Práctica 3

Gestión de usuarios y seguridad (2ª parte)

Objetivos

Saber crear una organización administrativa coherente en un sistema, con sus usuarios, grupos y carpetas. Saber configurar la ACL de las carpetas para que puedan acceder a ellas los usuarios necesarios con los permisos apropiados.

Comprender el significado preciso de los permisos utilizados en la ACL.

Aprender a utilizar la herramienta *Conexión a escritorio remoto* para iniciar sesión en un sistema de forma remota.

Comprender quién puede instalar y utilizar software en un sistema, así como la forma usada para proteger las carpetas de software de los usuarios del sistema.

Comprender el concepto de propiedad de archivos y carpetas.

Conocer el mecanismo apropiado para eliminar usuarios de un sistema.

Comprender el concepto de derechos de usuario. Saber asignar derechos a usuarios y grupos.

Desarrollo de la práctica

1 Creación de usuarios y grupos

En la práctica 2 has manejado usuarios y grupos y has visto su utilidad. En esta práctica, utilizando los privilegios del administrador del sistema, vas a crear usuarios y grupos, con el objeto de establecer una estructura administrativa coherente en un sistema.

Imagina que queremos administrar un sistema que va a ser manejado por alumnos de dos asignaturas y sus correspondientes profesores. Supongamos que se trata de las asignaturas de Tecnología de Computadores y Fundamentos de Computadores. En la tabla siguiente se muestran los nombres de usuario correspondientes a los alumnos y profesores de ambas asignaturas.

Tecnología de Computadores	Profesor: PTC Alumnos: ATC1 y ATC2
Fundamentos de Computadores	Profesor: PFC Alumnos: AFC1 y AFC2

Tabla 1: Conjunto de usuarios pertenecientes a una determinada estructura administrativa

Vamos entonces a crear una estructura administrativa que permita a profesores y alumnos compartir información. Cada asignatura contará con una carpeta, en la que el profesor deja información para los alumnos. Los alumnos tienen que tener capacidad para acceder a esta información, pero no deben de poder borrarla. Además, para facilitar la administración de estas carpetas, habrá que crear un grupo para contener a los alumnos de cada asignatura (ten en cuenta que en este ejemplo sólo manejamos dos alumnos por asignatura, pero lo normal es que sean muchos más. Así que para facilitar las tareas administrativas, la creación de estos grupos es fundamental). Vamos entonces a crear esta estructura administrativa.

H Comprueba que has arrancado el sistema como *Administrador*. Tienes que ser el administrador para llevar a cabo las operaciones que se indican en los pasos siguientes.

H En primer lugar vas a crear los seis usuarios indicados en la tabla 1. Para ello utilizarás la herramienta *Administración de equipos*. Utiliza la contraseña *practicas* para todos los usuarios (fíjate bien que no se encuentren las mayúsculas activadas). En cuanto a las opciones de la contraseña, usa las siguientes: *El usuario no puede cambiar la contraseña* y *La contraseña nunca caduca*.

La creación de un usuario no implica que se cree su perfil. Vamos a comprobar ahora que los perfiles de los usuarios que acabas de añadir al sistema aún no han sido creados. Recuerda que los perfiles se almacenan en la carpeta *Documents and settings*. Recuerda también que el nombre de la carpeta del perfil de un usuario es el mismo que el nombre del usuario.

H Teniendo en cuenta las indicaciones anteriores comprueba que aún no se ha creado el perfil de ninguno de los usuarios que acabas de añadir al sistema.

El perfil de un usuario se crea la primera vez que inicia sesión en el sistema. Vamos a comprobar esto.

H Abandona la sesión abierta como administrador y abre una nueva sesión como AFC1. Comprobarás que tarda un poco. Esto es debido a que se está generando el perfil. Abre la carpeta *Documents and settings* y comprueba que se ha generado en ella la carpeta AFC1. Esta carpeta contiene el perfil del usuario AFC1.

H Cierra esta sesión y comienza de nuevo una sesión como *Administrador*.

Ahora vamos crear grupos para facilitar el mecanismo de concesión de permisos de acceso a recursos para los diferentes usuarios.

H Utilizando de nuevo la herramienta *Administración de equipos*, crea un grupo llamado ATC y agrega a él los usuarios ATC1 y ATC2. A continuación crea otro grupo llamado AFC y agrega a él los usuarios AFC1 y AFC2.

En este punto ya hemos creado la estructura de usuarios que necesitamos. Ahora vamos a crear las carpetas para las diferentes asignaturas.

H Crea en la unidad `C:` la carpeta *Asignaturas*. ¿Qué usuarios podrán acceder a esta carpeta?

–Pregunta 1–

Es conveniente que los grupos *Administradores* y SYSTEM se encuentren siempre en la ACL. Mediante el grupo *Administradores* podrás controlar el objeto siendo *Administrador*. SYSTEM es una cuenta utilizada por los procesos del sistema. El grupo CREATOR OWNER es prescindible y el grupo *Usuarios* debemos eliminarlo, ya que no todos los usuarios del sistema deben tener acceso a la carpeta *Asignaturas*.

H Elimina los grupos CREATOR OWNER y *Usuarios* de la ACL de *Asignaturas*.

Ahora tenemos que conseguir que tanto los profesores como los alumnos de las asignaturas de Tecnología y Fundamentos de Computadores tengan acceso a la carpeta *Asignaturas*.

H Para ello agrega a la ACL de Asignaturas los siguientes grupos y usuarios: ATC (grupo de alumnos de Tecnología de Computadores), AFC (grupo de alumnos de Fundamentos de Computadores), PTC y PFC.

H ¿Qué permisos se dan por defecto a los usuarios y grupos que has agregado a la ACL de *Asignaturas*?

–Pregunta 2–

H Inicia sesión consecutivamente como AFC1 y PTC. Observarás que ambos usuarios se comportan de la misma forma respecto a la carpeta *Asignaturas*. Indica a continuación si estos usuarios pueden llevar a cabo o no las siguientes operaciones con la carpeta asignaturas.

–Pregunta 3–

Abrir la carpeta:
Cambiar el nombre de la carpeta:
Borra la carpeta:
Crear un fichero en la carpeta:

Observarás que *Asignaturas* se encuentra bien protegida respecto a posibles modificaciones que los usuarios pueden llevar a cabo en ella.

Queda por ver qué pueden hacer otros usuarios del sistema con la carpeta *Asignaturas*. Para ello puedes utilizar por ejemplo el usuario *Alumno*.

H Inicia una nueva sesión como *Alumno*. Intenta entrar en la carpeta *Asignaturas*. Observarás que ni siquiera no puedes entrar en ella, ¿por qué?

–Pregunta 4–

Esto debe ser así por que la carpeta *Asignaturas* no está pensada para dar servicio a todos los alumnos (que acceden al sistema mediante la cuenta *Alumno*), sino solo a los de Tecnología y de Fundamentos de Computadores.

Ahora continuarás con la creación de las carpetas necesarias para las asignaturas de Tecnología y Fundamentos de Computadores.

H Inicia una nueva sesión como *Administrador*. Crea dentro de *Asignaturas* las carpetas *TecnologiaComp* y *FundamentosComp*. Observa que estas carpetas heredan su ACL de *Asignaturas.*

Vamos a comenzar por adecuar las ACLs de *TecnologiaComp* a las necesidades específicas de esta carpeta.

H Empieza por eliminar de su ACL aquellos usuarios y grupos que no deben tener acceso a ella. Claramente se trata del grupo AFC y del usuario PFC, que no pertenecen a esta asignatura.

En estos momentos quedarán en la ACL de *TecnologiaComp* el grupo ATC y el usuario PTC (además de Administradores y SYSTEM que siempre están). Los permisos de ATC son correctos, ya que están activados los permisos típicos de lectura que son los que deben tener los alumnos. Sin embargo, en el caso de PTC habrá que modificar sus permisos, ya que el profesor tendrá que tener la capacidad de poner material en la carpeta *TecnologiaComp*, para que luego los alumnos puedan verlo.

H Activa el permiso *Modificar* para el usuario PTC. Este permiso permitirá a este usuario hacer todo tipo de modificaciones en la carpeta *TecnologiaComp*, como por ejemplo, modificar su contenido almacenado cosas en ella.

H Inicia una sesión como PTC. Abre la carpeta *TecnologiaComp*. Crea en ella el fichero `pruba1.txt`, escribiendo en él cualquier cosa. Crea ahora una carpeta llamada *Pruebas* y dentro de ella crea el fichero `prueba2.txt`, escribiendo en él lo que quieras.

Si has podido realizar estas operaciones, la seguridad de *TecnologiaComp* está bien configurada respecto al usuario PTC.

H Inicia sesión como ATC1. Observa que puedes entrar en *TecnologiaComp*, que puedes abrir *Pruebas* y también los ficheros `prueba1.txt` y `prueba2.txt`. Sin embargo, prueba también que no puedes realizar ningún tipo de modificación en los elementos que hay dentro de *TecnologiaComp*. Indica a continuación cuatro cosas diferentes que no puedes modificar, haciendo las pruebas correspondientes.

–Pregunta 5–

Veamos finalmente qué pueden hacer en *TecnologiaComp* otros usuarios del computador, como por ejemplo, un alumno de Fundamentos de Computadores.

H Inicia una nueva sesión como AFC1. Observa que ni siquiera puedes abrir la carpeta. Además, si mediante el botón derecho del ratón abres la ventana de propiedades de la carpeta, también observarás que no se muestra la ficha *Seguridad*.

Todo esto ocurre porque ni AFC1, ni ningún grupo en el que se encuentre AFC1 están en la ACL de la carpeta. Por tanto dicho usuario no tiene ningún tipo de acceso a esta carpeta.

La conclusión que podemos obtener de las operaciones anteriores es que el profesor tiene control total sobre la carpeta de la asignatura, los alumnos de la asignatura tienen acceso a la información de la carpeta pero no pueden modificarla, y el resto de usuarios no tienen ningún tipo de acceso a la carpeta. Hemos creado así una organización administrativa totalmente coherente. No obstante, todavía resta algún detalle. Vas realizar una última prueba.

H Inicia sesión como PTC. Este usuario puede hacer cualquier operación dentro de la carpeta *TecnologiaComp*, pero ¿podrá por ejemplo eliminarla? Haz la prueba. Habrás observado que PTC puede también eliminarla. Intenta volver a crearla, ¿puedes? ¿por qué?

–Pregunta 6–

El usuario que controla una carpeta ubicada dentro de otra sobre la que no tiene privilegios debe ser cuidadoso. Si accidentalmente borra la carpeta que controla no podrá volver a restaurarla por sí mismo. Para ello necesitará la colaboración del administrador del sistema.

H Inicia una sesión como *Administrador* y vuelve a crear la carpeta *TecnologiaComp*. Entonces configura su ACL como lo hiciste anteriormente.

Resta ahora preparar la ACL de la carpeta *FundamentosComp* siguiendo las mismas directrices que las usadas con la carpeta *TecnologiaComp*.

H Lleva a cabo las modificaciones necesarias en la ACL de la carpeta *FundamentosComp*.

H Realiza el conjunto de pruebas que se indican a continuación para determinar que la ACL de *FundamentosComp* ha sido correctamente configurada:

1. Inicia una sesión como PFC. Comprueba que tienes total acceso a la carpeta *FundamentosComp*. Usando el *Bloc de notas*, crea un fichero y dale el nombre `prueba2.txt`. Comprueba que puedes almacenarlo en *FundamentosComp* y que el fichero hereda su ACL.
2. Inicia una sesión como AFC1. Comprueba que no puedes borrar `prueba2.txt`, ni almacenar fichero alguno en *FundamentosComp*. Sin embargo, sí puedes copiar `prueba2.txt` a otra localización. Después de probar esto, borra `prueba2.txt` de esa localización, pero no borres el que se encuentra en la carpeta *FundamentosComp*.
3. Inicia una sesión como ATC1. Comprueba que no tienes ningún tipo de acceso a la carpeta *FundamentosComp*.

Si el sistema ha pasado todas las pruebas anteriores satisfactoriamente, has configurado la ACL de *FundamentosComp* correctamente. En este punto ya tienes una estructura de carpetas configuradas con los permisos adecuados.

2 Permisos

En este punto se analizará el funcionamiento de los permisos en profundidad. Para ello empezaremos preparando una carpeta con una ACL apropiada.

H Inicia una sesión como *Administrador*. Crea en la unidad `C:` la carpeta *Pruebas*. Abre su ficha *Seguridad* y deja en ella nada más que los grupos *Administradores* y SYSTEM. Ahora agrega a su ACL el usuario *Alumno*, que es el que vamos a utilizar para llevar a cabo las pruebas. Dale a este usuario los permisos *Lectura y ejecución*, *Mostrar el contenido de la carpeta* y *Leer*.

Ahora ubicaremos varios ficheros en esta carpeta y sobre ellos analizaremos el funcionamiento de los permisos.

H crea en *Pruebas* el fichero `prueba1.txt`, escribiendo en él cualquier cosa. Entonces haz las operaciones necesarias para que los permisos heredados por este fichero no se traten como permisos heredados, sino como permisos primarios del objeto. Selecciona una entrada cualquiera de la ACL de `prueba1.txt` (*Alumno* por ejemplo) y escribe a continuación los permisos que se le pueden asignar (escríbelos todos, independientemente de si están asignados o no).

–Pregunta 7–

Los permisos anteriores, a los que se accede seleccionando una entrada de la ACL, representan en realidad agrupaciones de permisos más simples. Vamos a analizar esto.

H En la entrada *Alumnos* de la ACL de `prueba1.txt` haz que solamente se encuentre seleccionado el permiso *Leer*. Ahora observaremos los permisos simples que corresponden a este permiso. Para ello pulsa el botón *Opciones avanzadas*. Se abre entonces la ventana *Configuración de seguridad avanzada*. Esta ventana muestra una lista de miembros de la ACL con los permisos que tienen asociados. Por ejemplo, observarás el usuario *Alumno* con el permiso asociado *Leer*. Selecciona la entrada correspondiente a *Alumno*, entonces pulsa sobre el botón *Modificar*. Se abre entonces una ventana en la que se muestran los permisos simples que corresponden al permiso *Leer*. Escríbelos a continuación:

–Pregunta 8–

Antes de analizar más detenidamente el funcionamiento de estos permisos simples, vamos a almacenar en la carpeta *Pruebas* otro fichero de características diferentes a las de `prueba1.txt`.

H Abre la carpeta de la asignatura. Entonces copia el fichero `prog1-1.exe` en la carpeta *Pruebas*.

En *Pruebas* tenemos ahora dos ficheros de características diferentes: `prueba1.txt` es un fichero de datos mientras que `prog1-1.exe` es un fichero ejecutable. Debido a su diferente naturaleza, estos ficheros pueden requerir configuraciones de seguridad

diferentes. De momento, vas a configurar la seguridad de `prog1-1.exe` igual que en `prueba1.txt`.

H Abre la ficha *Seguridad* de `prog1-1.exe`. Entonces haz las operaciones necesarias para que los permisos heredados por este fichero no se traten como permisos heredados, sino como permisos primarios del objeto. Selecciona la entrada *Alumno* de la ACL y haz que solamente se encuentre seleccionado el permiso *Leer*.

En este momento la configuración de seguridad de `prueba1.txt` y `prog1.exe` deben ser idénticas. Ahora vamos a analizar el comportamiento de la configuración de seguridad de estos ficheros.

H Inicia una nueva sesión como *Alumno*. Abre la carpeta *Pruebas*. Ahora observa que puedes abrir el fichero `pruebas1.txt` pero no puedes borrarlo. Esto debe ser así debido a la configuración de seguridad del fichero respecto al usuario *Alumno*.

H Intenta ahora ejecutar `prog1-1.exe`. ¿Qué ocurre? ¿Por qué?

–Pregunta 9–

Vamos entonces a configurar apropiadamente la seguridad de `prog1-1.exe`.

H Inicia una nueva sesión como *Administrador*. Abre la carpeta *Pruebas*. Abre la ficha *Seguridad* de `prog1-1.exe`. Selecciona el usuario *Alumno* en la ACL. Observa que sólo está activado el permiso *Leer*. Pulsa sobre *Opciones avanzadas*. Selecciona de nuevo *Alumno* en las *Entradas de permisos* y observa (como ya vimos antes) los cuatro permisos simples correspondientes al permiso *Leer*. Vuelve hacia atrás hasta la ACL de `prog1-1.exe`. Entonces agrega el permiso *Lectura y ejecución* al usuario *Alumno*. Pulsa de nuevo *Opciones avanzadas*. Selecciona *Alumno* en las *Entradas de permisos* y observa que se ha agregado un nuevo permiso simple, ¿cuál es?

–Pregunta 10–

Pulsa Aceptar las veces necesarias para salvar este nuevo permiso.

H Inicia una nueva sesión como *Alumno* y comprueba que ahora sí puedes ejecutar el fichero `prog1-1.exe`.

Vamos a explorar ahora los permisos de escritura. Recuerda que has probado antes que no puedes hacer ningún tipo de operación de escritura o modificación con el fichero `prueba1.txt`.

H Inicia una nueva sesión como *Administrador*. Abre la carpeta *Pruebas* y muestra la ficha *Seguridad* de `prueba1.txt`. En este momento solo está activado el permiso *Leer*. Abre la ventana en la que se muestran los permisos simples y recuerda una vez más los cuatros permisos simples que corresponden a *Leer*. Cierra esta ventana volviendo a la ficha *Seguridad*. Ahora agrega el permiso *Escribir*. Abre de nuevo la ventana en la que se muestran los permisos simples del usuario *Alumno*. Indica a continuación los permisos simples que corresponden al permiso *Escribir*.

–Pregunta 11–

Acepta las veces que sean necesarias para que el permiso Escribir sea agregado a *Alumno*.

Vamos a comprobar qué nuevas cosas puede hacer el usuario *Alumno* sobre `prueba1.txt`.

H Abre una nueva sesión como *Alumno*. Ahora haciendo las pruebas necesarias sobre el fichero prueba.txt indica cuáles de las operaciones que se indican a continuación son posibles. Contesta SÍ o NO a la derecha de cada operación.

–Pregunta 12–

Modificar el contenido del fichero: Borrar el fichero: Cambiar el nombre del fichero:

Vamos a seguir incrementando los privilegios del usuario *Alumno* sobre el fichero `pruebas.txt`.

H Inicia una nueva sesión como *Administrador*. Abre la carpeta *Pruebas* y muestra la ficha *Seguridad* de `prueba1.txt`. En este momento están activados los permisos *Leer* y *Escribir*. Abre la ventana en la que se muestran los permisos simples y recuerda todos los permisos simples que corresponden a *Leer* y *Escribir*. Cierra esta ventana volviendo a la ficha *Seguridad*. Ahora agrega el permiso *Modificar*. Observa que se activa también *Lectura y ejecución*. Respecto a los permisos simples que tenía el usuario *Alumno* cuando tenía asignados *Leer* y *Escribir*, ¿qué nuevos permisos simples se acaban de agregar al asignar el permiso *Modificar*?

–Pregunta 13–

Llamo tu atención sobre el permiso *Eliminar*, que es el que te permitirá borrar el archivo.

H Abre una nueva sesión como *Alumno*. Primero observa que sigues sin poder cambiar el nombre a `prueba1.txt`, a pesar de que ahora tienes el permiso *Modificar*. El problema es que cambiar el nombre significa eliminar el fichero y volver a crearlo con un nuevo nombre. Ahora sí tienes privilegio para eliminarlo, pero no para volver a crearlo, porque el usuario *Alumno* no puede escribir en la carpeta *Pruebas*. Finalmente borra el fichero, comprobando así que funciona el permiso *Eliminar*.

Falta analizar el permiso *Control total*. Con relación al permiso *Modificar*, que permite hacer todo tipo de operaciones de lectura y escritura sobre el fichero, el permiso *Control total* aporta la capacidad de cambiar los permisos de seguridad. Para probar *Control total* utilizaremos el fichero `prog1-1.exe` que debe encontrarse todavía en la carpeta *Pruebas*.

H Abre la ficha *Seguridad* de `prog1-1.exe`. Selecciona la entrada *Alumno*. En este momento deben estar seleccionados los permisos *Lectura y ejecución* y *Leer*. Observa que los cuadros de selección de permisos se encuentran sombreados. Esto es así porque *Alumno* no los puede modificar, ya que no tiene el permiso *Control total*. Para darle a *Alumno* este permiso inicia una nueva sesión como *Administrador*. Abre la ficha *Seguridad* de `prog1-1.exe` y concédele al usuario *Alumno* el permiso *Control total*. Abre la ventana en la que se muestran los permisos simples correspondientes al permiso *Control total*. Observa que todos los permisos simples se encuentran seleccionados. Acepta las veces que sean necesarias para que el permiso *Control total* sea agregado a *Alumno*.

H Inicia una nueva sesión como *Alumno*. Abre la ficha *Seguridad* de `prog1-1.exe`. Selecciona la entrada *Alumno* de la ACL. Observa que ahora los cuadros de selección de permisos no están sombreados, lo que significa que son modificables por el usuario. Esto es así porque *Alumno* tiene ahora asignado el permiso *Control total*. Quita la selección del permiso *Control total*, *Acepta* y abandona la ficha *Seguridad*. Vuelve a abrir la ficha *Seguridad*. Selecciona la entrada *Alumno*. ¿Qué ha ocurrido?

–Pregunta 14–

H Finalmente elimina `prog1-1.exe` de la carpeta *Pruebas*.

Ejercicio de permisos

Si has seguido sin problemas las explicaciones anteriores, intenta realizar el siguiente ejercicio.

H Abre una sesión como *Administrador*. Elimina la carpeta *Pruebas* y vuelve a crearla. Elimina de su ACL los grupos CREATOR OWNER y *Usuarios*. Ahora piensa en cómo debes completar la configuración de la ACL de esta carpeta para que su comportamiento de seguridad sea el siguiente:

- El usuario PTC debe poder colocar archivos en la carpeta, así como modificar su contenido y eliminarlos. Debe poder realizar también cualquier operación de lectura o ejecución sobre ellos.
- Los usuarios del grupo ATC pueden colocar archivos y modificar su contenido, pero no pueden eliminarlos. También pueden realizar cualquier operación de lectura o ejecución sobre los archivos de la carpeta.
- El usuario *Alumno* no puede colocar archivos en la carpeta. Tampoco puede modificar ni eliminar los archivos que se encuentren en la carpeta. Debe poder leer archivos de datos, pero no debe poder ejecutar los programas que se encuentren en la carpeta.

H Configura la ACL de Pruebas para que se comporte según las pautas indicadas. Entonces realiza la siguiente batería de pruebas. Si todas son afirmativas, habrás configurado la seguridad correctamente. Si no es así, busca dónde se encuentra el problema.

- Inicia sesión como PTC. Crea un archivo de texto en *Pruebas*. Después modifica su contenido salvándolo. Finalmente elimínalo.
- Inicia sesión como ATC1. Crea el archivo `prueba1.txt` en *Pruebas*. Después modifica su contenido. Finalmente intenta borrarlo y comprueba que no puedes.
- Continúas en la sesión de ATC1. Abre la carpeta de la asignatura. Entonces copia el fichero `prog1-1.exe` en *Pruebas*. Observa que puedes ejecutarlo.
- Inicia sesión como *Alumno*. Comprueba que puedes abrir `prueba1.txt`, pero no modificar su contenido. Comprueba que no puedes ejecutar `prog1-1.exe`.
- Inicia sesión como PFC. Ni siquiera puedes abrir la carpeta *Pruebas*.

H Después de pasar con éxito todas las pruebas anteriores, inicia una sesión como Administrador y borra la carpeta *Pruebas*.

3 Inicio de sesión en forma remota

Windows Server 2003 ofrece el servicio conocido como escritorio remoto, que significa que puede exportar el escritorio a otra máquina conectada a la red que actúa como cliente. En concreto, de forma estándar, Windows Server 2003 puede exportar hasta dos escritorios remotos simultáneos, además de encontrarse activo también de forma simultánea el escritorio local. Esto significa que hasta tres usuarios pueden tener abierta sesión de forma simultánea en el sistema. Para establecer la conexión remota, la máquina cliente utiliza la herramienta *Conexión a escritorio remoto*, a la que se accede a través de *Inicio* **à** *Todos los programas* **à** *Accesorios*. Vamos entonces a probar el funcionamiento de esta característica de Windows Server 2003.

H En primer lugar tienes que activar la posibilidad de acceso remoto al sistema. Para ello tienes que iniciar sesión como *Administrador*. Entonces pulsa con el botón derecho del ratón sobre *Mi PC* y elige *Propiedades*. Después elige la ficha *Acceso remoto*. En el cuadro *Escritorio remoto* tienes que habilitar la casilla de selección *Habilitar escritorio remoto en este equipo*. Una vez realizado esto, cierra la sesión abierta con el *Administrador*.

H Arranca la otra máquina de tu mesa de trabajo que actuará como máquina cliente y ejecuta en ella la herramienta *Conexión a escritorio remoto*. Se abre una ventana en la que tienes que indicar la identificación del equipo en el que deseas iniciar sesión. Para identificar el equipo puedes utilizar el nombre DNS del equipo o su dirección IP. En nuestro caso utilizaremos la dirección IP. Las direcciones IP de los equipos del laboratorio tienen la estructura 156.35.151.XXX, donde XXX es el número de la máquina, que se indica en su correspondiente pegatina de identificación. Teniendo en cuenta esta información conéctate a la máquina Windows Server 2003 de tu mesa de trabajo. Inicia sesión en ella como *Administrador*. En este momento tienes abierto el escritorio remoto en la máquina cliente. Mediante el escritorio remoto puedes prácticamente cualquier operación en la máquina que exporta el escritorio. Navega por ejemplo por su estructura de carpetas.

En la máquina cliente el escritorio remoto es una aplicación más. Entonces podemos minimizar el escritorio remoto y trabajar con otras aplicaciones locales. Para esto, el escritorio remoto tiene una barra de control en la parte superior que te permite cerrarlo y minimizarlo.

H Utiliza el botón *Minimizar* de la barra de control del escritorio remoto para minimizarlo. Entonces recuperas el control de la máquina cliente. Vuelve a maximizar el escritorio remoto. Ahora para terminar la sesión que has abierto en el servidor, utiliza el botón *Cerrar sesión*.

Analizaremos ahora quién puede iniciar sesión mediante el escritorio remoto. De momento sabemos que el *Administrador* puede hacerlo.

H Ejecuta de nuevo *Conexión a escritorio remoto* y conéctate a la máquina Windows Server 2003 de tu mesa de trabajo. Intenta iniciar sesión con el usuario PTC, ¿qué ocurre?

–Pregunta 15–

H Si no has leído el mensaje de error recibido, vuelve a intentar iniciar sesión como PTC y lee atentamente el mensaje de error.

H Inicia sesión como *Administrador* en la máquina Windows Server 2003. Haz las operaciones necesarias para que el usuario PTC pueda iniciar sesión de forma remota. Si no tienes esto claro, pregúntale a tu profesor.

H Una vez realizado el punto anterior y sin cerrar la sesión abierta con el *Administrador* en la máquina Windows Server 2003, ejecuta de nuevo *Conexión a escritorio remoto* en la máquina cliente y conéctate utilizando el usuario PTC, comprobando que ahora sí puedes conectar.

En este momento la máquina Windows Server 2003 se está comportando como una máquina multiusuario, que significa que múltiples usuarios (dos en nuestros caso) tienen una sesión interactiva abierta en el sistema. Los recursos de la máquina se comparten entre los diferentes usuarios. Así si un usuario utiliza los recursos de la máquina intensivamente, esto afectará al resto de usuarios del sistema. Vamos a probar esto.

H En la sesión local del *Administrador* en la máquina Windows Server 2003, entra en la carpeta de la asignatura y copia en el escritorio el programa `prog1-1.exe`.

H En la sesión remota del usuario PTC en la máquina cliente, entra en la carpeta de la asignatura y copia en el escritorio el programa `pro1-3.exe`. Ejecuta este programa. Anota a continuación el tiempo que tarde ejecutarse.

–Pregunta 16–

H En la sesión local del *Administrador* en la máquina Windows Server 2003, lanza dos ejecuciones del programa `prog1-1.exe`. Entonces en la sesión remota del usuario PTC vuelve a ejecutar `prog1-3.exe`. Debes observar que tarda aproximadamente el doble en ejecutarse. Esto es debido a que ahora este programa tiene que competir por los dos núcleos del sistema con los dos procesos `prog1-1.exe` lanzados por el usuario *Administrador*.

H Finalmente borra de los escritorios `prog1-1.exe` y `pro1-3.exe`.

4 Instalación y utilización de software

Este apartado de la práctica se realizará completamente desde una sesión remota utilizando el escritorio remoto. El único objetivo de esto es practicar el uso de esta herramienta.

H Empieza cerrando la sesión que tienes abierta como *Administrador* en la máquina Windows Server 2003, ya que todas las operaciones vas a realizarlas desde la máquina cliente.

En este apartado de la práctica trataremos de dar respuesta a las siguientes preguntas. ¿Quién puede instalar software en un sistema Windows Server 2003? Una vez que un nuevo paquete software ha sido instalado, ¿quién puede utilizarlo? ¿Es posible que un usuario normal (sin privilegios administrativos) pueda desinstalar un paquete de software, o dañarlo accidental o malintencionadamente? Para llevar a cabo las pruebas necesarias utilizaremos un paquete software ampliamente conocido, se trata de WinZip.

H Vas a iniciar una nueva sesión en el sistema utilizando la herramienta *Conexión a escritorio remoto* en la máquina cliente. Utiliza el usuario PTC, que no tiene privilegios de administración, pero sí puede acceder al sistema en forma remota.

A partir de aquí realizarás todas las operaciones de este apartado desde el escritorio remoto de la máquina cliente.

H Conéctate a la carpeta de la asignatura. En ella puedes observar el programa `Winzip90.exe`, que es el programa de instalación de una versión *freeware* de WinZip. Copia este fichero en la carpeta *TecnologiaComp*, ya que PTC tiene permisos para escribir en esta carpeta. Ahora intenta ejecutar este programa. Observarás que se produce un mensaje de error indicando que este programa sólo podrá ser instalado por un usuario con privilegios de administración.

Esta primera prueba nos indica que los usuarios que no tienen privilegios de administración no pueden instalar software en un sistema Windows Server 2003.

H Cierra la sesión que tienes abierta como PTC e inicia una nueva sesión como *Administrador* (recuerda que estás trabajando desde la máquina cliente). Entonces ejecuta de nuevo `Winzip90.exe`. Ahora observarás que se ejecuta sin problemas, ya que el *Administrador* tiene privilegios para llevar a cabo cualquier operación en el sistema. Lo primero que pregunta el programa de instalación es la ruta en la que se desea instalar el programa. Anota a continuación la ruta de instalación por defecto:

–Pregunta 17–

Pulsa *OK* para validar la ruta por defecto. Continúa con la instalación normalmente. Cuando el programa de instalación te pregunte, elige el modelo de funcionamiento *Classic* y el modelo de instalación *Express*. Una vez completada la instalación, observarás un icono de acceso directo a WinZip en el escritorio. Abre el menú *Programas* y observa también que se ha creado un grupo de programas para WinZip, que te permitirá ejecutarlo, desinstalarlo y obtener ayuda e información diversa acerca de él.

H Ahora mismo eres el administrador del sistema. Si inicias una nueva sesión con un usuario distinto, ¿tendrá dicho usuario el icono de acceso directo a WinZip en el

escritorio? ¿Tendrá el grupo de programas WinZip en su menú *Programas*? Usando el botón derecho del ratón explora las propiedades del icono de acceso directo a WinZip y de los elementos del grupo de programas WinZip y trata de contestar a las preguntas anteriores explicando por qué.

–Pregunta 18–

H Cierra la sesión como *Administrador* e inicia una nueva sesión como PTC y comprueba tu respuesta anterior.

Entonces, ahora eres el usuario PTC, es decir, un usuario normal, perteneciente al grupo usuarios y sin privilegios de administración. Vamos a ver qué puede hacer este usuario con el programa WinZip.

H En primer lugar comprueba que puedes ejecutarlo. Para ello puedes utilizar el acceso directo del escritorio. Ahora comprueba que también tienes acceso a la carpeta `C:\Archivos de programa\WinZip`, que es en la que se ha instalado WinZip. Abre esta carpeta. El fichero ejecutable correspondiente al programa WinZip se llama WINZIP32. Pulsa sobre él y comprueba que se ejecuta.

Hasta aquí todo normal. Si iniciases una nueva sesión con cualquier otro usuario de los creados en la sección 1 de esta práctica, también podrías ejecutar el programa WinZip sin ningún problema. Vamos a ver la explicación técnica de por qué esto es así.

H Abre la ficha *Seguridad* de la carpeta *WinZip*. Escribe a continuación los miembros de su ACL:

–Pregunta 19–

Observa que uno de los grupos de la ACL es *Usuarios*. Toma nota de los permisos que el grupo *Usuarios* tiene concedidos sobre la carpeta WinZip.

–Pregunta 20–

Recuerda también que cuando se crea un usuario nuevo en el sistema se añade por defecto al grupo *Usuarios*. Teniendo en cuenta los permisos concedidos a este grupo sobre la carpeta *WinZip*, todos los usuarios del sistema podrán acceder a esta carpeta y ejecutar los programas que se encuentren en ella.

Hasta aquí todo normal. El *Administrador* del sistema instala un programa y todos los usuarios tienen acceso a ese programa. Sin embargo, ¿podrán los usuarios hacer alguna operación más con el programa, como por ejemplo, desinstalarlo? ¿Podrán accidental o malintencionadamente eliminar algún elemento del programa?

H Empezaremos por probar la operación de desinstalación. Intenta desinstalar WinZip utilizando la herramienta *Agregar o quitar programas* del *Panel de Control*. Observarás que no puedes hacerlo. El sistema te indica que necesitas privilegios de administración para desinstalar.

H Abre la carpeta *WinZip* y trata de eliminar cualquier archivo. Observa que se te deniega el acceso.

La conclusión es que la carpeta *WinZip* esta protegida de los usuarios normales. En resumen, **los usuarios sin privilegios de administración pueden acceder al software y ejecutarlo, pero no pueden dañarlo ni desinstalarlo**.

¿Cómo se consigue que la protección del software funcione de una manera tan simple? La respuesta está en la carpeta *Archivos de programa* y en el mecanismo de herencia de permisos. Los paquetes software se instalan por defecto en la carpeta *Archivos de programa*. Si esta carpeta se configura con una ACL y unos permisos apropiados, ambos (ACL y permisos) se propagan a todo el software que se instale en esta carpeta.

H Abre la ficha *Seguridad* de la carpeta *Archivos de programa*. Observa su ACL. Indica a continuación los permisos que tienen concedidos los usuarios del grupo *Administradores* y los del grupo *Usuarios*.

–Pregunta 21–

Permisos grupo *Administradores*:
Permisos grupo *Usuarios*:

La carpeta *WinZip* ha heredado su ACL y sus permisos de la carpeta *Archivos de programas*. Gracias esto, cuenta con los permisos apropiados para que los usuarios puedan ejecutar su software, pero no puedan dañarlo.

H Cierra la sesión que tienes abierta como PTC en la máquina cliente.

A partir de ahora, salvo donde se indique lo contrario, no trabajarás mediante escritorio remoto en la máquina Windows Server 2003, sino mediante la propia consola del sistema.

5 Posesión de archivos y carpetas

En la práctica anterior hicimos una distinción entre el SD (Security Descriptor) y la ACL de un objeto. Así se indicó que la ACL es parte del SD. En este apartado vamos a presentar un nuevo componente del SD. Se trata del *Propietario*. El propietario se encontrará normalmente en la ACL del objeto, pero esto no tiene por qué ser siempre así. El propietario de un objeto es el usuario que lo crea, pero el propietario puede cambiarse. Empecemos viendo cómo ver el propietario de un objeto.

H Inicia una sesión como PTC (recuerda que estás ahora en la consola de la máquina Windows Server 2003). Usando el *Bloc de notas* crea un archivo, llámalo `prueba3.txt` y almacénalo en la carpeta *TecnologiaComp*. Para ver el propietario del archivo, abre la ficha *Seguridad*, pulsa sobre el botón *Opciones avanzadas* y, después, abre la ficha *Propietario*. En la parte superior de esta ficha se encuentra una entrada denominada *Propietario actual de este elemento*. En esta

entrada se indica el propietario del objeto, que en este caso debe ser PTC, porque es el que ha creado el fichero.

¿Qué importancia tiene el propietario de un objeto? Pues tiene mucha importancia, ya que el propietario, aunque no se encuentre en la ACL del objeto, tiene la potestad de modificar sus propiedades. Vamos a probar esto.

H Abre la ficha *Seguridad* de `prueba3.txt`. Elimina todos los miembros de la ACL del fichero. Un mensaje indica que nadie podrá acceder al fichero salvo el propietario.

H Comienza una nueva sesión como Administrador. Abre la carpeta *TecnologiaComp*. Intenta abrir `prueba3.txt`. No puedes aunque seas administrador, ya que éste no estás en la ACL del fichero. Vamos a ver qué ocurre con las propiedades de seguridad del fichero. Abre la ficha *Seguridad*. Puedes abrirla, pero todas sus opciones se encuentran deshabilitadas. No puedes hacer que el objeto herede permisos, ni tampoco puedes utilizar el botón *Agregar*. Así que el *Administrador* poco puede hacer con este archivo.

En principio, sólo el propietario del archivo podrá modificar su ACL y, así, volver a conceder permisos de acceso sobre el archivo. (Luego veremos cómo los administradores pueden saltarse esta restricción.) Comprobemos ahora cómo el propietario toma de nuevo el control del archivo.

H Inicia una nueva sesión como PTC. Intenta abrir el fichero `prueba3.txt`. Se deniega el acceso. El hecho de que PTC sea el propietario del fichero no le da ningún derecho sobre el fichero, salvo el de poder cambiar sus propiedades de seguridad. Como ahora PTC no está en la ACL del fichero (la ACL está vacía), no puede acceder a él. Sin embargo, al ser el propietario sí va a poder modificar las propiedades de seguridad. Abre la ficha *Seguridad*. Observa que ahora sí puedes utilizar por ejemplo el botón *Agregar*. Agrega el usuario PTC a la ACL del fichero y dale *Control total*. En este momento el propietario ha recuperado el control total del objeto (y ha podido recuperar el control porque es el propietario). Comprueba que ahora puedes abrir el fichero.

La conclusión de las pruebas anteriores es que **un objeto siempre tiene un propietario, y que el propietario siempre tiene la capacidad de modificar las propiedades de seguridad del objeto, aunque no se encuentre en su ACL**.

H Antes de pasar al apartado siguiente, modifica de nuevo la ACL de `prueba3.txt` dejándola completamente vacía.

El administrador y la toma de posesión

Antes hemos visto que si en la ACL de un objeto no se encuentra al administrador, éste no podrá llevar a cabo ninguna operación con el objeto. Esto es así sólo hasta cierto punto. Es cierto que, en principio, el administrador no tiene acceso al objeto, pero tiene un recurso que puede abrirle completamente las puertas del objeto. Este recurso administrativo recibe el nombre de *Toma de posesión*. Esto significa que el Administrador puede hacerse el propietario de cualquier objeto que haya en el sistema. Una vez que se ha convertido en propietario, podrá concederse los permisos que desee sobre el objeto y tomar completamente su control. Veamos cómo funciona este mecanismo de la toma de posesión.

En los ejercicios anteriores has dejado completamente vacía la ACL de `prueba3.txt`. En esas condiciones el administrador no puede hacer ninguna operación con dicho fichero. Vamos a hacer que tome posesión de él.

H Inicia una nueva sesión como *Administrador*. Abre la ficha *Seguridad* de `prueba3.txt`. Como se vio anteriormente, todo está desactivado en la ficha (ya que el administrador no está en la ACL del fichero), salvo el botón *Opciones Avanzadas*. Este botón es quien nos permitirá llegar hasta la ficha *Propietario* en la que el *Administrador* podrá tomar posesión. Pulsa sobre *Opciones Avanzadas*. Elige la ficha *Propietario*. En esta ficha puedes observar el cuadro de diálogo *Cambiar propietario a:*. En él se indican los usuarios y grupos que pueden pasar a ser el nuevo propietario del objeto. Cuando el usuario que está manejando el sistema es el *Administrador*, en este cuadro de diálogo, sea cual sea el objeto al que pertenezca, siempre se muestran las mismas entradas: *Administrador* y *Administradores*. Repito, esto solo se cumple cuando el usuario que maneja el sistema es un administrador. Para tomar posesión se elige una de las entradas y se pula *Aceptar*. En tu caso elige *Administradores* y toma posesión. Observarás que el nuevo propietario del objeto pasa a ser *Administradores*. A partir de este momento, el administrador recupera el control del objeto. Cierra la ventana *Propiedades* del objeto para que los cambios tengan efecto. Vuelve a abrirla. Elige la ficha *Seguridad* y observa cómo ahora el administrador tiene control total sobre esta ficha. Por ejemplo, se encuentra activo el botón *Agregar*. Usa este botón para agregar el grupo *Administradores* a la ACL del objeto. Una vez agregado dale permisos de lectura. Ahora comprueba que puedes abrir el fichero.

La conclusión es que mediante la toma de posesión un administrador puede tomar el control total de cualquier objeto del sistema.

6 Eliminación de usuarios y grupos

Analizaremos ahora cómo se debe llevar a cabo la eliminación de usuarios y grupos, así como algunas consecuencias interesantes derivadas de su eliminación.

Hay algunos usuarios con los que todavía no hemos hecho nada en esta práctica, como por ejemplo AFC2. Como este usuario no ha comenzado ninguna sesión, todavía no se ha creado su perfil. Vamos a crearlo.

H Inicia una nueva sesión como AFC2. Comprueba que en la carpeta *Documents and settings* se ha creado la carpeta *AFC2*, correspondiente al perfil de dicho usuario.

Ahora, la primera comprobación que vamos a hacer es que la eliminación de un usuario no implica la eliminación de su perfil. Vamos a comprobar esto eliminando el usuario AFC2.

H Inicia una nueva sesión como *Administrador*. Utilizando la herramienta *Administración de equipos*, borra el usuario AFC2. Comprueba, sin embargo, que la capeta correspondiente a su perfil no se ha eliminado. Para eliminar el perfil tendrás que borrarlo como se borra cualquier otra carpeta. Borra entonces la carpeta correspondiente al perfil de AFC2.

La conclusión de la prueba anterior es que para llevar a cabo la correcta eliminación de los usuarios del sistema, no basta con eliminar las cuentas de usuario, hay que eliminar también sus perfiles.

Vamos a analizar ahora cómo afecta la eliminación de usuarios y grupos a la ACL de los objetos. Tomaremos como ejemplo la carpeta *FundamentosComp*.

H Abre la ficha *Seguridad* de la carpeta *FundamentosComp* y toma nota de los miembros de su ACL:

–Pregunta 22–

Veamos qué ocurre con esta ACL si se elimina del sistema alguno de sus miembros. Empezaremos eliminado el usuario PFC.

H Utilizando la herramienta *Administración de equipos* elimina el usuario PFC. A continuación elimina la carpeta correspondiente a su perfil.

Veamos ahora cómo ha afectado la eliminación de PFC a la ACL de *FundamentosComp*.

H Abre la ficha *Seguridad* de *FundamentosComp*. Observa que el usuario PFC ya no se encuentra en su ACL. En su lugar aparece una larga cadena de números, que comienzan con una 'S'. Dicha cadena es el SID del usuario PFC.

El experimento anterior pone de manifiesto que lo que almacenan las entradas de la ACL son los SIDs de los usuarios y grupos creados en el sistema. Sin embargo, con objeto de hacer más legible la ACL (ya que el SID no es directamente comprensible por el usuario), la interfaz de Windows presenta en la ACL el nombre de usuario o grupo asociado a cada SID. Ahora bien, cuando el usuario o grupo asociado a un SID es eliminado del sistema, no se pude llevar a cabo la asociación SID/usuario o SID/grupo, y se representa directamente el SID. Dichas entradas de la ACL son inútiles, porque no se corresponden con ningún usuario o grupo en el sistema.

La idea final es que las entradas del tipo "S-1-5-21-13124455-..." mostradas en la ACL de un objeto corresponden a usuarios o grupos que alguna vez formaron parte del sistema, pero que han sido eliminados.

H Elimina el grupo *AFC* del sistema. Abre la ficha *Seguridad* de *FundamentosComp*. Comprueba que en la ACL ha desaparecido el grupo AFC, mostrándose ahora su SID.

Resta ya nada más que eliminar todos los usuarios y grupos, así como las carpetas, que han sido creados para los ejercicios de esta práctica. De esta forma dejaremos el sistema como estaba al comienzo de la práctica.

H Elimina los usuarios ATC1, ATC2, AFC1, y PTC (son los que faltan por eliminar). Recuerda que debes eliminar también las carpetas correspondientes a los perfiles. Elimina el grupo ATC. Finalmente, elimina las carpetas *TecnologiaComp*, *FundamentosComp* y *Asignaturas*.

7 Derechos de usuario

En algunos de los ejercicios anteriores hemos visto que no todos los usuarios del sistema pueden llevar a cabo todo tipo de operaciones. Por ejemplo, vimos que un administrador tiene la capacidad de instalar y desinstalar software, pero un usuario normal no puede realizar dicha operación. Lo que determina las diferentes operaciones que los usuarios o grupos del sistema pueden llevar a cabo es lo que se conoce como

Derechos de usuario. En primer lugar vamos a ver cuáles son las operaciones del sistema que requieren la concesión de derechos a usuarios o grupos. Para ello vamos a utilizar una herramienta denominada *Directiva de seguridad local*, a la que se accede a través del menú *Herramientas administrativas*.

H En este momento debes ser el usuario *Administrador*. Si no es así, inicia una sesión con este usuario. Abre *Directiva de seguridad local*. Entonces se muestra un árbol con diferentes directivas de seguridad. Abre *Directivas locales* y, dentro de ésta, *Asignación de derechos de usuario*.

Esto te muestra todas las operaciones del sistema que requieren la asignación de derechos de usuario. A la derecha del nombre de cada operación se indican los usuarios o grupos que tiene derechos asignados sobre esa operación, es decir, que pueden llevarla a cabo.

Vamos a ver algunos ejemplos de funcionamiento de los derechos de usuario. No obstante, primero, con objeto de tener unos grupos más diversificados en el sistema, vamos a hacer que los usuarios del sistema pertenezcan a grupos diferentes. En este momento, aparte del *Administrador*, quedan registrados en el sistema los usuarios *Alumno*, *AlumnoTC1* y *AlumnoTC2*. Comprueba que estos tres usuarios pertenecen al grupo *Usuarios*. Lo que haremos ahora será quitar al usuario *Alumno* del grupo *Usuarios*, ubicándolo en el grupo *Usuarios avanzados*.

H Utilizando la herramienta *Administración de equipos*, elimina *Alumno* del grupo *Usuarios* y agrégalo al grupo *Usuarios avanzados*.

El primer derecho que vamos a probar es *Permitir el inicio de sesión local*. Este derecho determina qué usuarios pueden comenzar una sesión desde la consola del propio sistema.

H Abre *Directiva de seguridad local* **à** *Directivas locales* **à** *Asignación de derechos de usuario*. Busca la directiva *Permitir el inicio de sesión local*. Pulsa sobre ella. Se abre una ventana indicando los usuarios y grupos que tienen asignada esta directiva. Indica a continuación cuáles son.

–Pregunta 23–

H Quita de esta directiva el grupo *Usuarios* y pulsa *Aceptar*. Esto hará que los miembros del grupo usuarios no puedan iniciar sesión localmente. Cierra la sesión actual e intenta comenzar otra como *AlumnoTC1*. Observarás que no puedes comenzar la sesión. El sistema indica que *Las directivas locales de este sistema no permiten iniciar una sesión interactiva*. Intenta ahora entrar como *Alumno*. Observarás que entras sin problemas, ya que *Alumno* pertenece a *Usuarios avanzados*, que sí tienen el derecho de inicio local de sesión. Cierra esta sesión de modo que no quede ninguna sesión local abierta.

El hecho de que *AlumnoTC1* no pueda iniciar sesión de forma local, no implica que no pueda hacerlo de forma remota, si su seguridad se configura de la forma adecuada. La directiva que concede el derecho de iniciar sesión de forma remota se llama *Permitir inicio de sesión a través de Servicios de Terminal Server*. Veamos que usuarios tienen asignado este derecho.

H Inicia sesión como *Administrador*. Abre *Directiva de seguridad local* **à** *Directivas locales* **à** *Asignación de derechos de usuario*. Busca la directiva *Permitir inicio de sesión a través de Servicios de Terminal Server*. Pulsa sobre ella. Indica a continuación qué grupos tienen asignado este derecho.

–Pregunta 24–

Uno de los grupos es *Usuarios de escritorio remoto*. Si agregamos *AlumnoTC1* a este grupo, adquirirá el derecho de iniciar sesión de forma remota.

H Utilizando la herramienta *Administración de equipos*, agrega el usuario *AlumnoTC1* al grupo *Usuarios de escritorio remoto*. Cierra la sesión que tienes abierta como administrador.

H Comprueba que sigues sin poder iniciar sesión localmente con el usuario *AlumnoTC1*, pero sí puedes abrir una sesión remota. Esto es debido a que ahora *AlumnoTC1* pertenece al grupo *Usuarios de escritorio remoto*, que tiene el derecho de abrir sesión de forma remota. Cierra entonces la sesión remota abierta.

En resumen, **los derechos de usuario determinan qué operaciones pueden ser llevadas a cabo por los usuarios en un sistema**.

Para terminar este apartado vamos a dejar los derechos usuario como estaban antes de llevar a cabo las modificaciones anteriores.

H Inicia una sesión como *Administrador* en la consola de la máquina Windows Server 2003. Abre *Directiva de seguridad local* **à** *Directivas locales* **à** *Asignación de derechos de usuario*. Busca la directiva *Permitir el inicio de sesión local* y agrega a ella el grupo *Usuarios*. Si tienes dificultadas al agregar este grupo, prueba con el botón *Tipos de objetos*.

H Después, utilizando la herramienta *Administración de equipos*, quita el usuario *AlumnoTC1* del grupo *Usuarios de escritorio remoto*.

Comprobemos ahora que los cambios han surtido efecto.

H Cierra la sesión como *Administrador* e inicia una nueva sesión local como *AlumnoTC1*. Comprueba que puedes entrar sin problemas y cierra la sesión.

H Intenta abrir una sesión de forma remota utilizando *AlumnoTC1*, comprobando que no puedes entrar.

Si las dos pruebas anteriores son satisfactorias, las directivas de seguridad modificadas en esta sección han sido restituidas a sus valores originales.

8 Ejercicios adicionales

E En la práctica anterior vimos que los usuarios del grupo *Usuarios* no tienen la capacidad de cambiar la hora del sistema. Haz las operaciones necesarias para que los usuarios de este grupo sí puedan cambiar la hora del sistema. Crea un usuario y comprueba que dicho usuario sí tiene en efecto este derecho. Deja las cosas cómo estaban al principio y comprueba que el usuario ha dejado de tener este derecho. Finalmente, elimina este usuario del sistema, así como su perfil.