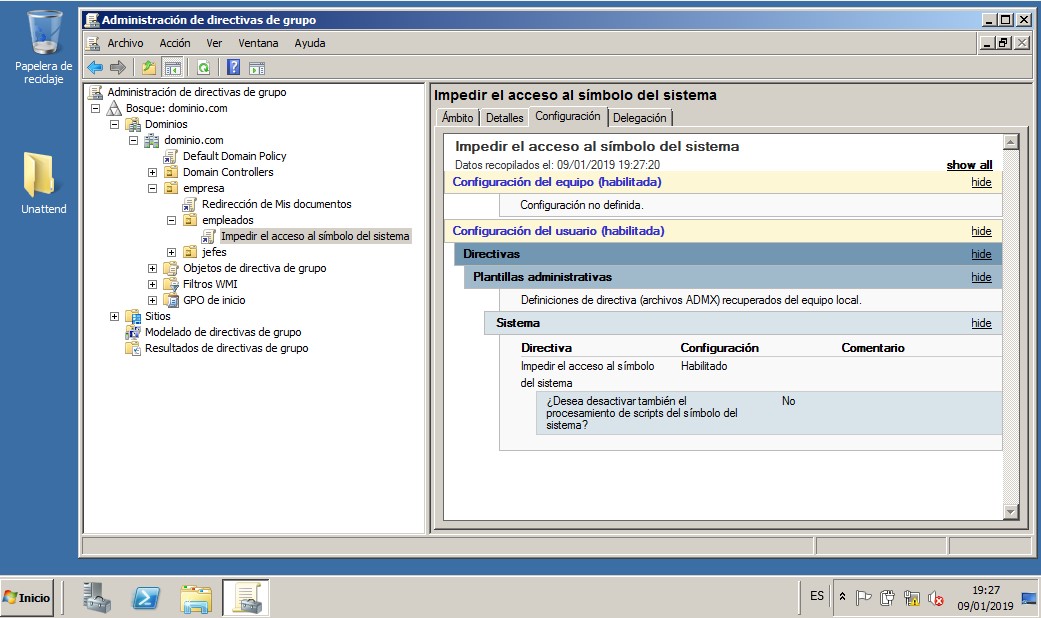
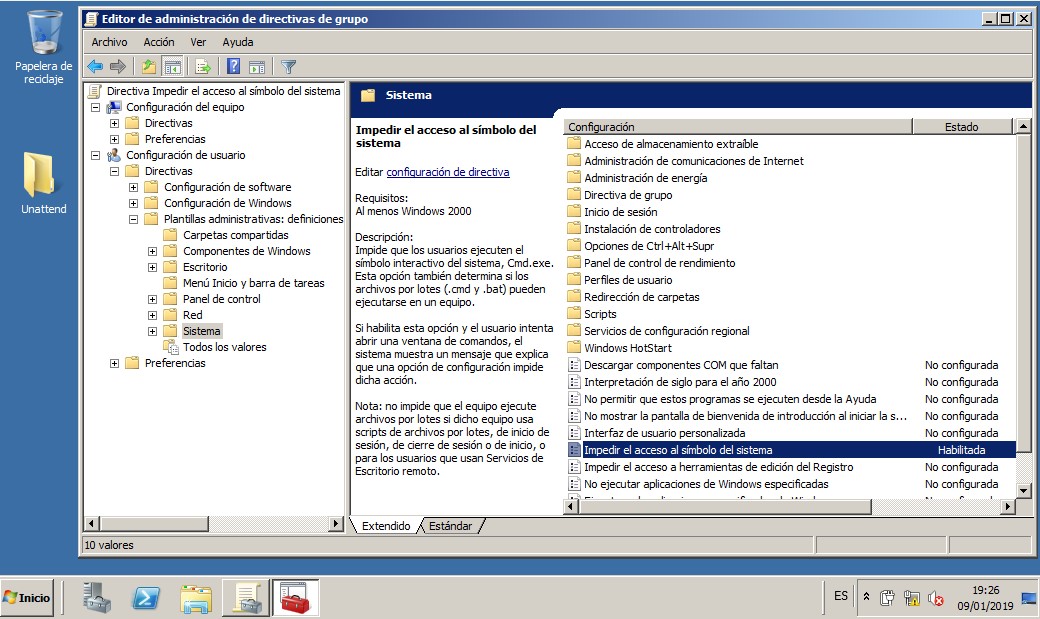
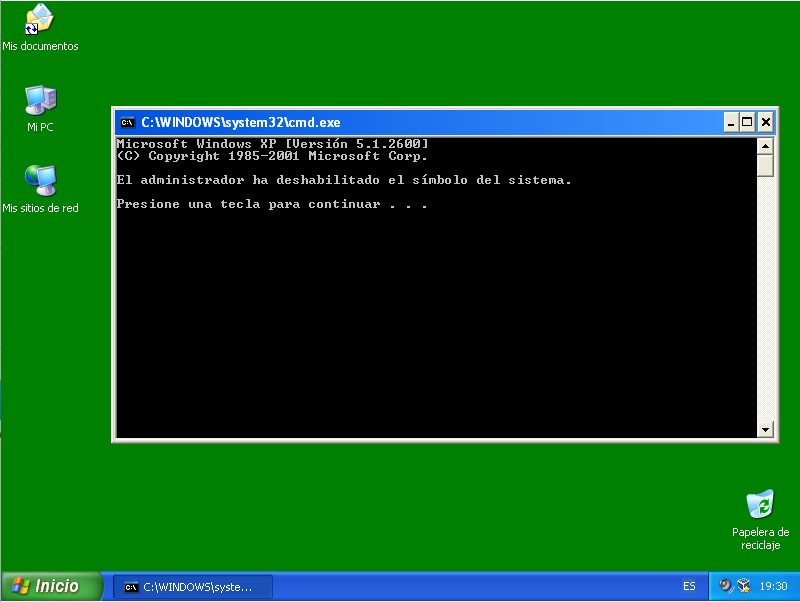
Administración de políticas de grupo (GPO) (I)

Podemos modular cómo queremos que se comporten nuestros usuarios en el dominio o cómo funcionen los equipos del mismo. A continuación te presento algunas políticas de grupo (en adelante GPO) que le harán la vida un poco más difícil a nuestros usuarios ...

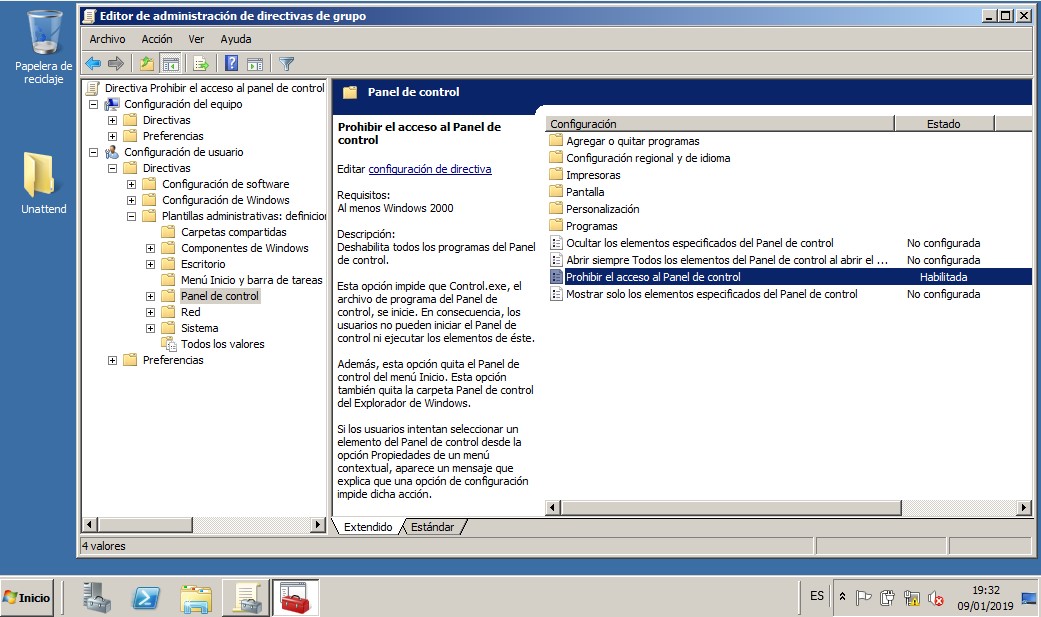
En esta primera GPO se puede ver cuál es su ruta y cómo queda configurada. Cuando se aplica se impide el acceso a una **ventada de comandos** por parte de los usuarios afectados.



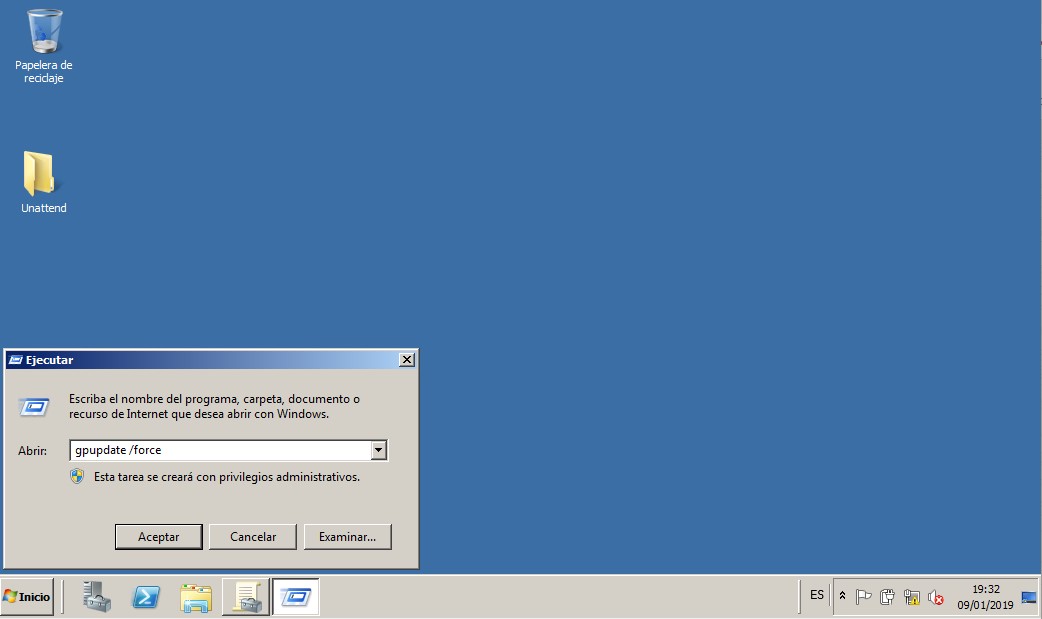
Cuando el usuario ejecuta (**Inicio>Ejecutar ... [cmd]**) le aparece la siguiente ventana, informándole que no tiene acceso a esta herramienta:



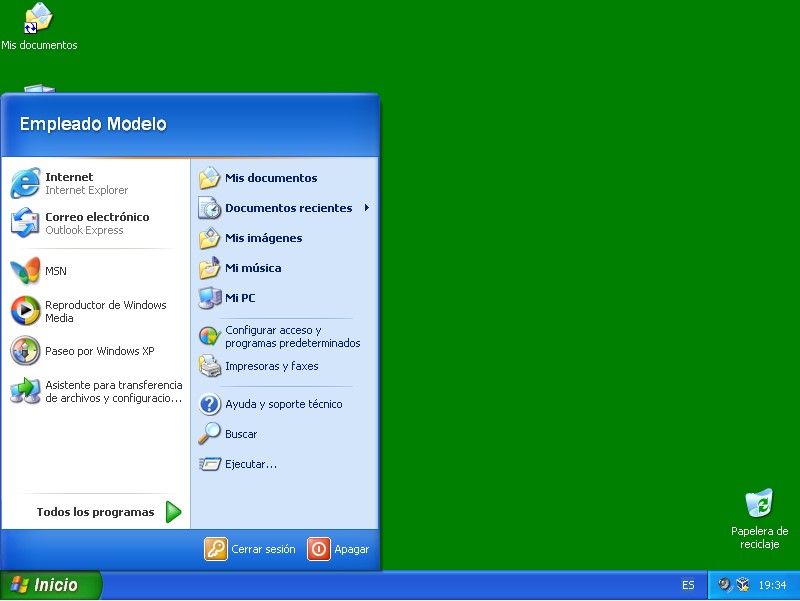
Con la siguiente GPO impediremos el **acceso al panel de control** por parte de los usuarios.



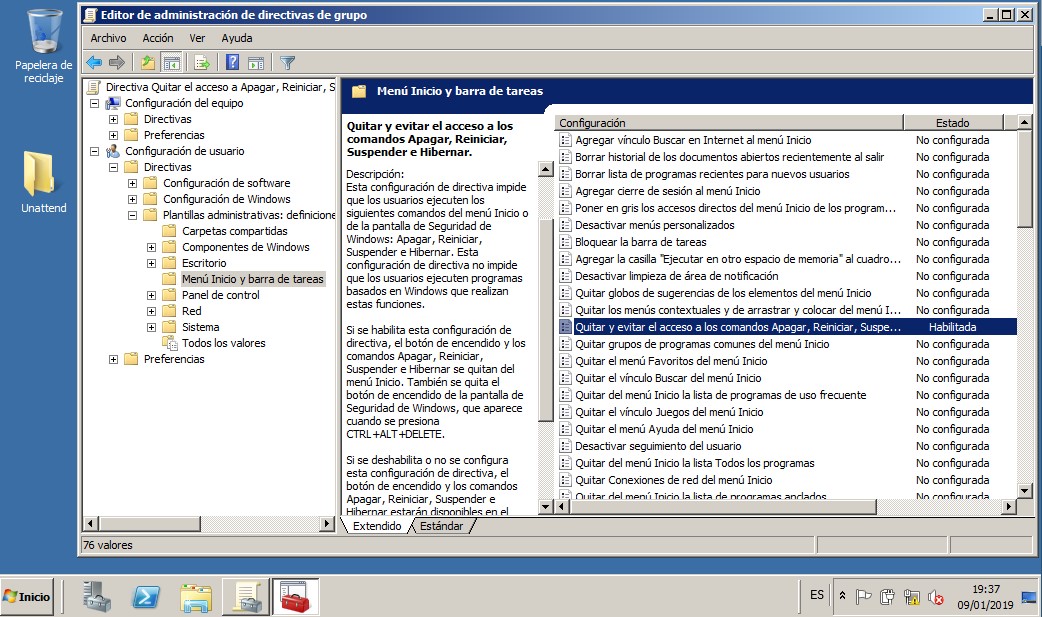
La propagación de políticas de grupo en un dominio conlleva un tiempo considerable. Es recomendable a veces "forzar" esa actualización de directivas, bien desde el controlador de dominio (la mayoría de las ocasiones), bien desde los clientes. Para ello, escribimos "**gpupdate /force**".



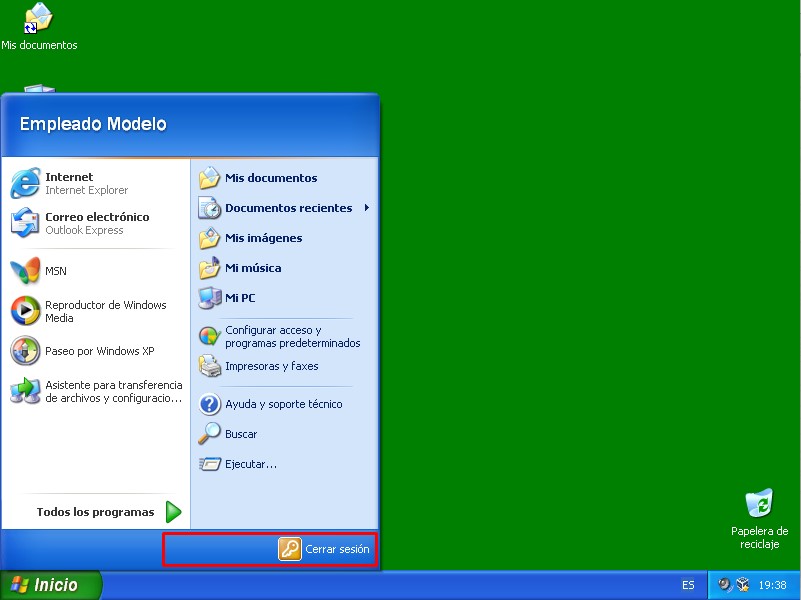
Volviendo a la GPO que impedía el acceso al panel de control, cuando los usuarios inician sesión, el icono ha desaparecido.



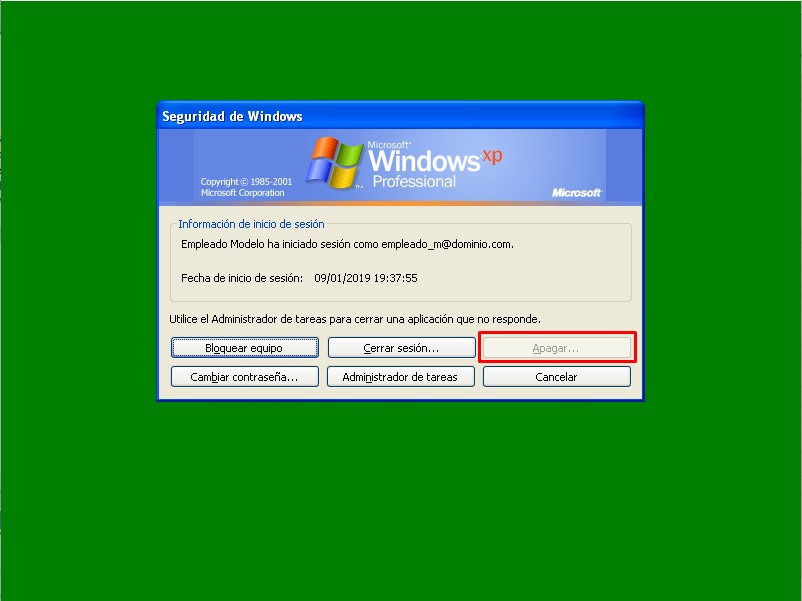
La GPO que figura a continuación tiene como objetivo **quitar los iconos de Apagar, Reiniciar y Suspender**, así como el acceso a estas funciones cuando se pulsa la combinación de teclas **CTRL+ALT+SUPR**.



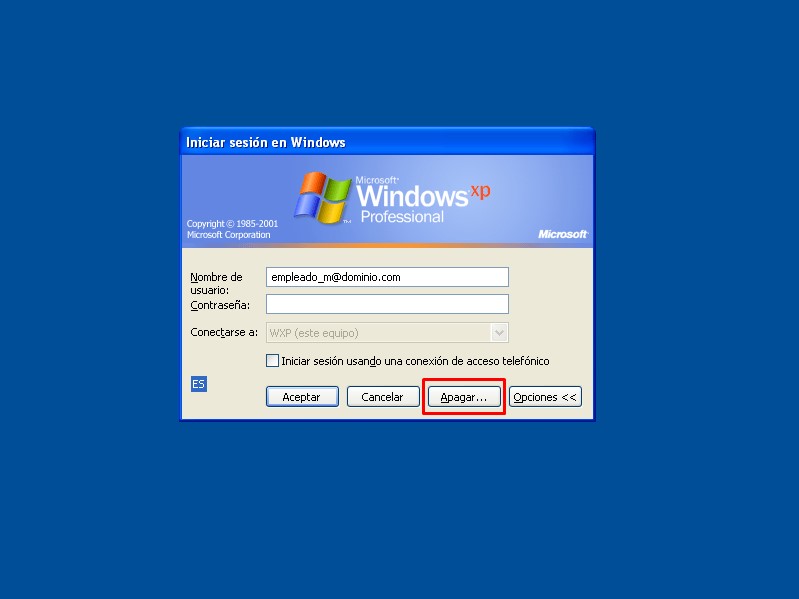
Como se puede comprobar, han desaparecido estos iconos.



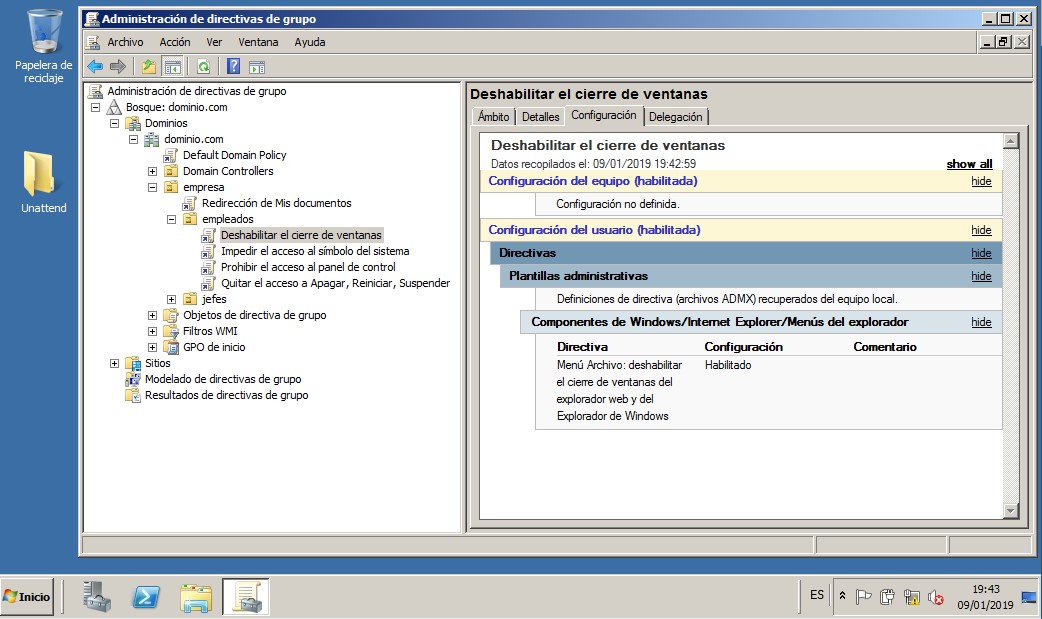
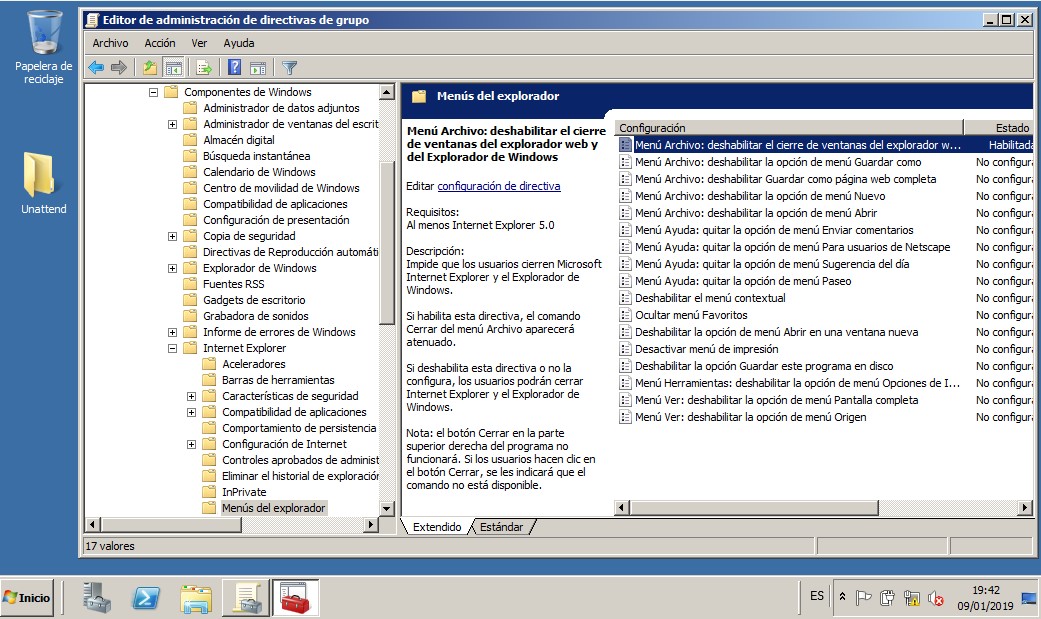
Cuando se pulsa la combinación de teclas **CTRL+ALT+SUPR** está inhabilitada esa opción.



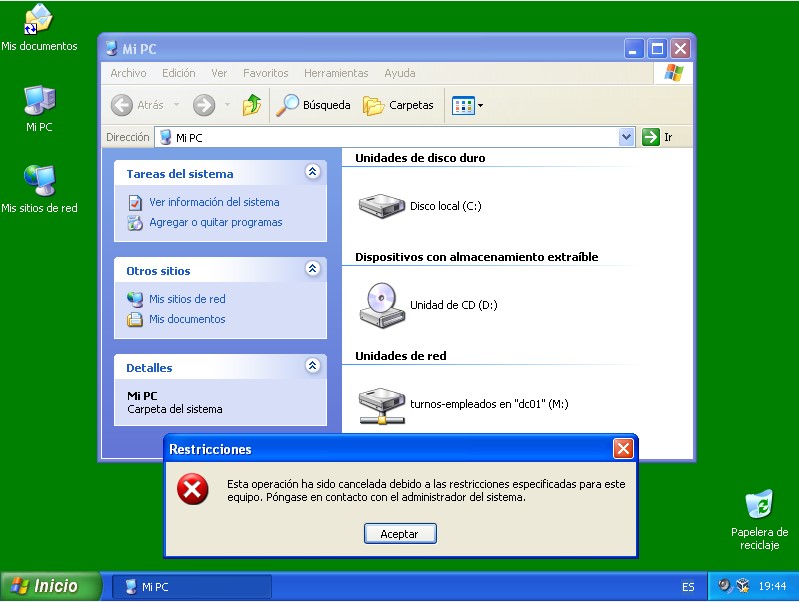
¿Qué ha ocurrido? Ahora sí que está accesible el apagado y el resto de funciones; sencillamente que el usuario ha cerrado sesión. Es en la sesión de usuario en la que hemos deshabilitado estos accesos.



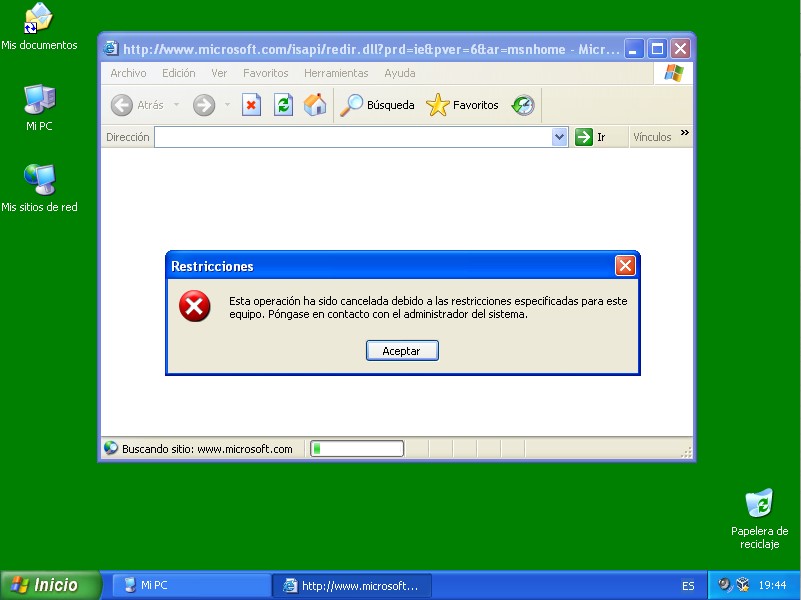
Esta GPO resulta llamativa. Gracias a ella impediremos que los usuarios **puedan cerrar la ventana del explorador de archivos o la del navegador web** (**Internet Explorer**). Nos puede servir para cuando en una exposición se les pide que no hagan nada en los equipos y se les sorprenda haciéndolo, pues no podrán cerrar estas ventanas ...



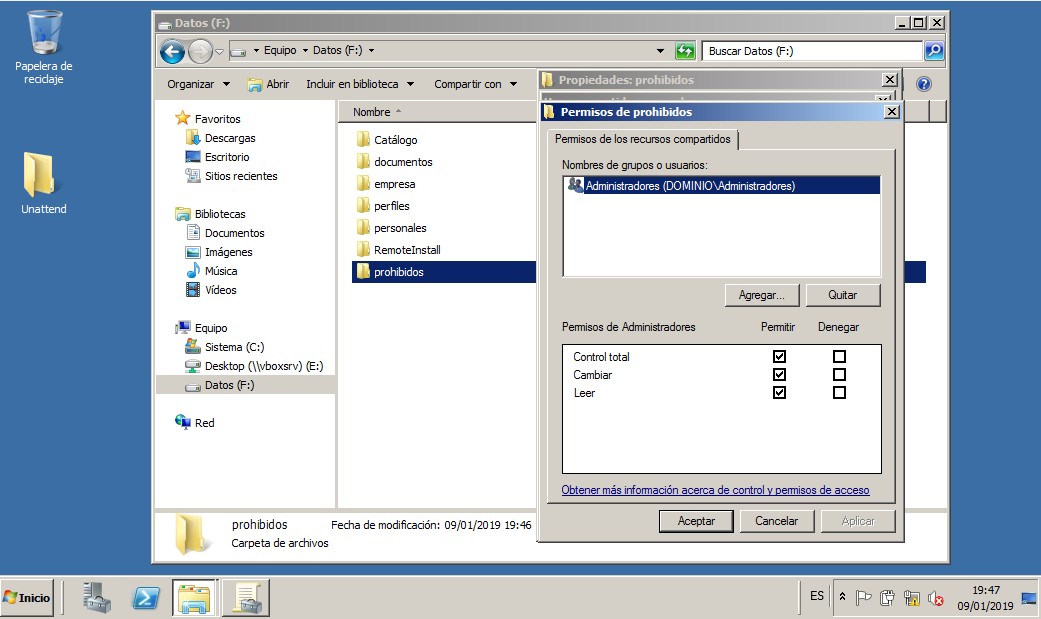
Como se puede comprobar, aparece una mensaje informándonos de la situación, pero no podemos cerrar la ventana del explorador de archivos.



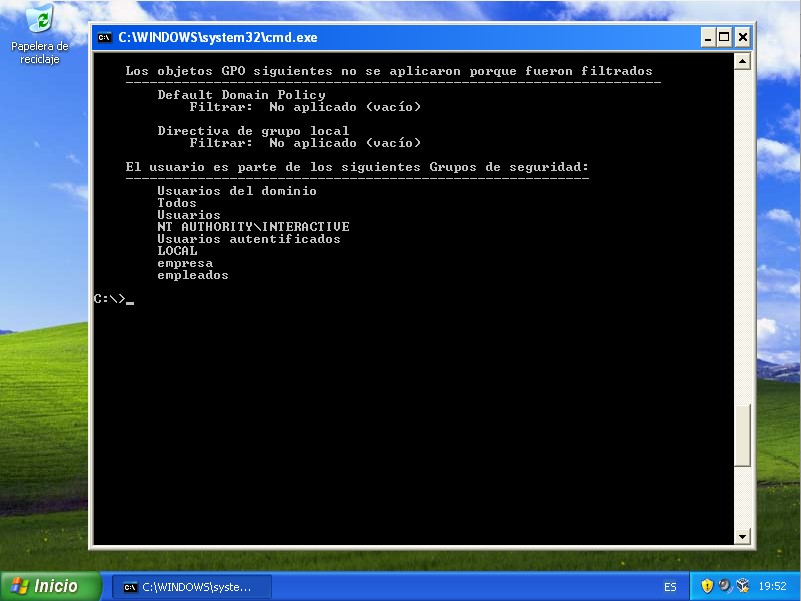
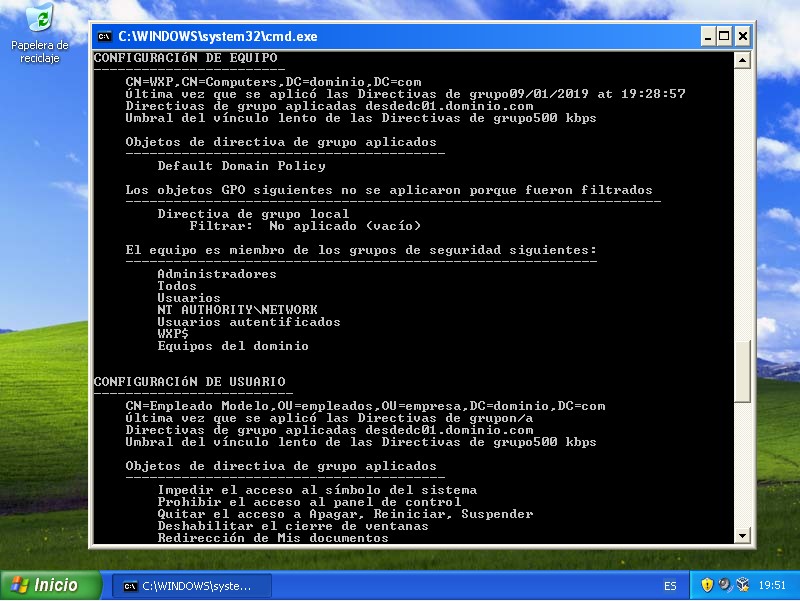
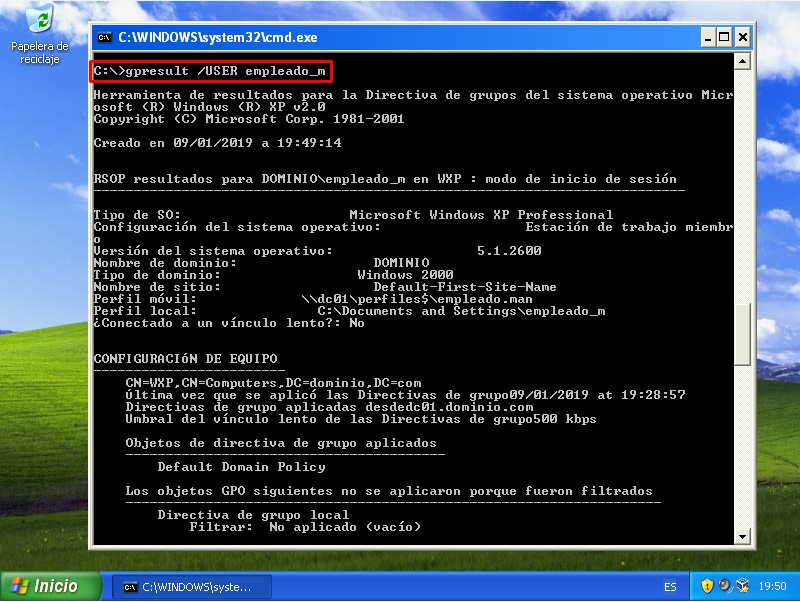
Ocurre lo mismo con el navegador web (Internet Explorer).



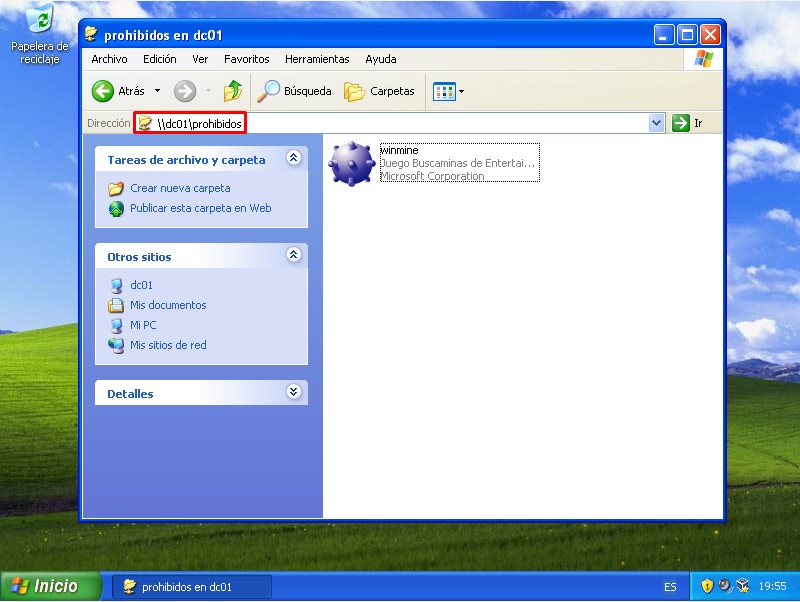
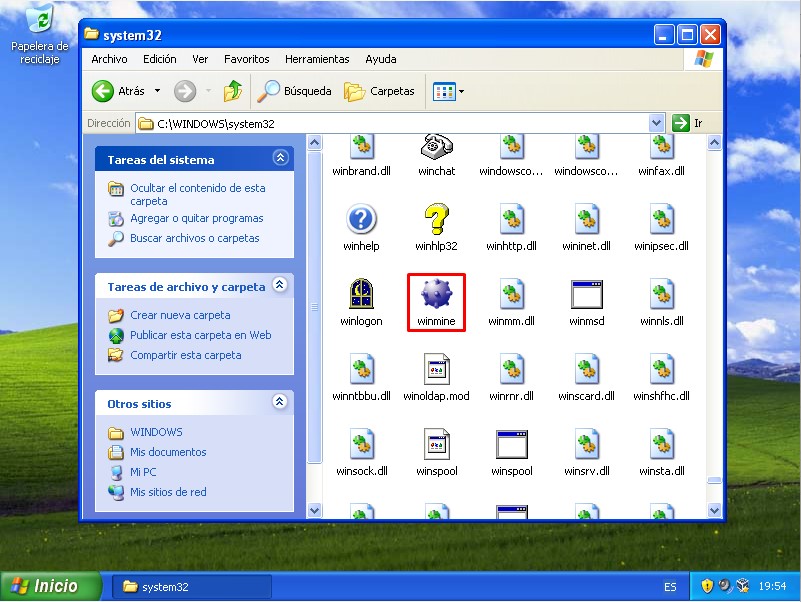
Nuestro siguiente objetivo será que los usuarios no puedan ejecutar algunos programas, especialmente los **juegos**. Para ello, creamos un directorio de nombre **prohibidos** y lo compartimos con **control total** para el grupo **Administradores**, disponiendo así de un directorio que podemos usar para copiar archivos y utilizarlos donde sea necesario, no siendo necesario el uso de otros medios de almacenamiento, como USBs, CDs, DVDs, etc.



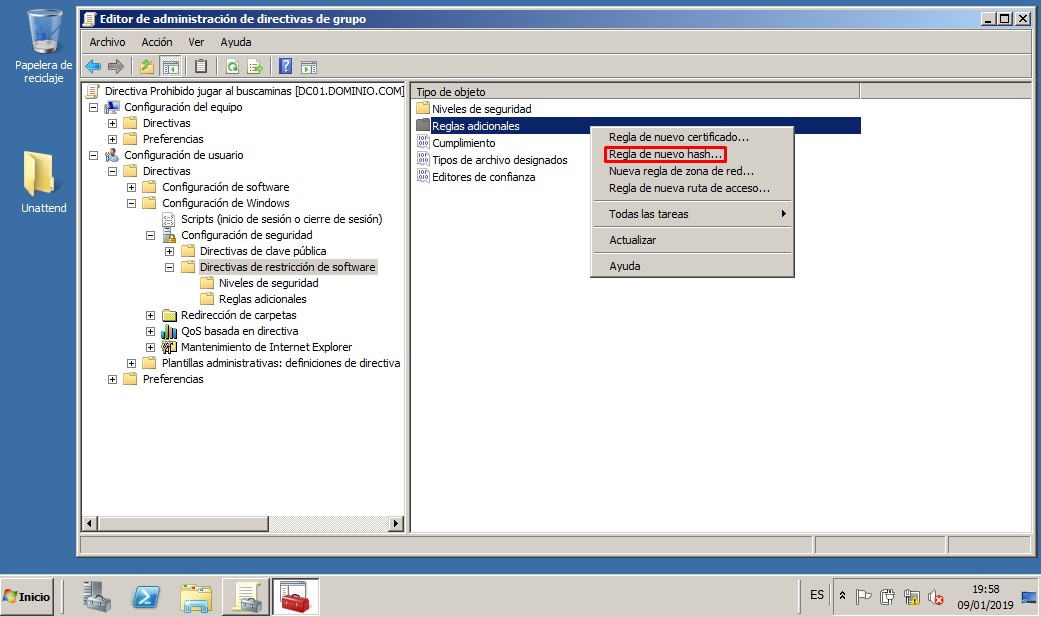
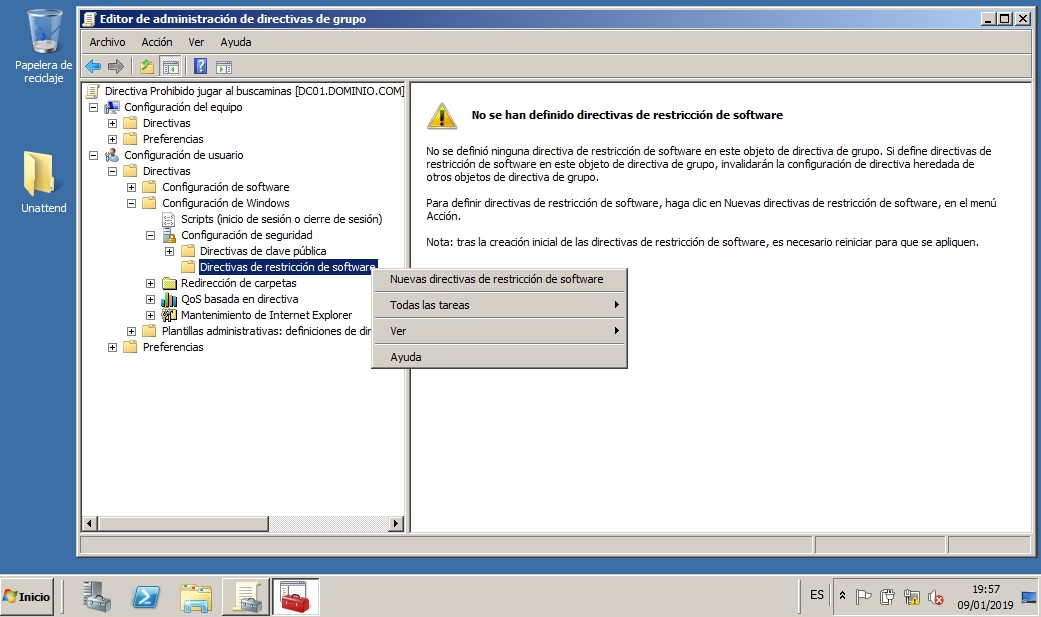
Podemos saber qué GPOs se están aplicando a un usuario concreto. Para ello, ejecutamos el comando que aparece en la siguiente imagen (**gpresult /USER *nombre\_usuario***):



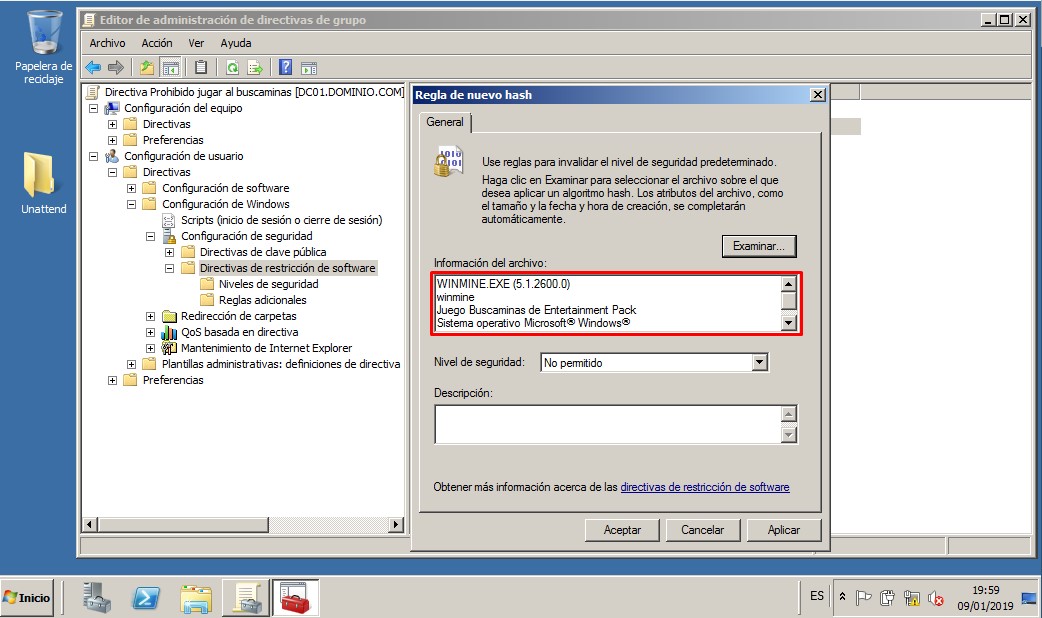
Regresando a la GPO que prohibía la ejecución de un juego (en concreto el **buscaminas**) iniciamos sesión en el cliente del que deseamos **copiar** este juego en la carpeta **prohibidos** y poder aplicarle una **regla de HASH** al mismo y posteriormente definir una GPO para el efecto que perseguimos.



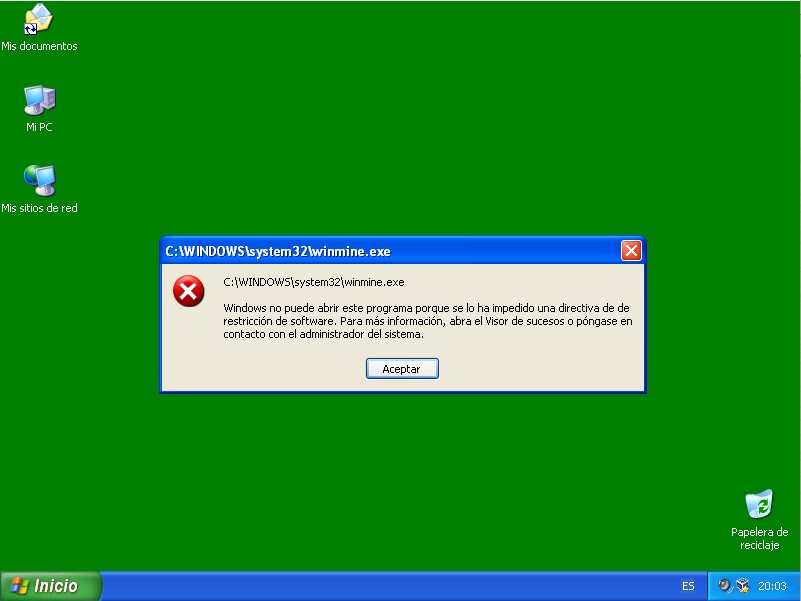
Procedemos a definir la GPO que aplica una **regla de HASH** al archivo:



Es importante destacar que la **regla de HASH** aplicada depende de la **versión del ejecutable**, pues podemos encontrarnos con otro ejecutable con otra versión y esta regla de HASH no aplicaría ...



 Cuando el usuario intenta **jugar al buscaminas**, le aparece la siguiente ventana:



* ¿Para qué sirven las GPOs que vienen por defecto (Default Domain Policy y Default Domain Controllers Policy?
* ¿Dónde se guardan las GPOs? ¿Cómo las elimino?
* ¿Qué ocurre si elimino una GPO aplicada a una unidad organizativa? ¿Qué elimino realmente?
* ¿Cómo puedo evitar la propagación de una GPO aplicada a una unidad organizativa respecto a su unidad organizativa contenedora?
* ¿Puedo utilizar una GPO en varias unidades organizativas? ¿Qué ocurre si elimino el vínculo en una de ellas?
* ¿Puede una GPO contener varios "comportamientos"? ¿Cómo lo trabajamos nosotros?