “Gestión” el documento sería nombrado como “`documento_gestión`” y la imagen como “`imagen_gestión`”).

Capturas:

- Muestra de la estructura departamental de carpetas y de su ubicación.
- Archivos de cada carpeta.

2.1.2. Solución

1. En primer lugar hemos creado los directorios desde la interfaz gráfica.

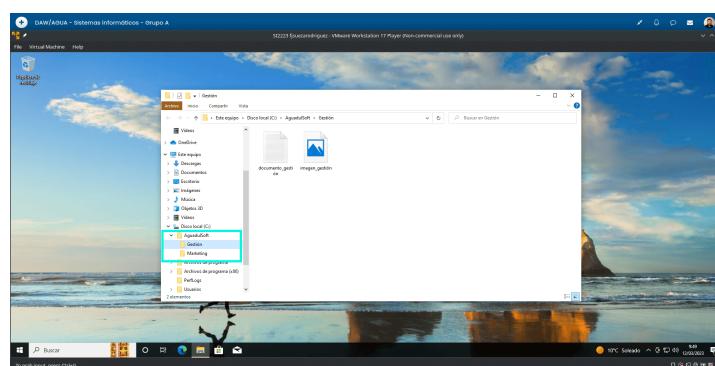


Figura 2.2: Estructura de directorios creada

2. A continuación, hemos añadido 2 archivos a cada directorio creado, como se especifica en el enunciado. Se ha usado también la opción “Nuevo →archivo de texto/imagen de mapa de bits” para crear estos archivos.

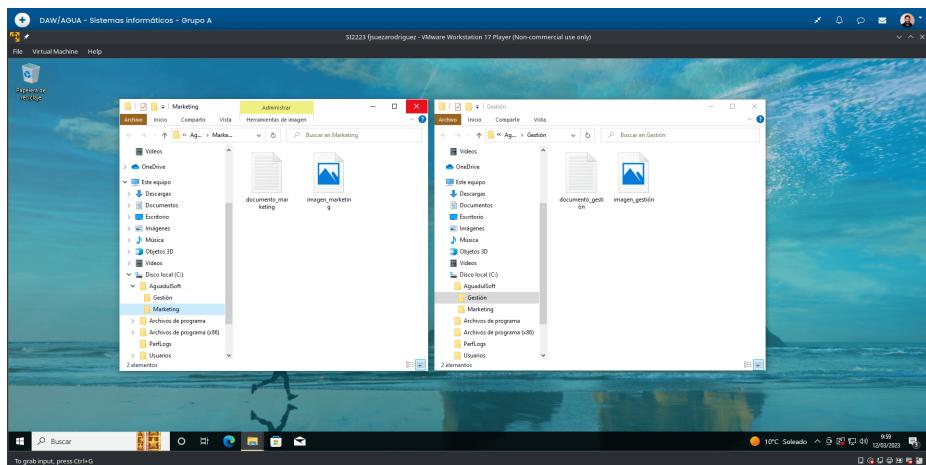


Figura 2.3: Archivos creados es las carpetas Marketing y Gestión

2.2. Actividad 2: Cuentas de Usuario Locales

2.2.1. Enunciado

- 2.a) **Creación de Usuarios:** crea las siguientes cuentas de usuarios locales (con privilegios limitados):

- Gestión: Graciela Góngora y Genaro García.
- Marketing: Matías Martínez y Marta Mejías.

Nombra cada cuenta de usuario como InicialNombreApellido e introduce en el campo “Nombre completo” su nombre y apellido completos y en el campo “Descripción” el nombre del departamento al que pertenece (por ejemplo, el usuario “Graciela Góngora” del departamento “Gestión” sería nombrado como “ggongora” y en sus campos se introduciría “Graciela Góngora” en “Nombre completo” y “Dpto. de Gestión” en “Descripción”).

Capturas:

- Ventana/consola donde se crea un nuevo usuario (indica textualmente cómo se accede a dicha ventana).
- Introducción del nombre y campos “Nombre completo” “Descripción” de la primera cuenta de usuario.
- Resumen de las cuentas de usuario creadas con sus respectivos nombres y itemize

- 2.b) **Creación de Grupos:** crea un grupo de usuarios para cada departamento, nómbralos con su nombre de departamento y en el campo “Descripción” introduce el texto “Departamento de X” donde X es el nombre del departamento (por ejemplo, el grupo de usuarios del departamento “Gestión” sería nombrado como “Gestión” y en su campo “Descripción” se introduciría “Departamento de gestión”).

Incluye en cada uno de ellos sus usuarios correspondientes, creados en la actividad anterior.

Capturas:

- Ventana donde se crea un nuevo grupo de usuarios (indica textualmente cómo se accede a dicha ventana).
- Introducción del nombre y campo “Descripción” del primer grupo de usuarios.
- Asignación de los usuarios del primer grupo de usuarios.
- Resumen de los grupos de usuarios creados con sus respectivos nombres, campos y usuarios.

2.2.2. Solución

1. En primer lugar, hemos **creado los usuarios solicitados** con los datos que se especifican en el enunciado. Hemos elegido la opción de crearlos mediante la aplicación **LUSRMGR.MSC**, ya que es la que proporciona las opciones de configuración más completas.

Para acceder a esta aplicación, hemos ejecutado el comando **LUSRMGR.MSC** en consola, aunque se puede poner también en la barra de búsqueda de Windows y clickar en la aplicación que nos da como resultado. Una vez ahí, hemos pulsado en la opción “**Acciones adicionales** → **Nuevo usuario**.

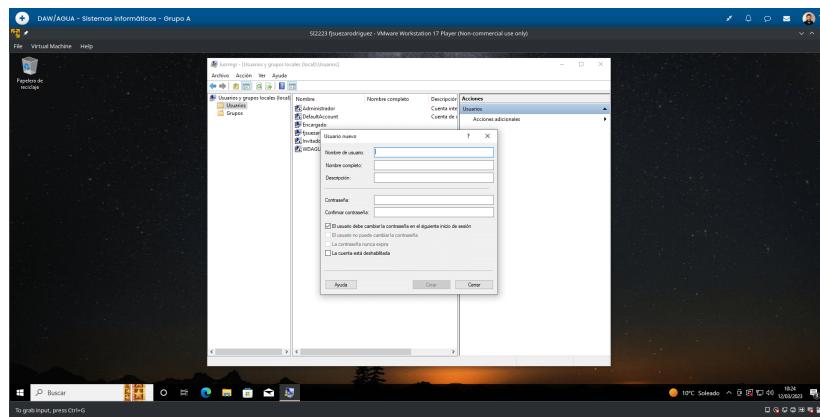


Figura 2.4: Ventana de creación de usuario

A continuación hemos introducido los datos solicitados, tal y como se explica en el enunciado.

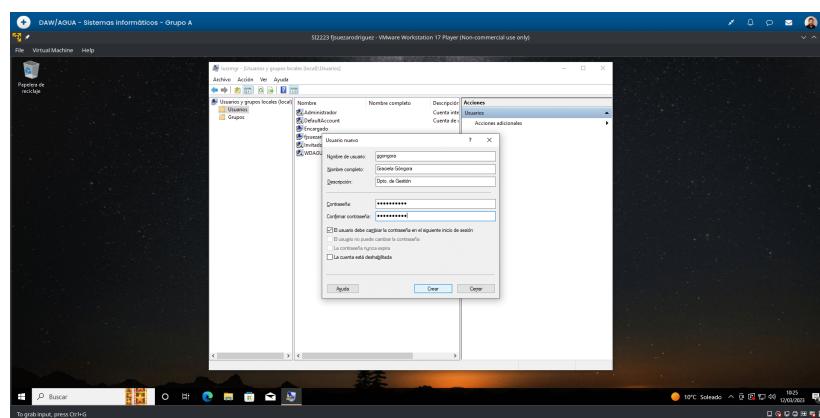


Figura 2.5: Introducción de datos de usuario

Tras haber creado los 4 usuarios que se piden, las cuentas de usuario que tenemos en el sistema las podemos ver en la ventana principal de **lusrmgr**, como vemos en la siguiente captura.

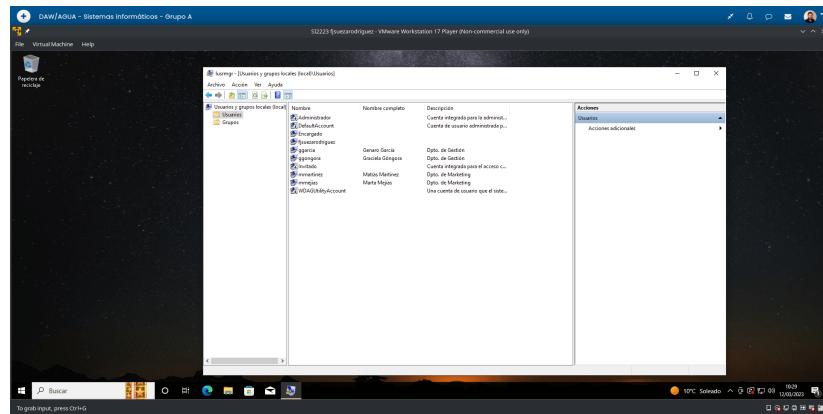


Figura 2.6: Usuario creados con lusrmgr

- En segundo lugar vamos a **crear los grupos** que se nos piden y añadir a ellos los usuarios pertinentes. Para esa tarea vamos a usar también la aplicación **lusrmgr**, tal y como hemos hecho en el punto anterior. La forma de acceso a la aplicación es la misma que en punto anterior, la única diferencia es que hemos pulsado en la opción **Grupos** del menú de la izquierda una vez abierta esta.

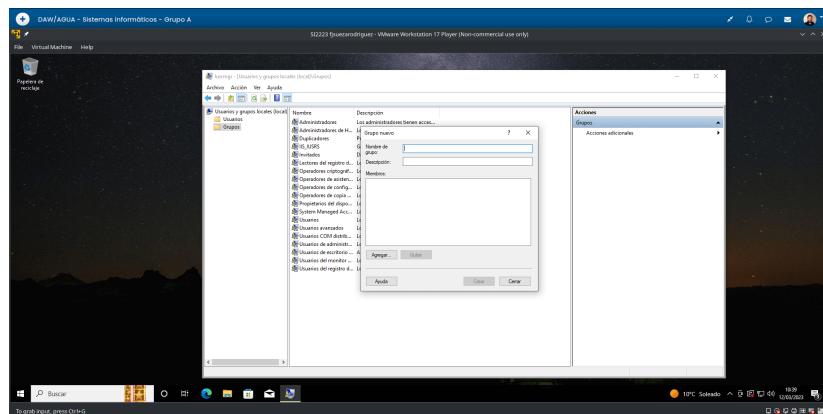


Figura 2.7: Ventana de creación de un nuevo grupo

Una vez que estamos en esta ventana, podemos introducir los diferentes datos que se nos piden, como es el nombre del grupo y su descripción.

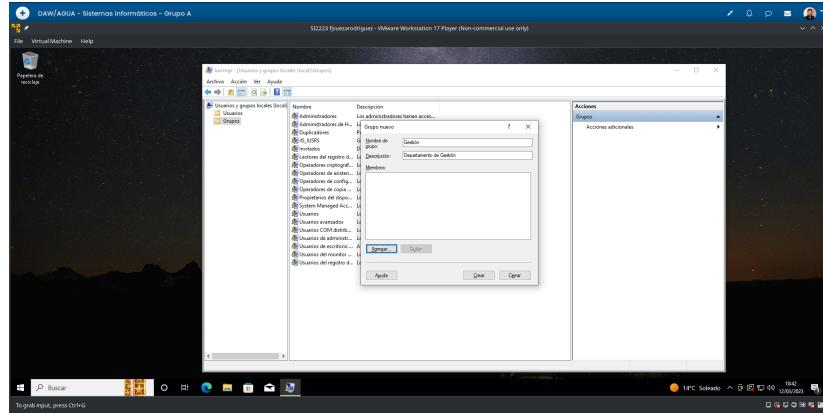


Figura 2.8: Introducción de datos del nuevo grupo

En esta misma ventana, podemos agregar los usuarios pertenecientes a dicho grupos, pulsando en el botón **Agregar** e introduciendo el nombre del usuario en cuestión.

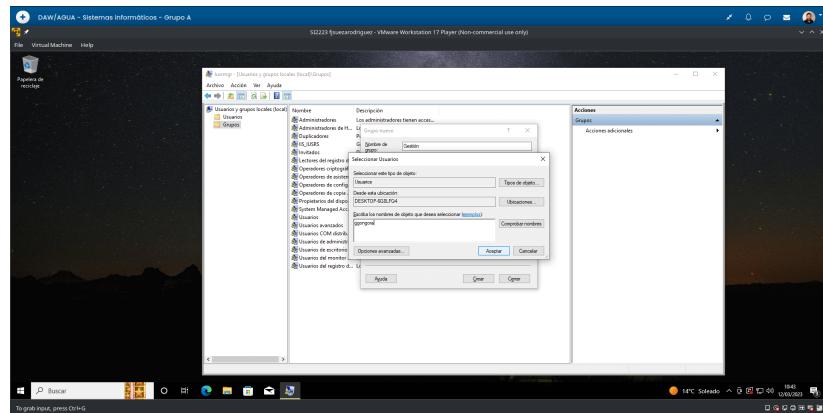


Figura 2.9: Agregación de un usuario al grupo

Una vez creados los dos grupos y agregados los usuarios que pertenecen a cada uno, estos han quedado como se puede ver en las siguientes dos capturas.

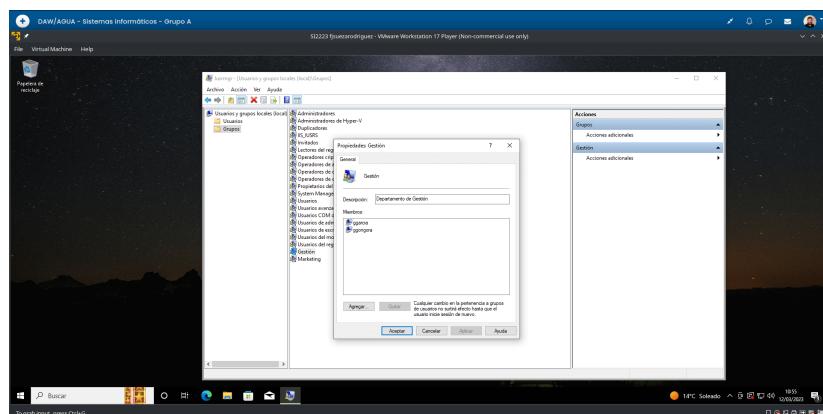


Figura 2.10: Grupo Gestión creado

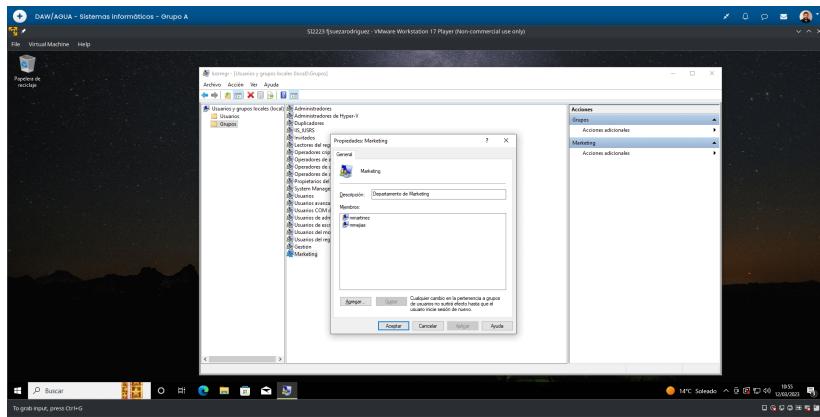


Figura 2.11: Grupo Marketing creado

2.3. Actividad 3: Permisos de Archivos y Carpetas

2.3.1. Enunciado

Configura los permisos de las carpetas creadas en la primera actividad, para que los usuarios creados en la segunda actividad, tengan permisos de lectura y escritura sobre la carpeta de su departamento. El resto de usuarios, aunque se cree posteriormente en el sistema, no tendrá ningún acceso si no pertenece a ese departamento. Los permisos se asignarán a los grupos que creaste en la actividad 2.b, no a los usuarios de manera individual.

A continuación, para comprobar que los permisos aplicados son correctos, inicia sesión con un usuario de un departamento, intenta acceder a la carpeta de su departamento y a la del otro departamento, e indica qué ocurre en cada caso. Realiza también la comprobación de acceder con el usuario creado en la instalación de Windows 10 a las carpetas de los departamentos.

Capturas:

- Ventana donde se asignan los permisos de la carpeta “Gestión” (indica textualmente cómo se accede a dicha ventana).
- Proceso de asignación de permisos a la carpeta “Gestión”. Deben mostrarse los nombres de los grupos implicados sus respectivos permisos.
- Resumen de la asignación de permisos a la carpeta “Marketing”. Deben mostrarse los nombres de los grupos implicados y sus respectivos permisos.
- Acceso de un usuario de un departamento a la carpeta de su departamento y a la del otro departamento.
- Acceso del usuario creado en la instalación de Windows 10 a las carpetas de los departamentos.

2.3.2. Solución

En esta actividad vamos a cambiar los permisos de las carpetas creadas en la Actividad 1 para que solo los usuarios pertenecientes a dichos departamentos puedan acceder a ellos y modificarlos. Para ello hemos realizado los siguientes pasos.

1. Primero hemos modificado los permisos del directorio **Gestión**. Para ello, nos hemos situado en su directorio padre, **AguadulSoft**, y hemos hecho click con el **botón derecho** sobre el directorio

y pulsado en la opción **Propiedades** del menú que se nos despliega. A continuación, hemos pulsado en la pestaña **Seguridad**.

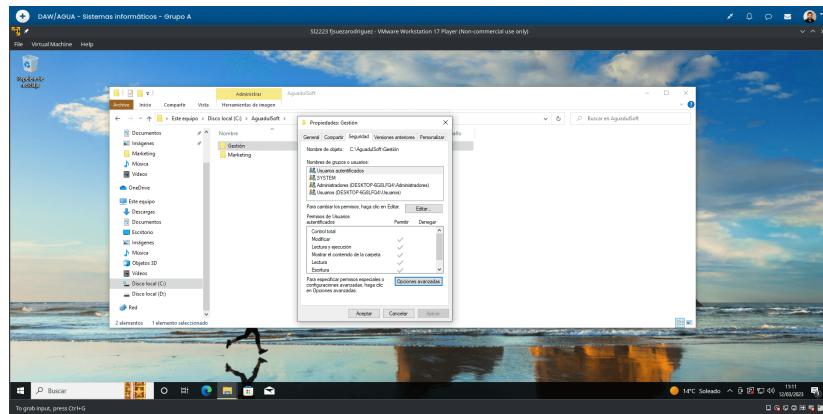


Figura 2.12: Ventana con permisos de la carpeta Gestión

Hay que tener en cuenta, que ahora mismo no podemos modificar estos permisos. Para ello deberemos modificar la opción de **herencia** en **Opciones avanzadas**, pulsando en el botón **Deshabilitar Herencia**. En la ventana que se nos muestra, deberemos elegir la opción para **Hacer los permisos heredados explícitos**, lo que nos permitirá modificar los permisos del directorio sin eliminar los que ya tiene, ya que hay ciertos grupos como **SYSTEM** o **Administradores** que nos interesa mantener dentro de los grupos que pueden modificar el directorio.

Una vez hecho esto, hemos vuelto a la ventana anterior y pulsado en la opción **Editar** para eliminar y añadir los grupos oportunos, como podemos ver en la siguiente captura.

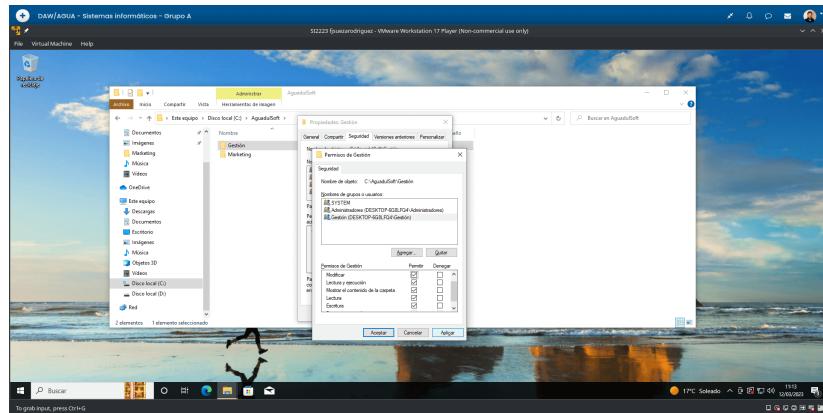


Figura 2.13: Modificación de los permisos de la carpeta Gestión

2. A continuación, hemos realizado el mismo procedimiento en la carpeta **Marketing**, quedando después de la modificación como vemos en la siguiente figura.

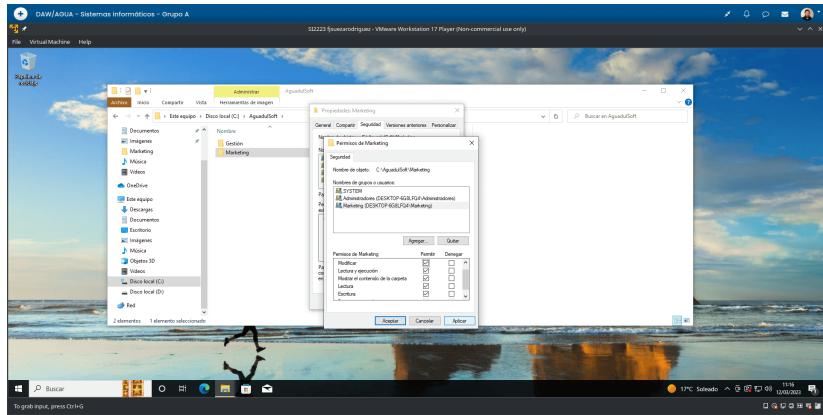


Figura 2.14: Modificación de los permisos de la carpeta Marketing

3. Por último, para **comprobar que los cambios se han realizado correctamente**, hemos intentado acceder a dichas carpetas con **usuarios que deberían tener permisos** y con **usuarios que no deberían** tenerlos. Hay que tener en cuenta que si el usuario que usamos tiene permisos de administrador se le va a poder habilitar en el directorio concreto, ya que los administrador han conservado sus permisos en dichos directorios.

Primero hemos intentado acceder a la **carpeta Gestión** con un **usuario** perteneciente al **grupo Gestión**, intentando, posteriormente, acceder con este usuario a la **carpeta Marketing**. Hemos elegido el usuario **ggongora**.

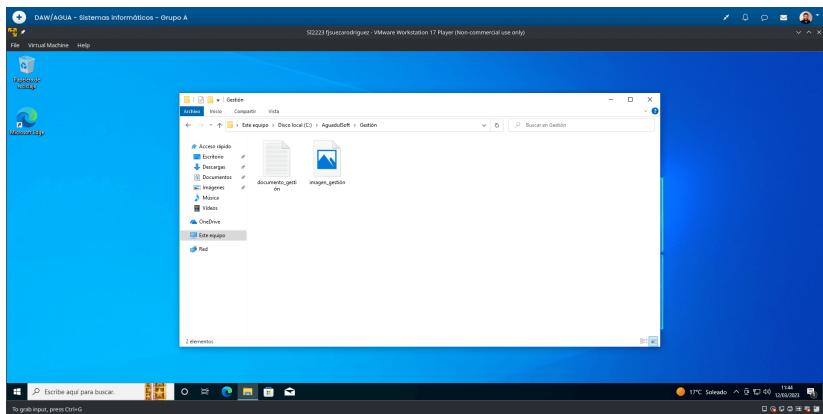


Figura 2.15: Acceso a la carpeta Gestión con la usuaria ggongora

En este caso, **no hemos tenido ningún problema** de acceder a la carpeta Gestión. Ahora vamos a intentar acceder a la carpeta **Marketing**.

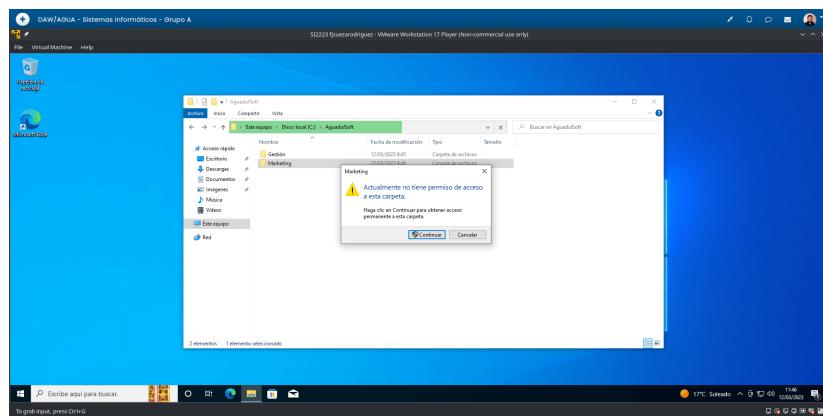


Figura 2.16: Acceso a la carpeta Marketing con la usuaria ggongora

Como vemos, se nos muestra una ventana informándonos de que no tenemos permisos. Como los administradores si los tienen, nos da la opción de agregarlos para tener permisos en esa carpeta, pero como *no sabemos la contraseña de administrador*, no podemos hacerlo. Por último, probamos a entrar en las carpetas con el **usuario creado** durante **la instalación** de Windows 10.

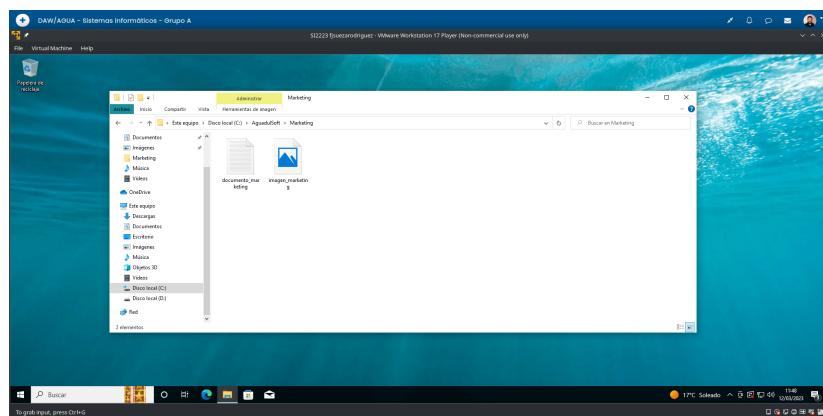


Figura 2.17: Acceso a las carpetas con el usuario creado en la instalación

Como este usuario **sí tiene permisos de administrador**, no tenemos problemas en acceder a ninguna de las carpetas.

2.4. Actividad 4: Directivas de Seguridad y Grupo Local

2.4.1. Enunciado

- Habilita las **directivas seguridad** de contraseñas correspondientes para que el sistema guarde el registro de las **5 últimas contraseñas** de usuario, requiera que sean **complejas**, tengan una vigencia máxima de **30 días** y una longitud mínima de **10 caracteres**. Establece también que se permitan hasta 3 equivocaciones de un usuario al iniciar sesión, y que en el caso de producirse la cuenta del usuario quede bloqueada durante **15 minutos**.

Capturas:

- Ventana donde se asignan las directivas de contraseñas y de bloqueo de cuenta (indica textualmente cómo se accede a dicha ventana).
- Proceso de asignación de las directivas de contraseñas exigidas.
- Resumen de asignación de las directivas de contraseñas aplicadas.
- Proceso de asignación de las directivas de bloqueo de cuenta exigidas.
- Resumen de asignación de las directivas de bloqueo de cuenta aplicadas.

b) **Directiva de grupo local:** Impide el acceso de los usuarios al símbolo del sistema editando la directiva correspondiente.

A continuación, para comprobar que se ha realizado correctamente, muestra qué ocurre cuando intentas acceder al símbolo del sistema.

Capturas:

- Ventana donde se asignan las directivas de grupo local (indica textualmente cómo se accede a dicha ventana).
- Proceso para impedir el acceso de los usuarios al símbolo del sistema.
- Intento de acceso al símbolo del sistema.

2.4.2. Solución

En este ejercicio vamos a configurar y modificar las directivas de seguridad en Windows 10, tanto las locales como las de grupos.

1. En primer lugar vamos a modificar las directivas de seguridad, en concreto, las **directivas de cuenta**, para añadir ciertas **restricciones** tanto a la **creación de contraseñas** como establecer ciertos parámetros para el **bloqueo de cuentas**.

Para acceder a la aplicación de **Directivas de seguridad local**, solo debemos buscar la aplicación por su nombre en la **búsqueda** de la barra de Windows 10, a la derecha del **Menú Inicio**. El primer resultado que nos arroja es dicha aplicación. Ya solo debemos pulsar en **Ejecutar como administrador** para iniciarla.

Una vez con la aplicación abierta, seleccionamos la carpeta **Directivas de Cuenta** y se nos mostrarán 2 subcarpetas, **Directiva de contraseña** y **Directiva de bloqueo de cuenta**, en las cuales podremos realizar los cambios que nos pide el enunciado.

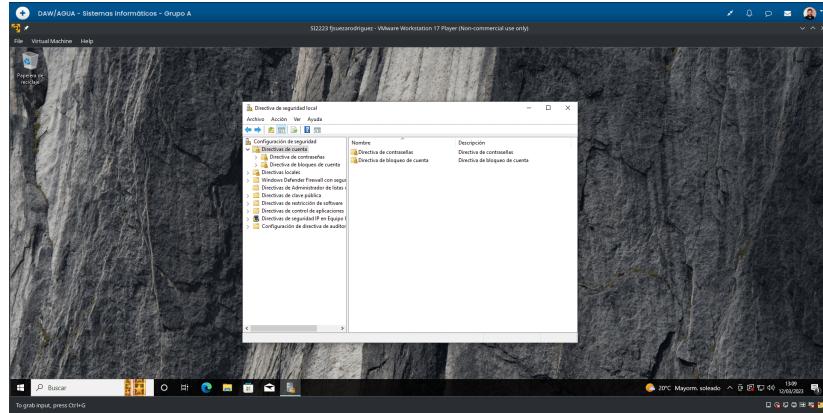


Figura 2.18: Ventana para el cambio de directivas de cuenta

Para cambiar las directivas respecto a las contraseñas, debemos pulsar en la opción **Directivas de contraseña**. Estos nos desplegará un conjunto de opciones que podremos ir cambiando.

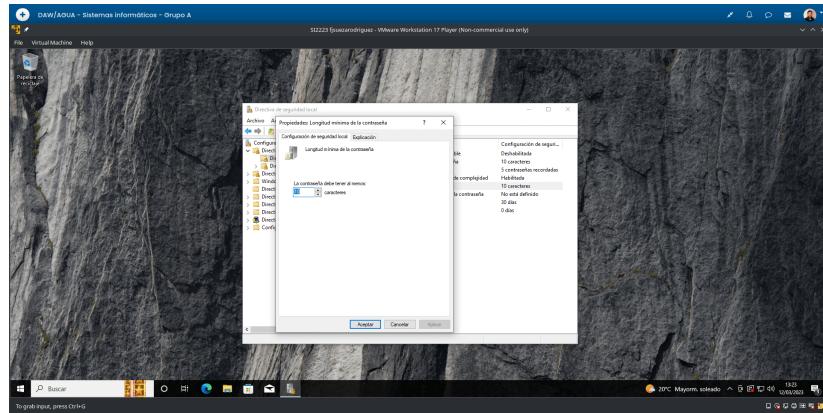


Figura 2.19: Cambio de la longitud de contraseña requerida

Tras realizar todas las modificaciones solicitadas, las directivas de contraseña quedan de la siguiente manera.

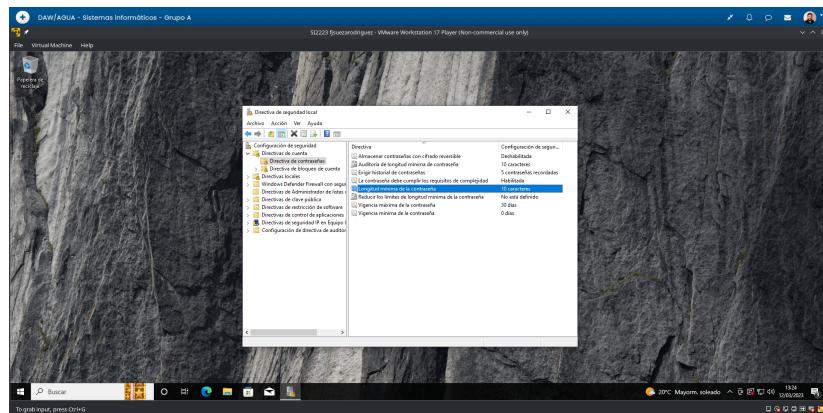


Figura 2.20: Resumen de las directivas de contraseña

A continuación, desde la carpeta de **Directivas de cuenta**, pulsamos sobre la opción **Directiva de bloqueo de cuenta**. Al igual que en la acción anterior, se nos mostrará un conjunto de opciones que podremos modificar, con una diferencia, y es que para que las opciones **Duración del bloqueo de cuenta** y **Restablecer bloqueo de cuentas después de** se nos habiliten, primero debemos establecer un número de intentos predeterminados con la opción **Umbral de bloqueo de cuenta**, como vemos en la siguiente figura.

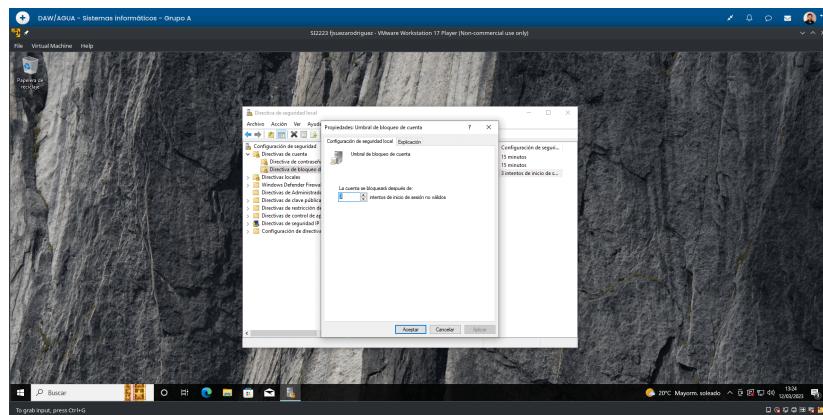


Figura 2.21: Cambio del umbral de bloqueo de cuenta

Una vez realizado esto, ya podremos cambiar las otras dos opciones, quedando las directivas de bloqueo de cuenta como podemos ver a continuación.

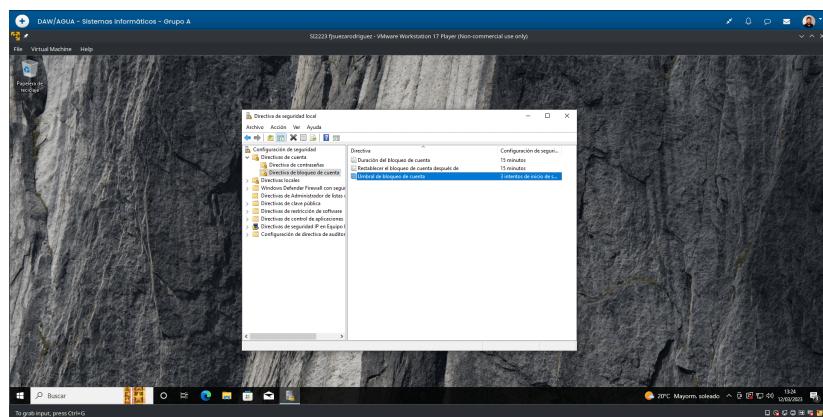


Figura 2.22: Resumen de la directivas de bloqueo de cuenta

2. Una vez cambiadas las directivas de cuentas, vamos a proceder a modificar las **Directivas de grupo local**, impidiendo el acceso al **símbolo del sistema** a los usuarios.

Para ello, hemos usado el comando **gpedit.msc**, introducido desde la consola. Eso nos abrirá la aplicación, que nos mostrará multitud de opciones para modificar las directivas locales, resaltando dos opciones principales: **Configuración de Equipo** y **Configuración de Usuario**. Esta última es la que nos interesa a nosotros, como veremos en el siguiente paso.

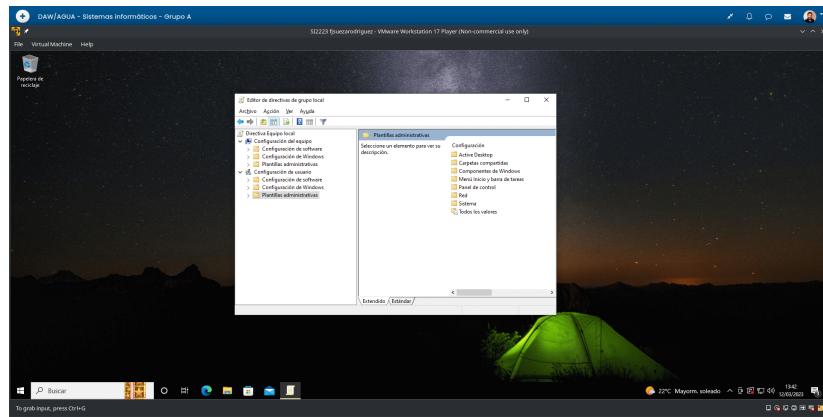


Figura 2.23: Ventana de la aplicación gpedit para modificar la directivas de grupo local

Una vez abierta la aplicación, debemos buscar la opción para **impedir el acceso de los usuarios al símbolo de sistema**. Para llegar a esta opción debemos pulsar en **Configuración de Usuario —>Plantillas Administrativas —>Sistema**. Aquí, si nos fijamos en la parte derecha de la ventana, nos saldrán un conjunto de carpetas y directivas que configurar, entre las que podemos encontrar **Impedir el acceso al símbolo del sistema**. Debemos pulsar en esta opción, lo que nos abrirá una ventana con una explicación sobre el funcionamiento de esta directiva y como cambiarla.

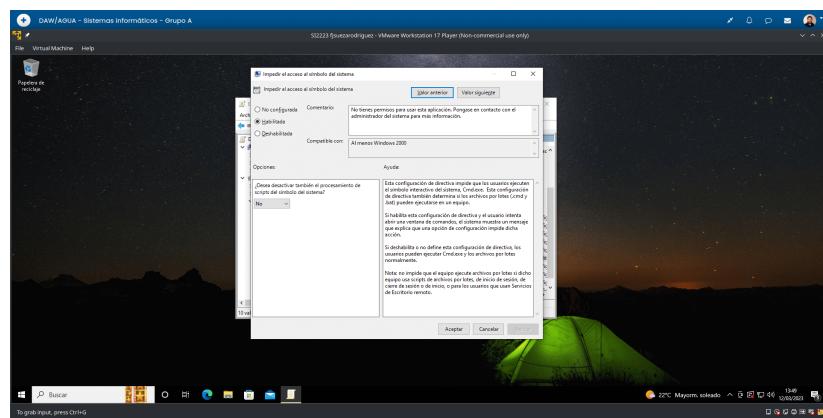


Figura 2.24: Directiva para impedir el acceso al símbolo del sistema

Una vez cambiada, no se podrá acceder al símbolo del sistema, ni siquiera, teniendo permisos de administrador, como vemos en la siguiente captura.

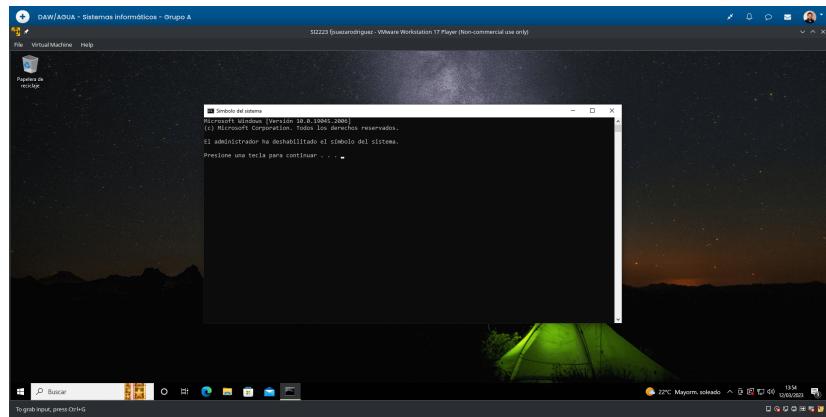


Figura 2.25: Intento de acceso al símbolo del sistema

2.5. Windows Defender: Programar Análisis

2.5.1. Enunciado

Si tienes instalado un software antivirus en tu MV, activa la ejecución periódica de Windows Defender.

Si no tienes ningún antivirus de terceros instalado, accede a “Protección Antivirus y contra amenazas” y asegúrate de que tienes todas las protecciones habilitadas (en tiempo real, en la nube, envío de muestras automático, contra alteraciones, ...). Esta protección no ralentiza mucho el sistema y puede ser suficiente para evitar software indeseado, aunque debes mantener siempre actualizado el sistema con las updates de seguridad.

Accede a la Biblioteca del Programador de Tareas, y en la carpeta Microsoft\Windows\Windows Defender, modifica la tarea que realiza el análisis “Windows Defender Scheduled Scan” para que no se ejecute en una hora programada, sino cuando se registre un evento de categoría “Registros de Windows” (subcategorías “Aplicación”, “Seguridad”, “Instalación”, “Sistema” y “Eventos reenviados”), de nivel crítico o de error, y además haya ocurrido en la última hora. Para todo esto debes crear un filtro de eventos personalizado.

Capturas:

- Ventana de configuración donde se verifica que todas las protecciones están activas, o que se permite examen periódico de Windows Defender (en caso de tener un antivirus externo).
- Abre la tarea modificada y muestra la pestaña “Desencadenadores” con el máximo nivel de detalle (indica textualmente cómo realizas el acceso).
- Muestra el filtro personalizado en formato XML.

2.5.2. Solución

En este ejercicio vamos a realizar la configuración de **Windows Defender** para que realice exámenes de forma periódica, así como a comprobar que todas las protecciones están habilitadas.

1. En primer lugar, hemos comprobado que tenemos todas las protecciones activadas. Lo cual podemos hacer en **Protección antivirus y contra amenazas**. Como podemos ver en la siguiente captura, todas las protecciones están activadas correctamente.

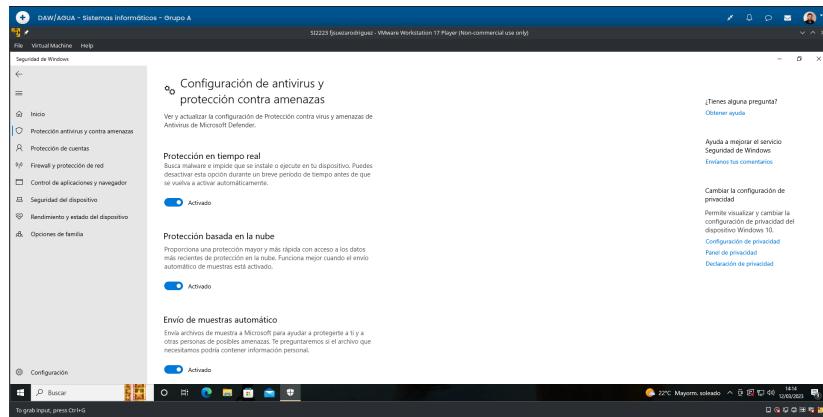


Figura 2.26: Protección antivirus y otras amenazas

- Una vez hemos comprobado que tenemos todas las protecciones activas, vamos a modificar la tarea de sistema que se encarga de ejecutar Windows Defender.

Para ello, en primer lugar, abrimos la aplicación **Programador de tareas**, buscando la barra de búsqueda del sistema. Una vez abierta la aplicación, la opción de Windows defender se encuentra en la ruta de carpetas **Biblioteca del programador de tareas —>Windows —>Windows Defender**.

Una vez abierta esta carpeta, se nos mostrarán las diferentes tareas vinculadas a Windows Defender, aunque a nosotros la que nos interesa es **Windows Defender Schedule Scan**. Pulsamos con el botón derecho sobre esta tarea y seleccionamos la opción **Propiedades**.

Se nos abrirá una ventana con las propiedades de la tarea. Nosotros, vamos a pulsar sobre la pestaña **Desencadenadores** y a añadir uno nuevo, pulsando en el botón **Nuevo**. En la ventana que se nos abre, deberemos seleccionar la opción **Al producirse un evento** en el menú desplegable **Iniciar tarea**, y posteriormente marcar la opción **Personalizada** en el recuadro inferior, lo que nos mostrará el botón de **Nuevo filtro de evento...**, el cual vamos a pulsar.

En esta nueva ventana, en primer lugar vamos a seleccionar la opción **Última hora** en el menú desplegable **Registrado**. A continuación marcamos **Criticó** y **Error** en las opciones de **Nivel de evento**. Por último seleccionamos la opción **Registros de Windows**, en el menú desplegable **Registro de eventos**. Eso no seleccionará automáticamente todos los eventos de los registros de Windows.

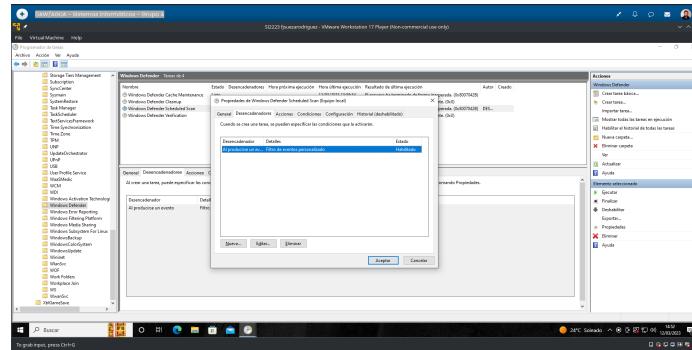


Figura 2.27: Desencadenador creado para la tarea de Windows Defender

Una vez modificada la tarea y creado el nuevo filtro, mostramos la salida en XML del nuevo filtro de evento creado.

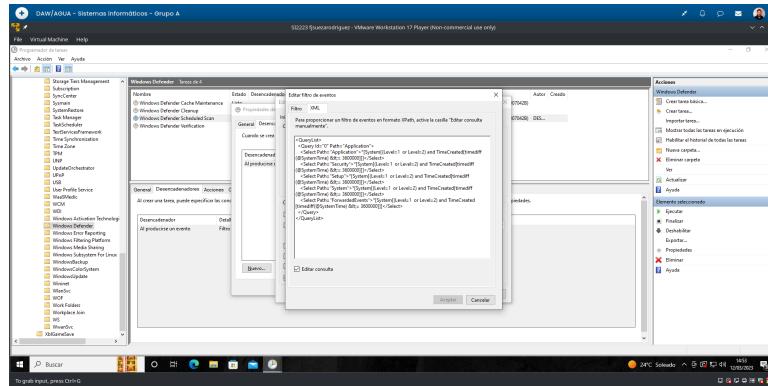


Figura 2.28: Filtro de evento creado en formato XML

2.6. Actividad 6: Windows Update

2.6.1. Enunciado

Realiza una captura de **Windows Update** que muestre si el sistema está actualizado, con la fecha y hora en la que se realizó la última comprobación. Establece también el horario de **8:00 a 16:00 horas** como horas activas del equipo y que se muestre una notificación cuando el equipo requiera un reinicio para finalizar una actualización.

Capturas:

- Ventana de Windows Update (indica textualmente cómo se accede a dicha ventana).
- Información sobre el estado actual del sistema y última actualización.
- Introducción de las horas activas del equipo.
- Activación de la notificación cuando el equipo requiera un reinicio para finalizar una actualización.

2.6.2. Solución

Ahora vamos a trabajar con **Windows Update**, el gestor de actualizaciones de Windows.

1. En primer lugar vamos a acceder a la ventana de Windows Update. Esto podemos hacerlo buscando en la barra de búsqueda del sistema el término **Windows Update** y pulsando en el primer resultado **Buscar Actualizaciones**, aunque también lo podemos hacer desde la opción **Actualización y seguridad** del menú **Configuración**. En la siguiente captura podemos ver la ventana principal de Windows Update.

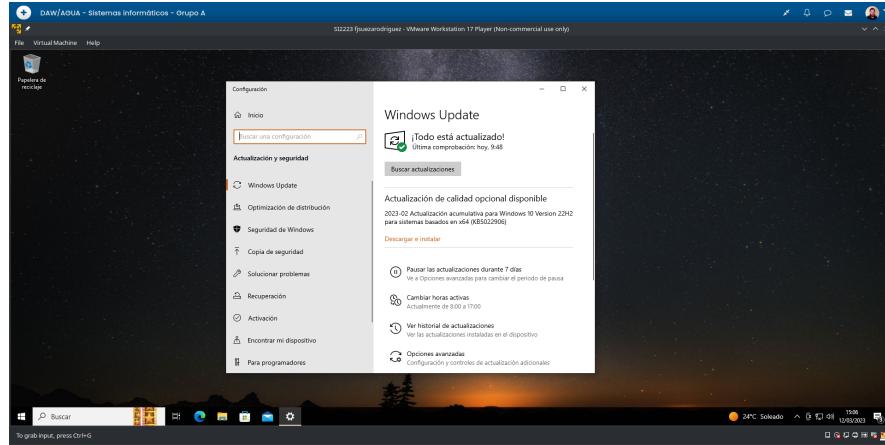


Figura 2.29: Ventana principal de Windows Update

- Para verificar que el sistema esta actualizado, podemos mirar a la parte superior de la captura anterior. Donde podemos observar que el sistema **esta actualizado** y que la última comprobación se realizo **hoy a las 9:48**. Vemos también que hay una actualización pendiente, aunque esta es una **actualización opcional**.

NOTA: no se incluye captura en este punto ya que es la misma que en el punto 1.

- A continuación, vamos a cambiar el **rango horario** en el que se va a ejecutar Windows Update. Para ello, en la ventana anterior pulsamos en el apartado **Cambiar horas activas**, donde se nos dará la opción de cambiar el rango horario, como vemos en la siguiente figura.

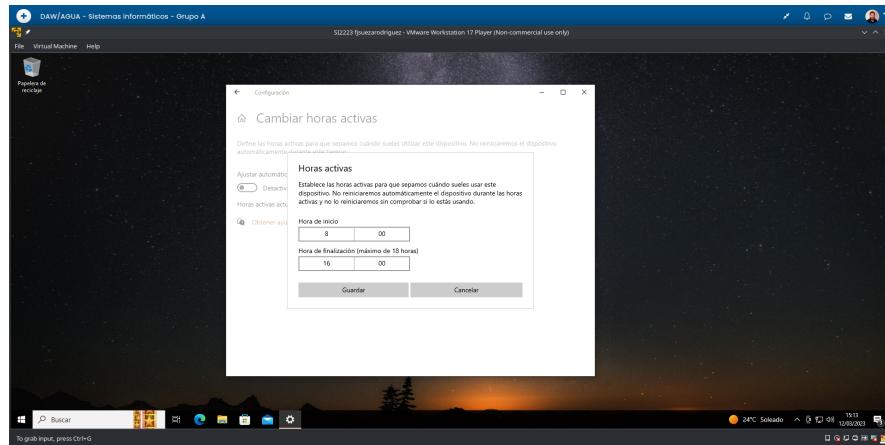


Figura 2.30: Cambio de rango horario para la ejecución de Windows Update

- Por último, vamos a activar la **Notificación de Actualización**, para que nos notifique cada vez que el sistema necesita reiniciarse para realizar una actualización. Esta opción la encontramos en el apartado **Opciones avanzadas**, donde podemos activarla.

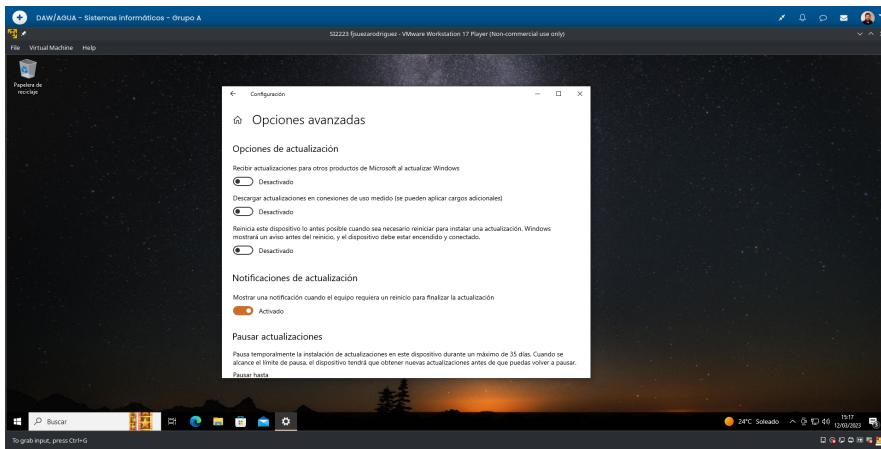


Figura 2.31: Activación de notificaciones de Windows Update

2.7. Actividad 7: Monitor de Rendimiento

2.7.1. Enunciado

Antes de empezar debes consultar la sección “**Conocimiento Previo**” (al final de esta página).

La actividad consiste en crear un nuevo conjunto recolector de datos dentro del Monitor de rendimiento, que tendrá como nombre recolector_InicialNombreApellidos. Usa la plantilla de creación “System Diagnostics” con la que se recogerán todas las estadísticas de rendimiento posibles. Establece como usuario del recolector el usuario creado al instalar el sistema (con permisos de Administrador).

Inicia manualmente el conjunto recolector recién creado y detenlo después de 1 minuto.

Para la 2^a ejecución del recolector deberás realizar una prueba de estrés al sistema (abre varias instancias del navegador, descarga un comprimidor de archivos tipo WinRAR o 7-zip, comprime/descomprime carpetas con bastante volumen, reproduce videos 4k, descarga videos pesados y usa un reproductor para visualizarlos, abre tantos programas como puedas, ...).

Comenta las diferencias que encuentras en los 2 informes generados en cada ejecución: ¿Qué contadores del sistema se han visto más afectados al estresar el equipo? Relaciona contadores con la carga de trabajos realizada. ¿Hay algún cuello de botella crítico en la configuración actual de tu máquina virtual que podrías modificar? Valora posibles soluciones.

Capturas:

- Ventana donde se muestra el Monitor de rendimiento con el colector creado ejecutándose.
- Ventanas donde se muestren cada uno de los informes resultado, teniendo desplegados los epígrafes “Rendimiento” y “Advertencias” (si las hubiera).

2.7.2. Solución

En esta actividad vamos a analizar el rendimiento del sistema usando el **Monitor del Sistema**, para lo que vamos a crear un nuevo recolector de datos y realizar 2 análisis, uno con el sistema en reposo y otro estresándolo.

- En primer lugar hemos creado el recolector de datos, llamado **recolector_fjsuezarodriguez** y usando la plantilla **System Diagnostics**. En la siguiente captura, podemos ver el recolector creado ejecutándose.

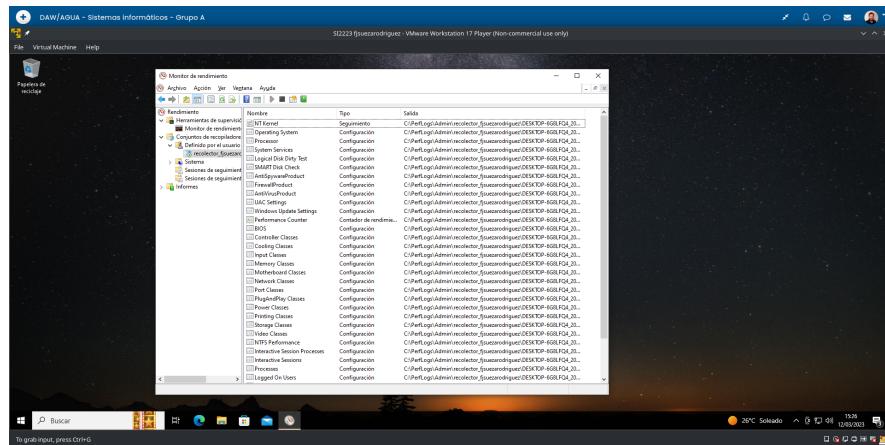


Figura 2.32: Recolector de datos creado en ejecución

- Una vez realizados los dos análisis, podemos ver los resultados.

En el **primer análisis**, los resultados han sido satisfactorios en tema de **rendimiento**, aunque el sistema nos ha lanzado varias advertencias, a modo de información sobre la **evaluación baja** de la **CPU**, los **gráficos** y el **disco duro**. También se nos informa de que la memoria RAM es **muy insuficiente**.

Esto es debido a las propias limitaciones del **Host**, ya que solo la MV tiene asignados solo **2 GB de RAM** y esta usando **2 núcleos**, de los 4 que tiene el sistema Host. Además, la gráfica es una Vega 8 integrada, que no es la mejor para utilizarla en juegos. En la siguiente captura, podemos ver el resultado del análisis.

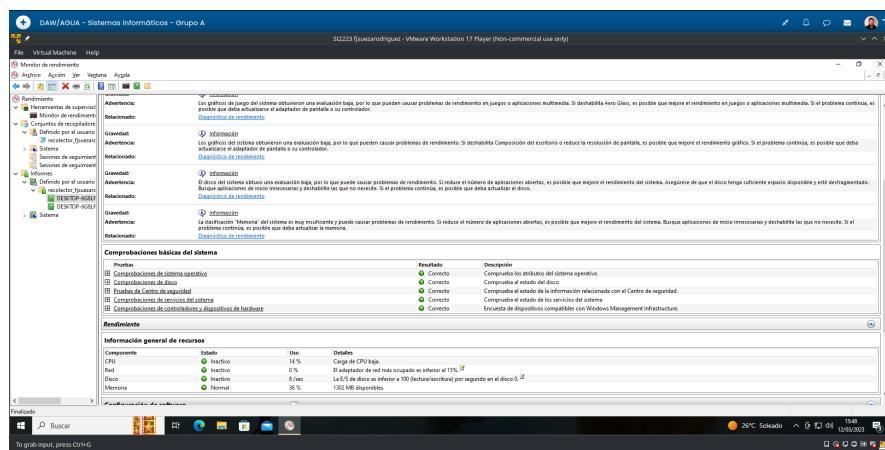


Figura 2.33: Informe del primer análisis de rendimiento

- Tras el primer análisis, hemos realizado un segundo intentando estresar el sistema, para lo que hemos abierto varias aplicaciones, varias pestañas en Edge, etc... El **resultado es muy similar**,

salvo que en este segundo análisis la **CPU** ha salido con una carga muy elevada, en concreto del **90 %**, como vemos en la siguiente captura.

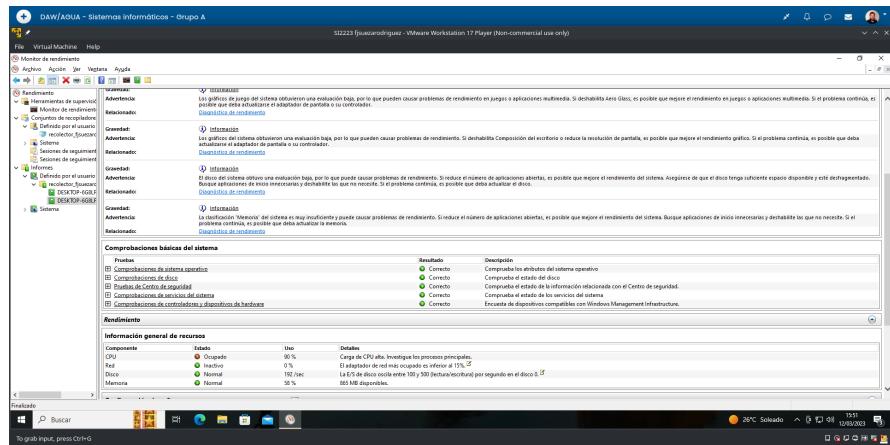


Figura 2.34: Informe del segundo análisis de rendimiento

Por último, **comentar los análisis**, aunque como ya hemos dicho estas advertencias se deben a las **limitaciones de host**, por lo que la única solución sería, o bien **actualizar el hardware** del sistema anfitrión, o intentar **asignar más recursos** a la máquina virtual a ver si así se soluciona alguno de los problemas de **performance**.

2.8. Actividad 8: Servicios

2.8.1. Enunciado

Inicia el servicio “**Cliente web**” y detiene el servicio “**Audio de Windows**” (una vez hecha la captura solicitada, vuelve a iniciar el servicio).

Capturas:

- Ventana donde se muestran los servicios (indica textualmente cómo se accede a dicha ventana).
- Activación/Inicio del servicio “Cliente web”.
- Captura donde se vea el icono de volumen en rojo en la barra de estado, indicando que el servicio “Audio de Windows” no está activo.

2.8.2. Solución

En esta actividad vamos a gestionar los **servicios locales** de Windows 10. En concreto, vamos a **habilitar el cliente web** y vamos a **deshabilitar** el servicio **audio de windows**.

1. En primer lugar tenemos que abrir el gestor de servicios. Si buscamos en la barra de búsqueda de Windows el término **servicios** nos aparecerá como el primer resultado. Pulsando en éste, se nos abrirá el **gestos de servicios**.

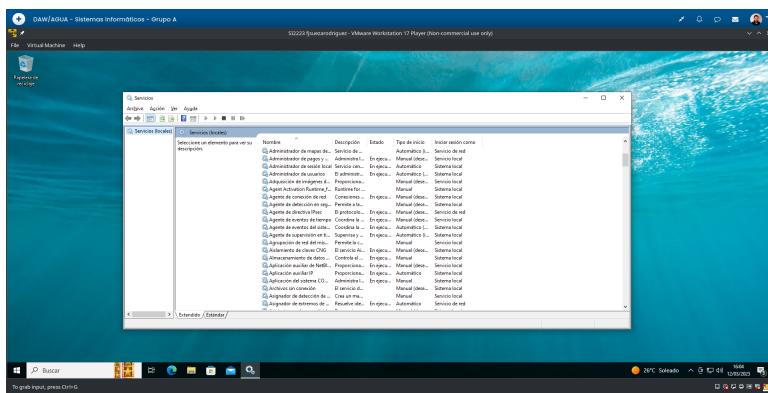


Figura 2.35: Gestor de servicios de Windows 10

2. A continuación, vamos a activar el servicio **Cliente Web**. Para ello, buscamos el servicio en la lista y a continuación en **Iniciar** en la ventana que se nos abrirá.

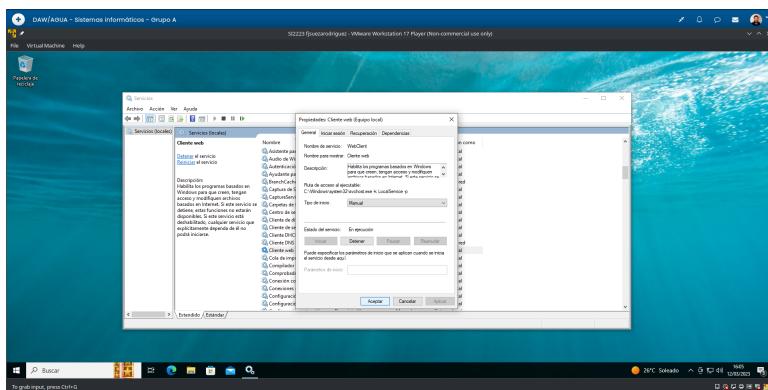


Figura 2.36: Inicialización del Cliente Web

3. Por último, vamos a deshabilitar el servicio **Audio de Windows**. Para ello, al igual que en el punto anterior, buscamos el nombre del servicio en la lista, solo que ahora pulsaremos en la opción **Detener**. En la siguiente captura, se muestra como el ícono de volumen aparece en rojo.

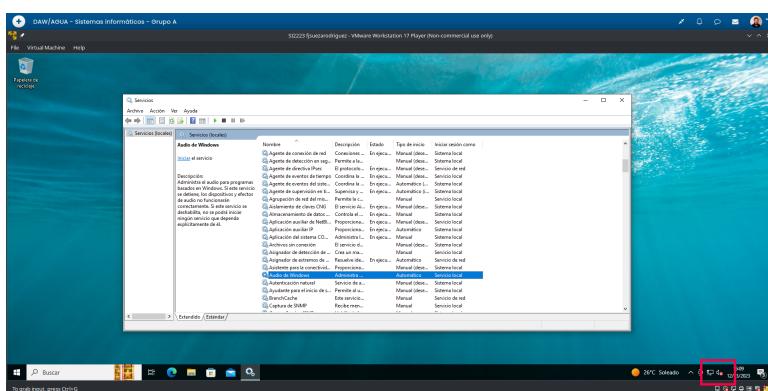


Figura 2.37: Audio de Windows deshabilitado

2.9. Actividad 9: Puntos de Restauración

2.9.1. Enunciado

Los puntos de restauración sirven para volver a configuraciones guardadas del sistema previas a alguna modificación o instalación de programas.

Crea un punto de restauración con el nombre SI2223InicialesApellido1Apellido2 (por ejemplo, para “José Luis Pérez Puertas” sería “SI2223 jlpperezpuertas”). Después cambia el tema de Windows por otro que sea lo más distinto posible al que tenías. A continuación restaura el sistema y comprueba que el cambio de tema realizado ha quedado sin efecto.

Capturas:

- Ventana donde se crea un punto de restauración y se aprecie la hora del sistema (indica textualmente cómo se accede a dicha ventana).
- Ventana con el nuevo tema configurado y se aprecie la hora.
- Ventana después de la restauración en la que se aprecie la hora y el tema previo.

2.9.2. Solución

En este ejercicio vamos a establecer un **punto de restauración** del sistema, lo que nos permitirá volver a un configuración anterior en caso de que el sistema operativo sufra algún fallo.

1. En primer lugar, vamos a abrir la aplicación para establecer un punto de restauración. Nosotros hemos accedido buscando el término **punto de restauración** en la **barra de búsqueda** y pulsando en el primer resultado, **Crear punto de restauración**, ya que esto nos lleva directamente a la pestaña **Protección del sistema**, donde podemos crearlo. Aunque también podemos acceder desde **Panel de Control —> Sistema y Seguridad —> Sistema**.

En esta ventana, primero, deberemos seleccionar la unidad sobre la que queremos crear el punto de restauración, pulsar en **Configurar**, y activar la protección del sistema. De otro modo, no nos permitirá crear un punto de restauración. Una vez hecho esto, pulsamos en crear para crear un nuevo punto de restauración e introducimos el nombre que queramos.

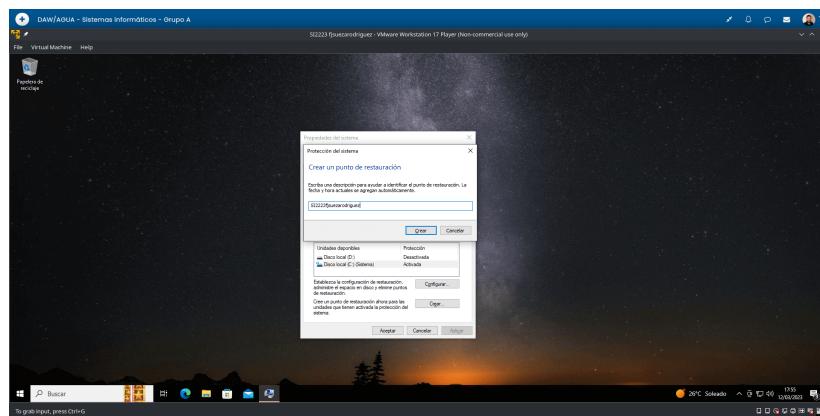


Figura 2.38: Creación de un punto de restauración

2. A continuación hemos cambiado el tema de escritorio a Windows (claro), como se puede ver en la siguiente imagen.

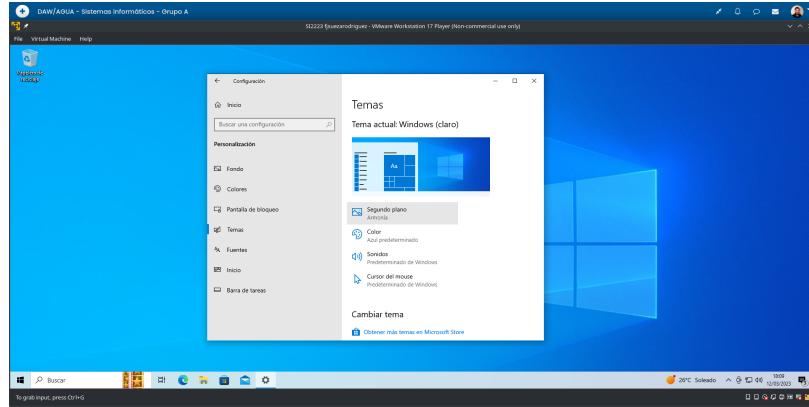


Figura 2.39: Tema cambiado a Windows(claro)

3. Por último, hemos realizado la restauración del sistema, volviendo a los valores que teníamos en el momento que se creó el punto de restauración, incluyendo el tema de escritorio.

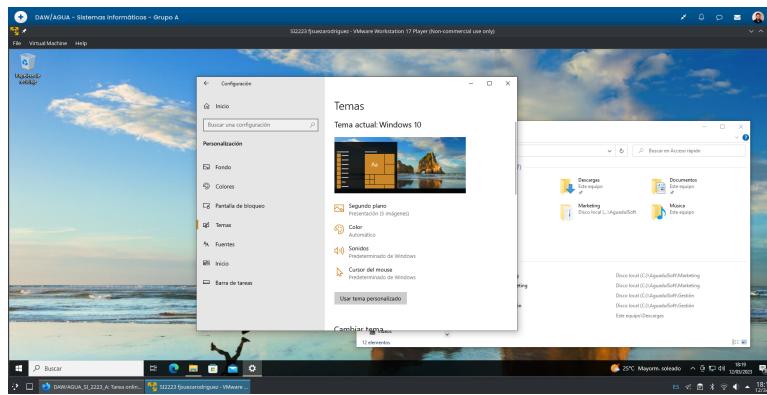


Figura 2.40: Sistema Restaurado

2.10. Actividad 10: Copia de Seguridad

2.10.1. Enunciado

Para poder realizar copias de seguridad de los archivos necesitas un disco distinto al de la partición donde se aloja Windows. Debes crear un nuevo disco virtual, siempre con la MV apagada. Añade un nuevo disco duro al conector sata desde la configuración de Almacenamiento y asígnale unos 10 GB con reserva dinámica de espacio.

Cuando inicies la MV el sistema aún no reconocerá el disco (hay que montarlo), tienes que usar la herramienta de administración de discos y crear un volumen simple con el nuevo disco creado y darle formato NTFS. A partir de aquí nuestro sistema ya sí reconocerá el nuevo disco.

Abre **Copia de Seguridad** para añadir la nueva unidad creada. Configura la copia de seguridad para que además de todas las carpetas asociadas al usuario logueado, incluya en el backup la carpeta **C:\AguadulSoft** de la actividad 1.

La copia de seguridad se realizará cada **3 horas**, y se mantendrán los archivos durante **1 año**.

Capturas:

- Ventana del Administrador de discos donde se crea el nuevo volumen.
- Ventana donde se aprecian las opciones de la Copia de Seguridad, como periodicidad y permanencia de la copia.

2.10.2. Solución

Como última actividad de esta tarea, vamos a establecer una política de creación de copias de seguridad.

1. En primer lugar, hemos usado el **gestor de volúmenes** para añadir la unidad que hemos creado previamente, una **unidad de disco duro** de tipo **SATA** con un tamaño de 10 GB. En la siguiente imagen podemos ver la unidad, a la que le hemos asignado la **letra F** y hemos llamado **backup**, correctamente formateada en el **gestor de discos**.

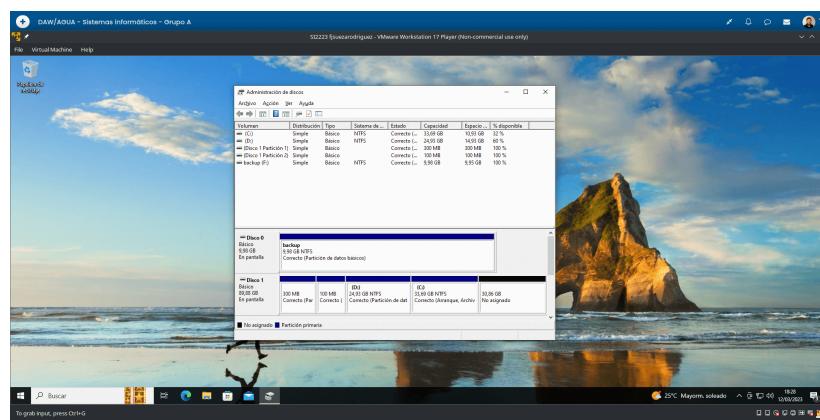


Figura 2.41: Nueva unidad formateada en el gestor de discos

2. A continuación hemos creado la política de copia de seguridad con los parámetros que se nos han indicado. Esto es, realizado una copia de seguridad cada **3 horas**, con una permanencia de **1 año** y añadiendo la carpeta **C:\AguadulSoft**. En la siguiente imagen se puede ver la configuración final de las copias de seguridad.

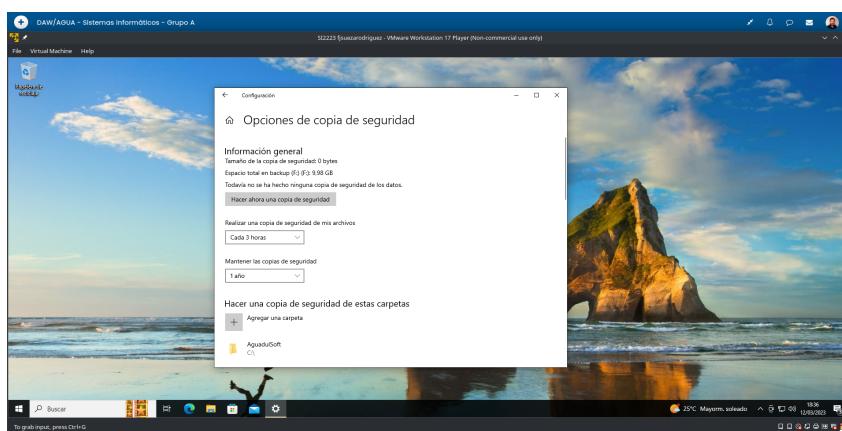


Figura 2.42: Configuración de copias de seguridad