

Práctica 11		Fecha:
Nombre ordenador multimedia:		Hora:
Alumnos		
DNI:	Nombre:	Apellidos:
DNI:	Nombre:	Apellidos:
DNI:	Nombre:	Apellidos:

Objetivos

Comprender el Registro de Windows. Manipular el registro usando las herramientas proporcionadas por Windows 2000. Manipular el Registro mediante programa.

Material necesario

Es necesario acudir al laboratorio con un disquete en blanco, en el que se guardarán los ficheros obtenidos durante la sesión de prácticas. Al finalizar la sesión el profesor recogerá los disquetes para evaluarla.

Desarrollo

1. Herramientas de manipulación del Registro

Como se ha visto en la teoría de la asignatura, Windows 2000 proporciona dos herramientas que permiten inspeccionar y manipular el Registro, **regedit.exe** y **regedt32.exe**. La utilidad regedt32 es más completa, por lo que será la utilizada durante la sesión de prácticas. De todas formas, la primera parte de la práctica pondrá de manifiesto las diferencias más evidentes entre ambos editores.

- Arrancar las aplicaciones **regedit.exe** y **regedt32.exe** utilizando el menú de Inicio

¿Cuántos documentos muestra **regedt32.exe**? ¿Cómo se relacionan con el árbol que muestra **regedit.exe**?

- Cuando se desea simplemente inspeccionar el contenido del Registro, es conveniente poner al editor en modo de sólo lectura.

¿Es posible poner en modo de sólo lectura a **regedit.exe**? ¿Cómo?

¿Es posible poner en modo de sólo lectura a **regedt32.exe**? ¿Cómo?

Aunque parece que **regedt32.exe** sólo introduce ventajas, no siempre es así. Mediante la opción Buscar del menú Edición de **regedit.exe**, busca la entrada de valor de nombre "SystemBiosDate". ¿Cuál es su ruta completa y su valor?

¿Es posible encontrar la entrada de valor anterior usando **regedt32.exe**? ¿Por qué?

2. Restricción y control del uso de la información del Registro

- El acceso a la información del registro puede restringirse de varias formas. Una de ellas es mediante **regedt32.exe**.

Utilizando la información que se obtuvo usando **regedit.exe**, arranca **regedt32.exe** y localiza la información que almacena la clave "SYSTEM". A la vista de la información que puede obtenerse usando el menú "Seguridad", ¿qué privilegios de acceso a la información almacenada en esa clave tienen los usuarios normales del equipo?

- Windows 2000 permite, mediante **directivas de seguridad local**, auditar las modificaciones del Registro. Para ello, debe estar activa la **auditoría de acceso a los objetos del sistema**.
- Abrir la carpeta *Herramientas Administrativas* del *Panel de Control*. Arrancar la consola destinada a la gestión de directivas de seguridad local. En *Directiva de auditoría*, que se encuentra en el grupo *Directivas locales*, activar la auditoría de accesos a los objetos del sistema (tanto para accesos correctos como para accesos erróneos).
- A continuación se activará la auditoría de una clave del Registro y, para comprobar su eficacia, se modificará una clave de registro que controla el comportamiento del Símbolo del Sistema de Windows 2000. Pero antes de ello, se guardará su valor inicial.
- Ejecutar **regedit.exe** y localizar la clave "HKEY_CURRENT_USER\Software\Microsoft\Command Processor". Con la clave anterior seleccionada, elegir la opción *Exportar archivo de registro* del menú *Registro*. Guardar el archivo con el nombre **ATCXXX**, sustituyendo las **XXX** por el número del equipo en el que se esté trabajando.

¿Qué extensión se le asigna por defecto al archivo que acaba de guardarse?

¿Qué operación por defecto lleva a cabo el Explorador de Windows con estos archivos? (Pulsa con el botón derecho sobre el archivo generado, e incluye a continuación la opción que se muestra en negrita).

Selecciona la opción *Edición* e incluye a continuación el contenido del archivo.

- Fíjate en el valor de "CompletionChar".
- Ejecutar **regedt32.exe** y localizar la clave "HKEY_CURRENT_USER\Software\Microsoft\Command Processor". Utilizando el menú *Seguridad*, opción *Permisos*, y pulsando el botón *Avanzada*, activar la auditoría de la consulta o la modificación (con éxito y sin él) de las subclaves de "Command Processor" para todos los usuarios.
- Arrancar una sesión del Símbolo del Sistema de Windows. Cambiar a la unidad de disco del sistema y teclear "cd Archi". A continuación pulsar "TAB". No debería ocurrir nada "especial". Cerrar la ventana y volver a regedt32.exe. Modificar el valor de "CompletionChar" a "9".

Arrancar una sesión del Símbolo del Sistema de Windows. Cambiar a la unidad de disco del sistema y teclear "cd Archi". A continuación pulsar "TAB". ¿Qué ocurre?

- Arrancar el Visor de sucesos de Windows 2000 (**eventvwr.exe**) y borrar todos los sucesos del *Registro de seguridad* hasta el momento (así será más fácil identificar los sucesos nuevos).
- Hacer doble clic sobre el archivo **ATCXXX.reg** para restaurar el valor de la clave.

Si la auditoría se activó correctamente, la modificación del valor de "CompletionChar" debió quedar registrada. Comprueba si en los sucesos de la sección "seguridad" aparece. Usando

toda la información de la que dispones, averigua el **identificador de operación** de la modificación, e inclúyelo a continuación.

- Antes de continuar, desactiva la auditoría tanto en las opciones de seguridad locales como en el Registro.

3. Copias de seguridad del Registro

Dado que la información almacenada en el Registro del equipo es crítica, Windows 2000 permite crear copias de seguridad del Registro de forma sencilla.

- Ejecutar la utilidad *Copia de Seguridad*, que forma parte de las herramientas del sistema proporcionadas por Windows 2000. En el menú *Herramientas*, seleccionar *Crear un disco de reparación de emergencia*, y completar la creación de un disco a la vez que se guarda una copia del Registro en el directorio de reparaciones del sistema.

¿Cómo se llama el directorio en el que se guarda la copia de los archivos asociados al Registro? (El directorio buscado incluye la cadena "RegBack")

4. Manipulación del Registro mediante archivos .INF

Puesto que el Registro es una fuente primordial de información para las aplicaciones instaladas en un equipo, los *archivos de información de instalación* o archivos .INF permiten no sólo controlar la copia de archivos a los directorios del equipo, sino manipular el registro de forma sencilla.

El alumno modificará a continuación un archivo .INF para conseguir instalar y registrar un programa, que se ejecutará en cada inicio de sesión.

- Ejecutar Visual Studio y crear una aplicación de consola que imprima “**Hola, usuario de ATCXXX**”, siendo **ATCXXX** el nombre del equipo inestable en el que se está trabajando. El nombre del ejecutable obtenido será **ATCXXX.exe**. Copiar el ejecutable al disquete de la práctica.
- Preguntar al profesor de prácticas la ubicación del archivo **ATCXXX.inf** y copiarlo al disquete. Debe cambiarse el nombre de dicho archivo siguiendo los criterios mencionados y modificarlo de forma adecuada para que instale (desde el disquete) y registre como programa de inicio el ejecutable obtenido en el punto anterior. Para que durante la instalación se reconozca el disquete, se debe crear en su directorio raíz un archivo llamado **ATCXXX** (sin extensión) que debe estar vacío. Para probar si funciona el .INF creado, bastará hacer clic con el botón derecho sobre el archivo .INF y elegir la opción *Instalar*.

- Comprobar la clave Run con el editor del registro, que se ha creado el directorio seleccionado y que en él fue copiado el ejecutable creado. Salir de la sesión y volver a entrar para probar si funciona.
- Borrar la clave del registro, el archivo y el directorio.

5. Manipulación del Registro mediante programa

El archivo también puede modificarse mediante programa, usando funciones de la API del sistema.

- Ejecutar Visual Studio y crear una aplicación de consola que imprima “**Hola otra vez, usuario de ATCXXX**”, siendo **ATCXXX** el nombre del equipo inestable en el que se está trabajando. Tras mostrar el mensaje anterior, el programa debe modificar el registro para que sea ejecutado cada vez que se inicie una sesión en el equipo.
- Copiar el archivo fuente y el ejecutable al disquete de la práctica, y entregárselo al profesor de prácticas para su evaluación.
- Comprobar que en el equipo no queda ninguno de los ficheros generados durante la práctica, y que el registro no tiene ninguna de las claves añadidas durante la práctica.