6-3-2020

Aarón Cañamero Mochales

Las naves salesianos

Registro de Windows

[Explicación: 2](#_Toc34378782)

[HKEY\_CURRENT\_USER: 3](#_Toc34378783)

[HKEY\_LOCAL\_MACHINE: 4](#_Toc34378784)

[HKEY\_CLASSES\_ROOT: 5](#_Toc34378785)

[HKEY\_CURRENT\_CONFIG: 6](#_Toc34378786)

[HKEY\_USERS: 7](#_Toc34378787)

Explicación:

El registro de Windows es un conjunto de archivos que contienen información acerca de cómo funciona el equipo.

Windows tiene una base de datos jerárquica donde almacena su propia configuración, la del hardware, la de las aplicaciones instaladas y la personalización de cada usuario.

La información en el registro se ordena en un sistema de árbol como las carpetas y ficheros, muy parecido al explorador.

La información se guarda en claves, que pueden tener subclaves, como las carpetas y subcarpetas.

El registro de Windows está divido en 5 secciones:

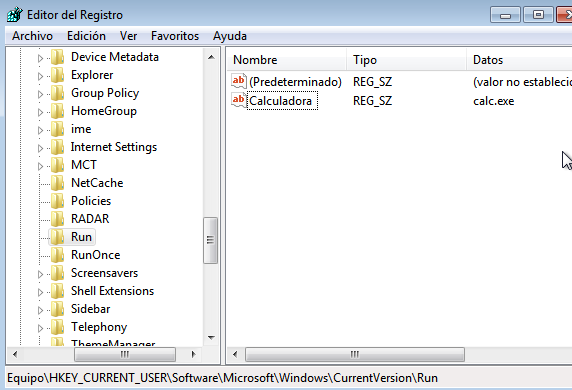
1. HKEY\_CURRENT\_USER
2. HKEY\_LOCAL\_MACHINE
3. HKEY\_CLASSES\_ROOT
4. HKEY\_CURRENT\_CONFIG
5. HKEY\_USERS

HKEY\_CURRENT\_USER:

Contiene la información de configuración del usuario que ha iniciado sesión.

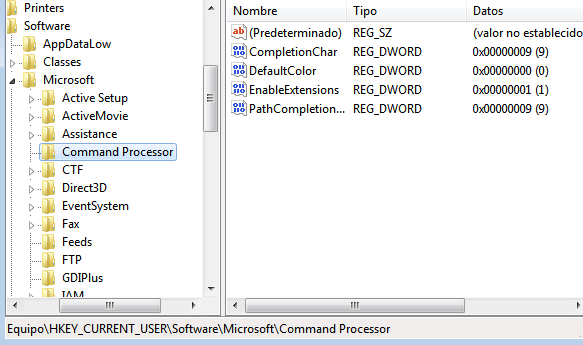
Esta clave a veces aparece abreviada como HKCU.

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

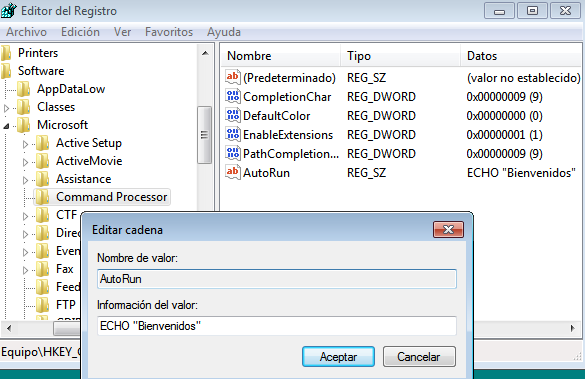


Desde aquí podemos ver los programas que se inician con el sistema en este caso nosotros hemos añadido uno, en el panel derecho creamos un nuevo valor de cadena llamado en este caso Calculadora y le ponemos el valor calc.exe y siempre que iniciamos el sistema se abrirá la calculadora, también tenemos varias opciones de configuración, también lo podemos eliminar si queremos.

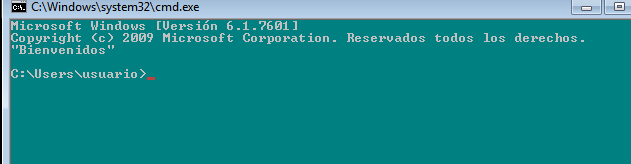
HKEY\_CURRENT\_USER\Software\Microsoft\CommandProcessor



En esta ruta encontramos la configuración de nuestro CMD en el sistema dentro de aquí vamos ha crear un mensaje de bienvenida, con el clic derecho sobre el panel derecho creamos un nuevo valor de cadena.

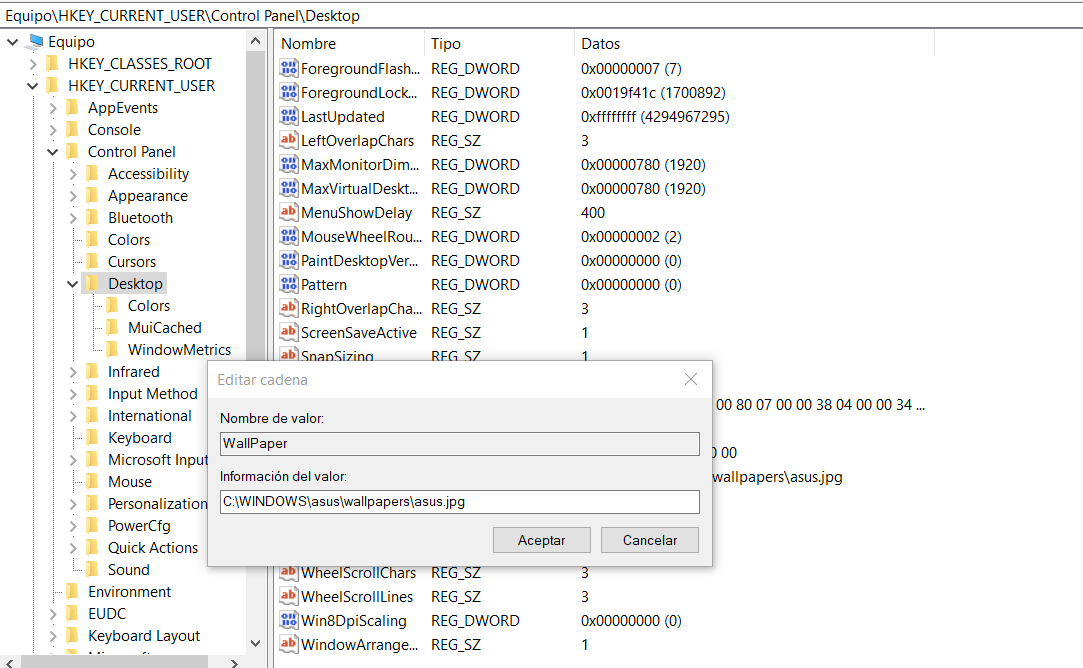


Aquí le llamamos AutoRun y escribimos el comando ECHO “Bienvenidos” esto es para cerrar y abrir el texto que vamos a escribir con el comando, también podemos cambiar y modificar las diferentes opciones del CMD.



Aquí vemos como se ha creado el mensaje correctamente, no hace falta poner las comillas, para que funcione el AutoRun.

HKEY\_CURRENT\_USERS\Control Panel\Desktop



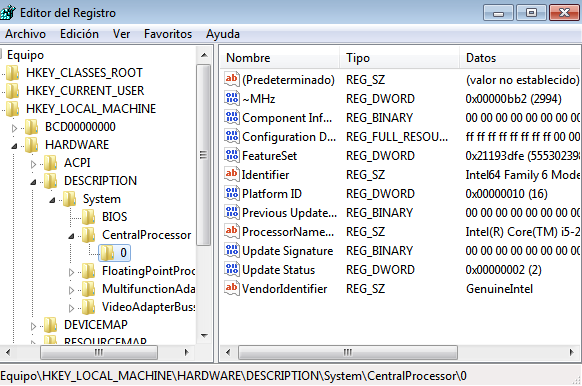
En la ruta siguiente entramos en la configuración y opciones de nuestro escritorio desde el panel de control, en este caso vamos a ver el WallPeper de nuestro escritorio es decir el fondo de pantalla y vemos que en la información del valor nos pone la ruta de la imagen y la imagen que es y su extensión.

HKEY\_LOCAL\_MACHINE:

Contiene información de configuración especifica del equipo.

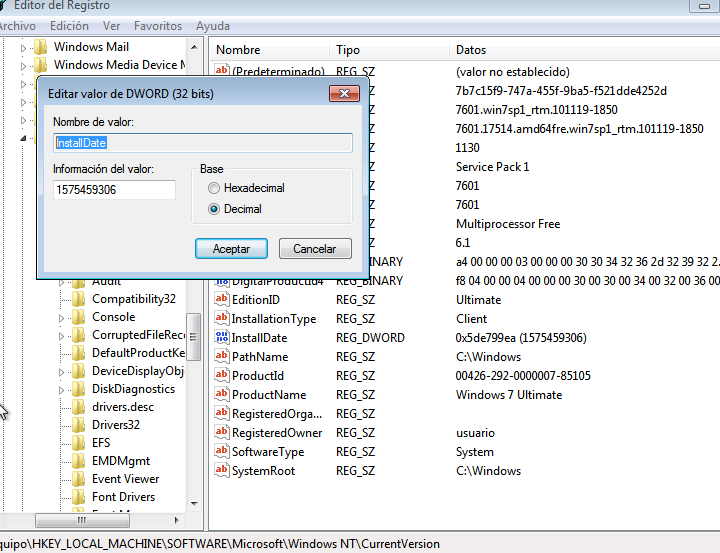
Esta clave a veces aparece abreviada como HKLM.

HKEY\_LOCAL\_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0



Aquí se despliega información que se recoge en las propiedades de Mi pc o en el Panel de control.

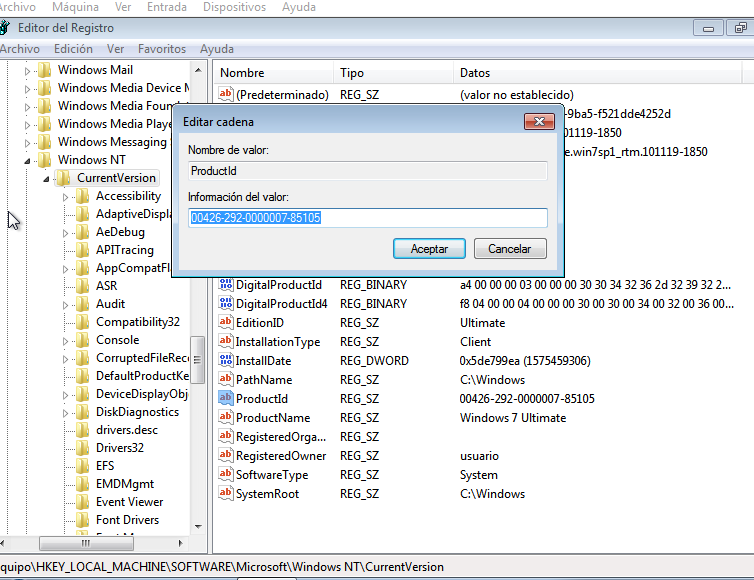
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



Aquí encontramos la fecha y hora de instalación de nuestro sistema, lo encontramos en un valor decimal, esto lo podemos pasar en cualquier conversor a hora y fecha y nos saldría los siguientes datos:

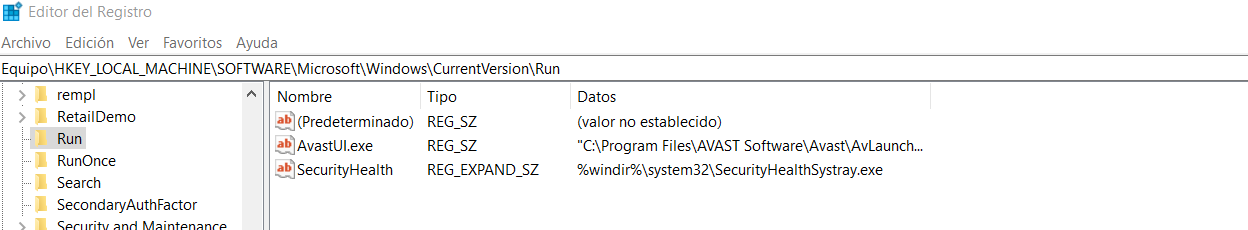


HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



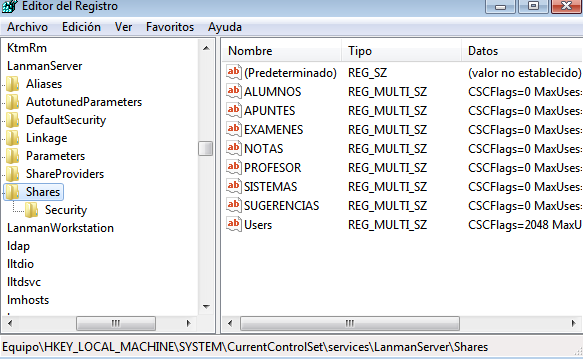
Este es el ID de producto de nuestro sistema.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

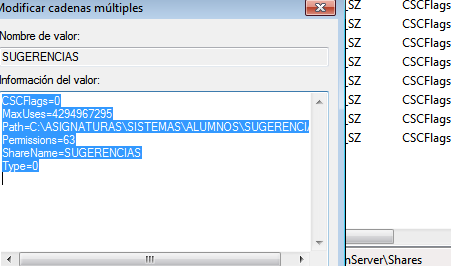


Desde esta lista podemos ver los programas que tenemos ejecutándose e inicio, así como las opciones adicionales de ejecución que se añaden al arranque de cada programa.

HKEY\_LOCAL\_MACHINE\System\CurrentConrtolSet\Services\lanmanserver\Shares

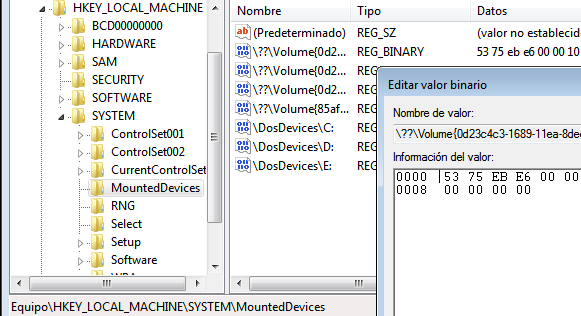


Aquí encontramos la información sobre los recursos compartidos.



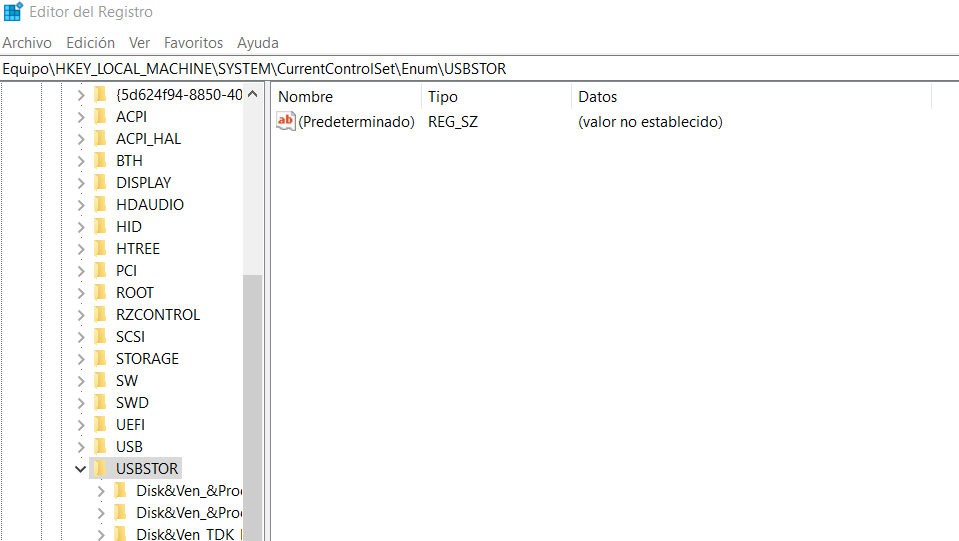
Aquí vemos toda la información relacionada con el recurso seleccionado.

HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices



MountedDevices almacena información sobre dispositivos y volúmenes montados en el sistema de archivos NTFS.

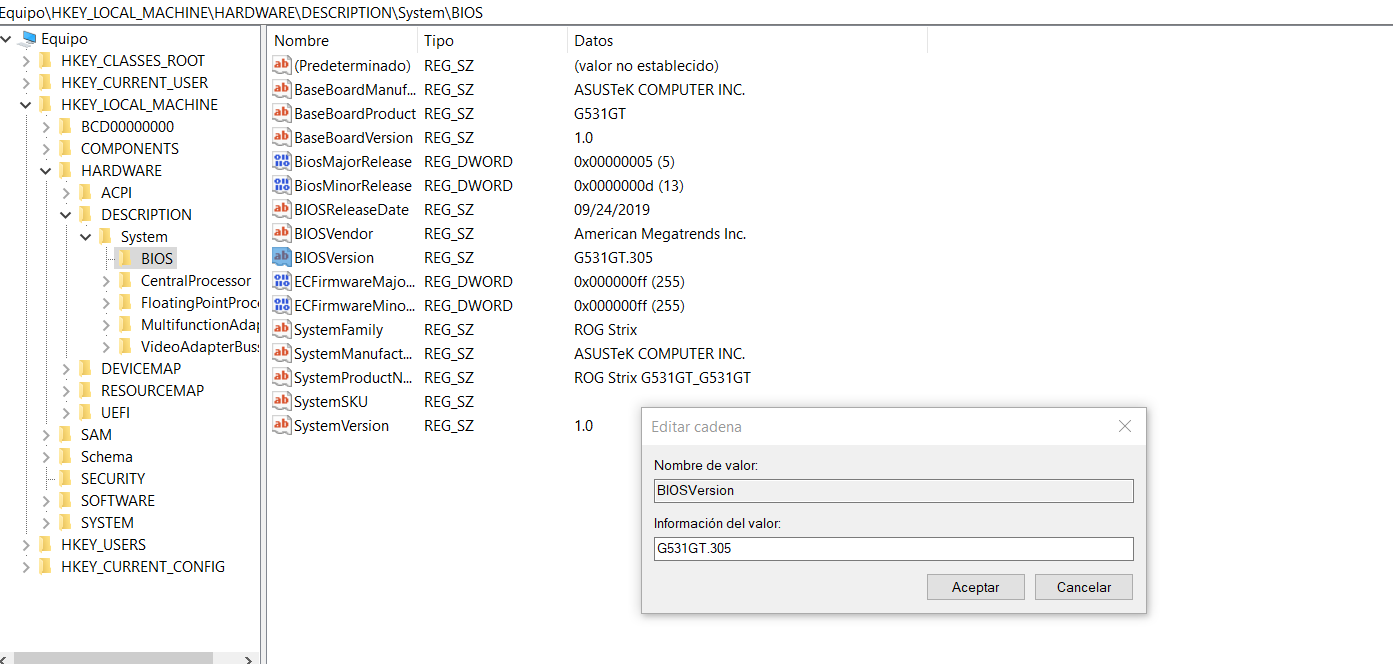
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR



Aquí se guardan los identificadores de los dispositivos USB, la clave de registro será creada debajo de la clave

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

HKEY\_LOCAL\_MACHINE\HARDWARE\DESCRIPTION\System\BIOS

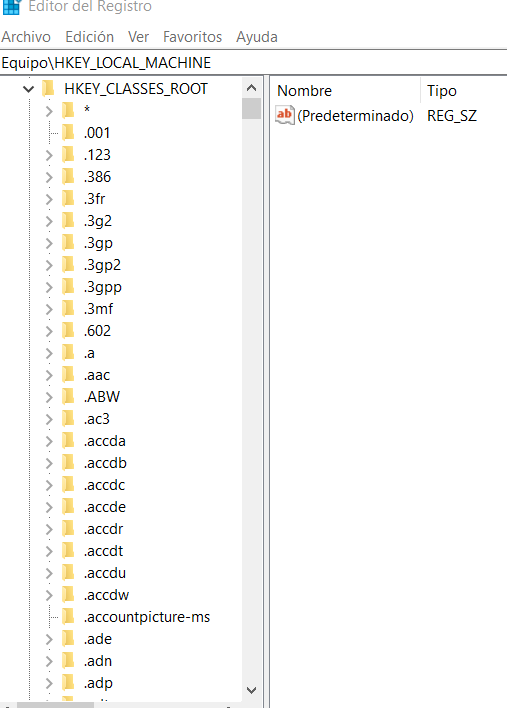


En esta ruta encontramos todo tipo de información sobre la bios, en este caso nosotros hemos entrado al tipo de versión del mismo.

HKEY\_CLASSES\_ROOT:

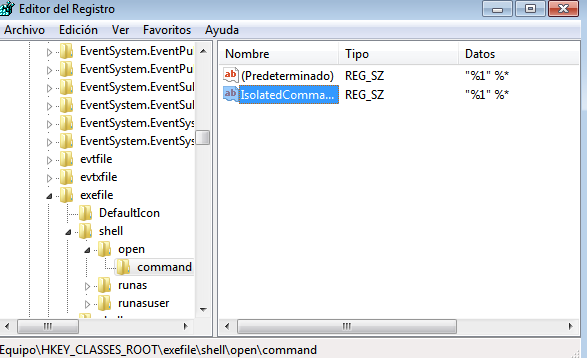
Contiene la relación entre las extensiones de archivos, y los archivos en el sistema.

También se puede encontrar en la subclave de HKEY\_LOCAL\_MACHINE\Software.



Aquí encontramos todas las extensiones, cada programa tiene su tipo de extensión, aquí encontramos la de Word .doc, .avi, etc.

HKEY\_CLASSES\_ROOT\exefile\shell\open\command

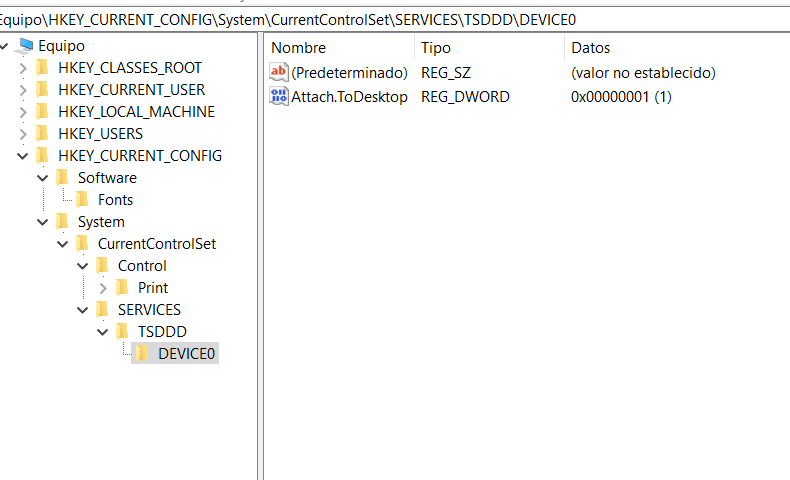


Aquí podemos encontrar si hay malware en nuestro sistema, en este caso no hay ningún tipo de Malware, también lo podemos buscar en la ruta

HKEY\_LOCAL\_MACHINE\Software\Classes\Exefile\Shell\Open\command

HKEY\_CURRENT\_CONFIG:

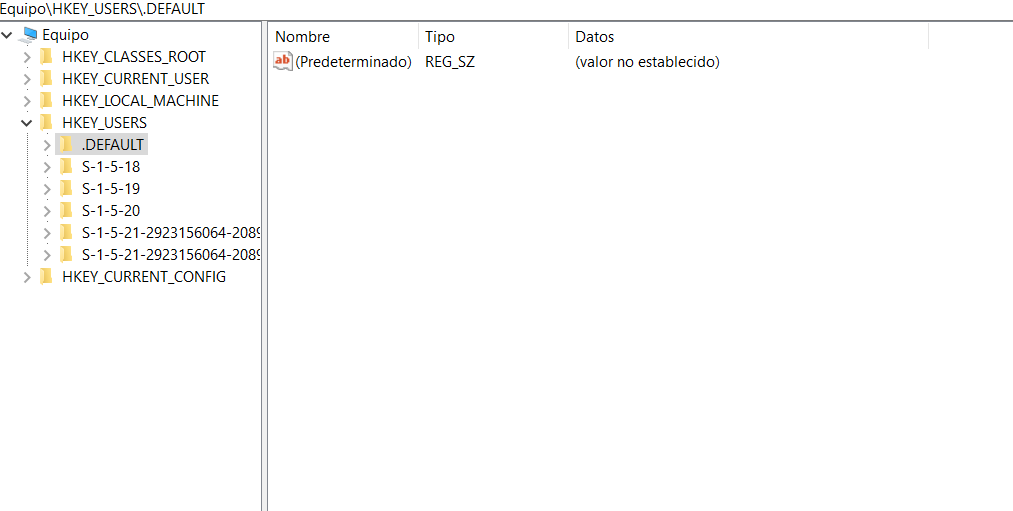
Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.



Desde este lugar podemos podemos ver la configuración de perfil Hardware que utiliza nuestro equipo local cuando se inicia el sistema.

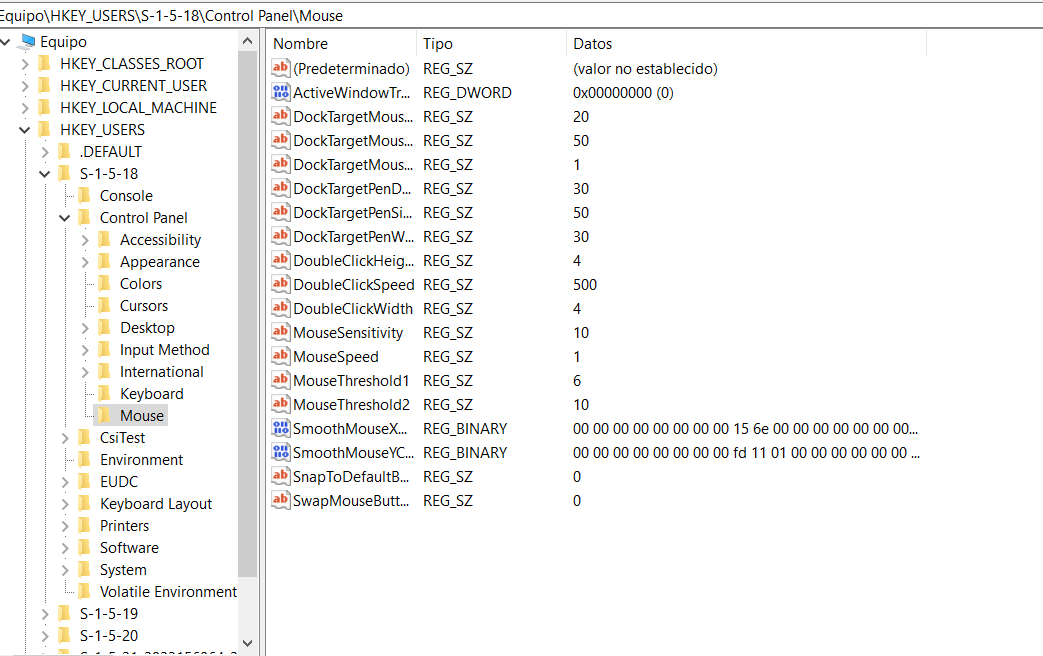
HKEY\_USERS:

Contiene todos los perfiles de usuario cargados activamente en el equipo.



Aquí encontramos los perfiles de usuario cargados en el equipo, vemos que tenemos 6 perfiles.

HKEY\_USERS\S-1-5-18\Control Panel\Mouse



Aquí encontramos la configuración del ratón en este perfil, desde los DPI, como los botones adicionales que tenga, etc.