

Estudio de Problemas de Seguridad

con los

Permisos en Windows NT 4.0

Enero 2000

1.-Introducción

Se presenta un problema que podríamos considerar grave, y que, aunque tenga una sencilla solución, presenta un tedioso proceso de administración en la creación normal de cuentas de usuario.

También encontraremos algunos conflictos y relaciones difíciles entre los permisos NTFS que ofrece NT, y los del sistema, como la compartición de recursos.

Según lo que vamos a ver podremos seguramente concluir con la sospecha de la poca seguridad de NT si lo comparamos con sistemas distribuidos parecidos como UNIX.

2.-Presentación del problema

El problema se basa en las opciones por defecto que se crean y que suelen ser las que se utilizan, pero que, como veremos, al no ser muy restrictivas podrán crear situaciones poco seguras en el sistema .

Estudiemos las opciones que se dan por defecto cuando vamos crear nuevos usuarios:

- Primeramente crearemos un directorio en el disco del Controlador Principal de Dominio para que albergue los directorios personales de los usuarios.(Por ejemplo el directorio C:\Usuarios).
- Para que los usuarios puedan acceder a estos y trabajar en ellos, debemos **compartir** esta carpeta; Inicio | Programas | Explorador | Seleccionar c:\usuarios|Botón Dcho. | Compartir.
- Aquí aparecen los primeros permisos. Al compartir la carpeta se dan sobre ella unos derechos por defecto:

*Según el sistema :(Seleccionando la carpeta c:\usuarios |Compartir|Permisos)

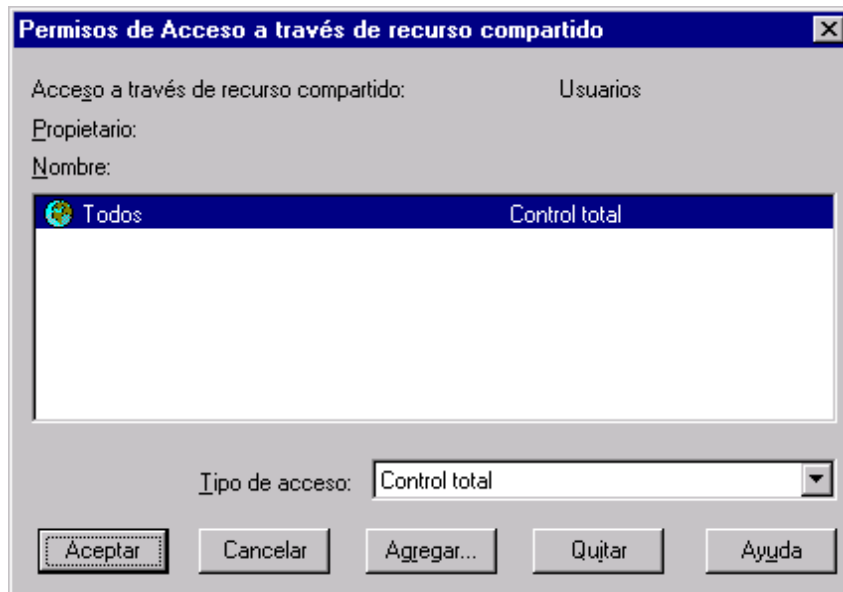


Fig. 1

*Según NTFS (Seleccionar c:\usuarios| boton dcho | Propiedades|Permisos).

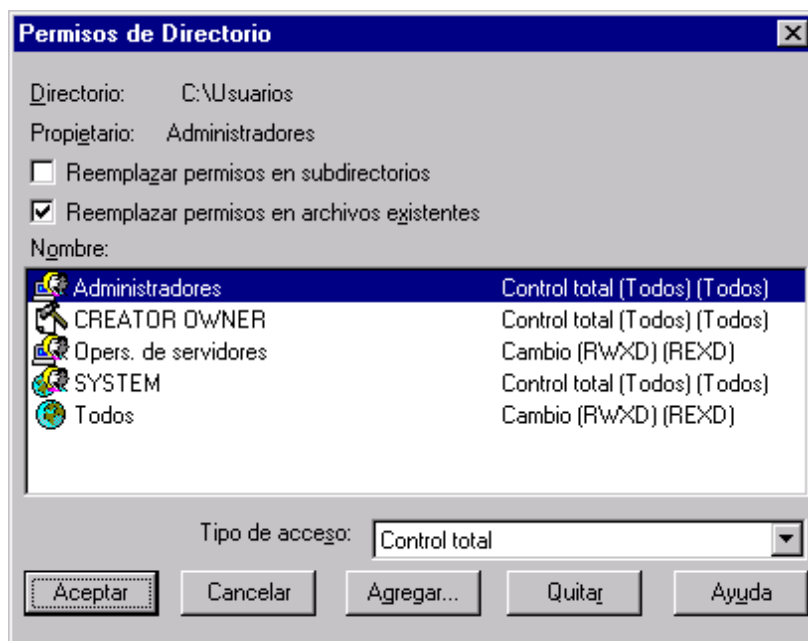


Fig 2.

3.-Creación de Usuarios

Ahora se trata de que creamos el/los usuario/s. Para esto en Inicio | Programas | Herramientas Administrativas | Gestor de Usuarios y Grupos | Archivo | Nuevo . Creamos un nuevo usuario con su Nombre(por ej. Luis), Username y Password.

No lo asignaremos a ningún grupo , (por defecto pertenece a Usuarios del Dominio).

En la opción Perfiles , elegiremos que se cree un directorio personal en una unidad virtual asignada al

Controlador Principal de Dominio \\soft000\usuarios\Luis.

Cuando vamos al Explorador de NT nos damos cuenta de que al intentar entrar en la nueva carpeta que se ha creado para el usuario.....:

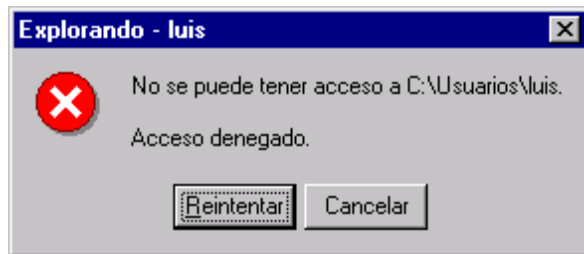


Fig. 3

Estos son otros permisos, son los asignados al crearse el directorio personal para este usuario, (C:\usuarios\Luis), y si vemos los permisos NTFS de este nuevo directorio nos encontramos con la primera cuestión extraña :

–Sobre el directorio solo tiene permisos el propio usuario, además con **Control Total**, y sin embargo el grupo Administradores no aparece, con lo que inicialmente el Administrador **no tiene ningún permiso** sobre el directorio no pudiendo incluso, ni acceder a él.

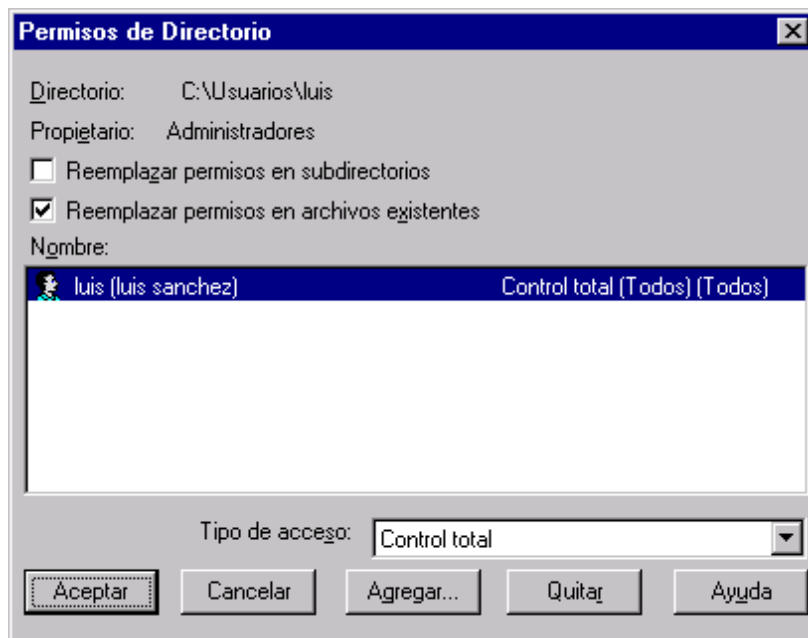


Fig. 4

Luego aquí tenemos que, si el Administrador quiere tener control para acceder a los directorios, así como permisos para modificar, borrarlos, etc...¡Tiene que darse permisos explícitamente sobre cada directorio de cada usuario!!.

Este podría ser el primer problema tomando las opciones por defecto, y luego el Administrador, podría volverse loco buscando el punto donde falló, puesto que no puede acceder a ningún directorio de los usuarios. Afortunadamente si conoce esta pequeña acción y ayudándose de una herramienta de automatización como ADDUSERS, podrá subsanar esto.

4.- Permisos cedidos al Usuario por defecto

¿Qué puede hacer ahora nuestro usuario Luis?:

- Puede manejar su directorio, crear, borrar,..., lo cual es normal.
- No puede ponerse como propietario de la carpeta, puesto que el Administrador es el prop. Normal.
- Pero también puede crear carpetas fuera de su directorio personal, en C:\Usuarios, saliendo así de sus 'territorios' y creando espacio no deseado en el disco del CPD, lo cual no está nada bien.
- Lo peor de todo es que el usuario Luis puede volver a quitar los derechos al Administrador, y este se quedará de nuevo sin poder acceder a la carpeta del usuario Luis, aunque el Administrador puede volver a ponerse los permisos que desee, y luego el usuario para volvérselos a quitar... de esta forma habría un 'toma y daca' de permisos.

Este último problema es quizá el más importante, pero que tiene su solución en los permisos NTFS. Se trata de acceder a los permisos de la carpeta c:\usuarios\luis y limitar los accesos del usuario, y dejárselos en CAMBIO (esto permite todas las acciones menos modificar los permisos) .

Esta acción deja a cada uno en su sitio, al Administrador como tal, con control total sobre los recursos de los usuarios y a estos últimos como propietarios de sus carpetas, de modo que puedan escribir, leer, y todas las demás acciones excepto las acciones que entrañen cambio de los permisos por parte del usuario.

****Pero aun podríamos pensar algo más...:**

Si antes de que el Administrador establezca los permisos del usuario Luis dejándolos en ' CAMBIO', el usuario (aun con Control Total) dejase al Administrador con los permisos de 'Cambio':

¿Quedaría el Administrador sin posibilidad alguna de poder retomar permisos en esa carpeta al no poder modificarlos??

Afortunadamente, **NO**, ¡¡Hemos encontrado algo bueno en esto!!, el Administrador aunque se quede con 'Cambio', podrá modificar sus permisos y volver a dejarlos en 'Control Total', y al usuario de nuevo con lo que debe tener, 'Cambio'.

Gestión del Recurso Compartido.

Pero queda el inconveniente de que el usuario aun puede crear directorios fuera de su carpeta personal. Para limitar esto deberemos acceder ahora a los permisos de la compartición de recursos de la carpeta contenedora (c:\usuarios).

Como vimos al principio (fig.1), todos tienen 'Control Total', pero si limitamos estos derechos sobre el recurso compartido, y los dejamos en 'Solo Lectura', lo que ocurre es que esto afecta a los directorios por debajo de C:\Usuarios con lo que los usuarios *no pueden hacer **nada*** en sus propios directorios.

El recurso compartido no es la solución, debemos dejar control máximo en el recurso e ir limitando los permisos NTFS en las carpetas que nos interesen.

Una vez más debemos actuar sobre los permisos NTFS en

C:\usuarios | Botón Dcho | Propiedades | Seguridad | Permisos

y aquí vemos la fig. 2 donde el grupo Todos tiene los permisos 'Cambio', pues modificamos esto dejándolo en Lectura, esto permite que en esta carpeta C:\Usuarios ningún usuario pueda escribir, pero cuando el usuario entre en su carpeta personal, (en la que tiene 'Cambio'), pueda hacer todo lo que quiera.

5. -Pasos para Definir Bien los Permisos

Con esto quedarían configurados todos los permisos para un funcionamiento normal, hagamos un pequeño repaso por orden de lo que deberíamos hacer:

- *Crear el usuario con su carpeta en el CPD, etc....

- *Dar de alta al Administrador con permiso 'Control Total' en la carpeta del usuario para que pueda acceder y hacer lo que quiera (ejerciendo de Administrador).

- *Limitar los permisos del usuario en su carpeta y dejarlos en 'Cambio' para que no pueda restringir permisos al Administrador.

- *Limitar los permisos del grupo en la carpeta compartida modificando los NTFS dejandolos en Solo Lectura, para que no puedan hacer nada fuera de sus carpetas personales.

Conclusiones

Con todo esto podemos concluir que mientras otros sistemas como UNIX tiene bastante solucionados este tipo de problemas, NT parece ser más lioso, e incluso algunas veces contradictorio.

Una cosa se observa claramente si nos ponemos a comparar a los dos sistemas, mientras en uno (UNIX), contamos con que las opciones por defecto son *las más restrictivas para el usuario*, (proporcionando más seguridad al sistema), en Windows NT las opciones por defecto *no son nada restrictivas* en cuanto al tema de los permisos, implicando luego al Administrador en tareas de búsqueda en el sistema de 'huecos' para remendar.

Podríamos decir que en temas de sistemas distribuidos con accesos de usuarios, más aun si se permite movilidad, el sistema debe ser siempre *mal pensado* de forma que no deje al usuario hacer demasiadas cosas (por lo menos inicialmente) de modo que más adelante si el Administrador lo cree conveniente, y en casos puntuales, pueda dar algunos accesos especiales.

Administración de Sistemas Informáticos.

5º Ingeniería Informática.

9

Problemas de Seguridad con los Permisos en Windows NT 4.0