Práctica 10		**Fecha:**
Nombre ordenador par:		**Hora:**
Alumnos		
DNI:	Nombre:	Apellidos:
DNI:	Nombre:	Apellidos:

Objetivos

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

Material necesario

El alumno no necesita ningún material aparte del que le será proporcionado en el laboratorio.

Desarrollo

1. El editor del Registro

Windows proporciona una herramienta que permite inspeccionar y manipular el Registro: el editor del registro.

- Arrancar en el ordenador par la aplicación **regedit.exe** utilizando Inicio->Ejecutar.
- ¿Cuántos árboles muestra? ¿Cuáles son los dos principales?

- Si insertas una entrada de valor nueva, ¿qué tipos te permite asignar el editor?

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

El acceso a la información del registro puede restringirse de varias formas.

Localiza la información que almacena la clave SYSTEM. A la vista de la información que puede obtenerse usando el menú Edición->Permisos, ¿qué privilegios de acceso a la información almacenada en esa clave tienen los usuarios normales del equipo?

- Windows 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 (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. Pero antes de ello, se guardará su valor inicial.

- Localiza en el editor del Registro la clave HKEY_CURRENT_USER\Software \Microsoft\Command Processor. Con la clave anterior seleccionada, elegir la opción *Exportar* del menú *Archivo*. 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".

- Utilizando el menú *Edición*, opción *Permisos*, y pulsando el botón *Opciones Avanzadas*, agregar el grupo *Todos* y activar la auditoría (con éxito y sin él) de la consulta y el establecimiento del valor de las subclaves de "Command Processor".

- Arrancar una sesión del Símbolo del Sistema de Windows. Cambiar a la raíz del sistema y teclear "cd Archi". A continuación pulsar la tecla de tabulación. Debería completarse la ruta. Cerrar la ventana y volver al editor del registro.exe. Modificar el valor de "CompletionChar" a "0".

Arrancar una nueva sesión del Símbolo del Sistema de Windows. Cambiar a la raíz del sistema y teclear "cd Archi". A continuación pulsar la tecla de tabulación. ¿Qué ocurre?

- Arrancar el Visor de sucesos de Windows (**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 suceso** en el que se ha accedido a la clave para fijar su valor, e inclúyelo a continuación.

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

3. Manipulación del Registro mediante programa

El registro también puede modificarse mediante programa, usando funciones de la API del sistema. En esta parte de la práctica vas a desarrollar un programa en el Visual Studio del ordenador impar que se va a ejecutar en el ordenador par.

- Ejecutar Visual Studio. Crear un proyecto nuevo en C++ de tipo "Aplicación de consola". Ir a las propiedades del proyecto. En el cuadro de diálogo que te aparece, escoger *Opciones generales de configuración->C/C++ ->Generación de código* y en la opción *Biblioteca en tiempo de ejecución*, escoger *Depuración multiproceso (/MTd)*.

- Hacer que el programa imprima "**Hola, usuario de ATCXXX**", siendo **ATCXXX** el nombre del equipo par 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, para lo que necesitará modificar una clave del Registro, ¿cuál?

- Crear un archivo comprimido con el código fuente y el ejecutable y entregárselo al profesor siguiendo el método que indique.

- Comprobar que en el equipo no queda ninguno de los ficheros generados durante la sesión, y que el registro no tiene ninguna de las claves añadidas durante la práctica.