# Práctica 6: Exploración y análisis de registros del sistema en Windows

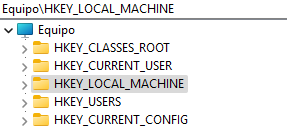
## Curso: IFCT0609 - Programación de Sistemas Informáticos

## Objetivo:

Familiarizarse con el uso de herramientas del sistema operativo Windows para acceder, identificar y describir registros del sistema relevantes para la administración y la seguridad informática.

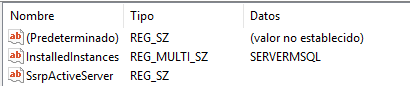
## Enunciado:

Accede al sistema operativo Windows de tu equipo y realiza las siguientes tareas:  
1. Entra al Editor del Registro ejecutando el comando regedit.  
 a. Navega por las claves principales del registro (HKEY\_LOCAL\_MACHINE, HKEY\_CURRENT\_USER, etc.).

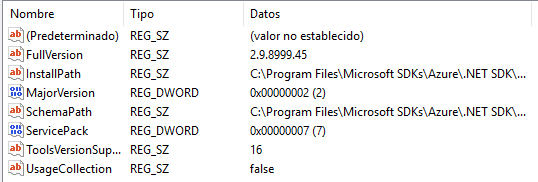


b. Selecciona dos claves y describe:  
 - Su ruta completa.

El servidor sql: Equipo\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server, almacena información de la instancia, y valores opcionales de configuracion. En este caso la instancia del servidor sql existente es clave para poder usarla en los programas que usen ese servidor de bbdd para almacenar la informacion con la que trabajan, si no estuviera indicada en el registro, no podrian usar sus bbdd hasta no tener una nueva instancia registrada



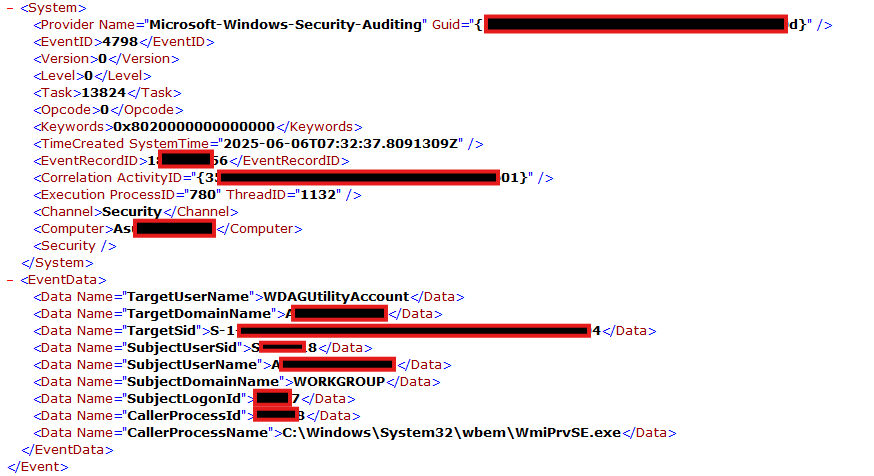
Microsoft SDK: Equipo\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft SDKs\ServiceHosting\v2.9

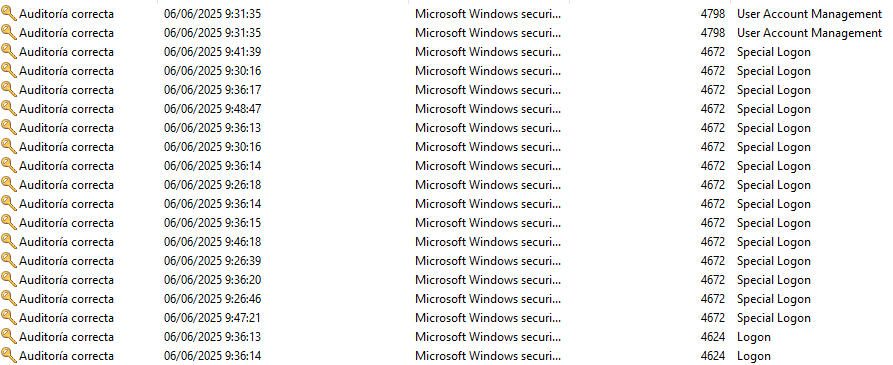


guarda la version instalada, el path de instalación, y el path de los esquemas de la bbdd de azure, asi como valores de configuracion de uso de la herramienta, al igual que la anterior estos datos son los que informan a las aplicaciones que usan sdk de los datos de configuracion que necesitan para usarlo, por ejemplo donde esta el programa, o donde estan los schemes

2. Abre el Visor de eventos desde:  
 Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos.  
 a. Accede a tres categorías de registros (por ejemplo: seguridad, sistema, aplicación).

- Eventos de Seguridad, como su propio nombre indica son eventos de seguridad, en este caso veo autenticaciones en programas, y servicios el mas reciente es en esta fecha y hora: 06/06/2025 9:36:15, en seguridad no tengo ningun evento sospechoso, y tampoco hay ninguno que destaque sobre el resto, todos los mostrados son o de categorias: logon, special logon ,o user account management, y todos Auditoria Correcta. Respecto a special logon este es el XML compatible con json





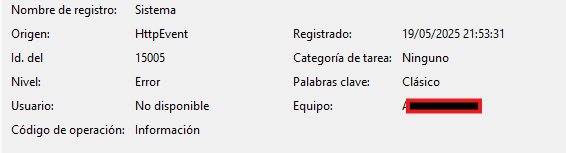
Eventos de Sistema

Estos son los eventos de los programas procesos, y servicios que maneja el sistema operativo, su vivel puede ser Informacion, Advertencia, error, y crítico, aunque en este caso solo me han salido los tres primeros

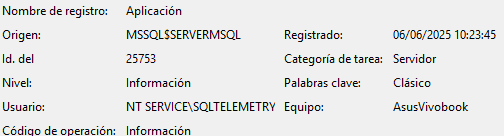
el ultimo es uno informativo en fecha y hora: 06/06/2025 9:36:21

y un evento sospechoso es un error en un evento HttpEvent indicando: No se puede enlazar con el transporte subyacente para 127.0.0.1:50094. Es posible que la lista IP de solo escucha contenga una referencia a una interfaz que no existe en este equipo. El campo de datos contiene el número de error.

La ip indicada es local, y el puerto 50094, que es un puerto privado temporal fue el dia indicado en la imagen de abajo, y tendria que hacer una auditoria de lo que hice tal día a tal hora para trazar de donde proviene el error



Eventos de Aplicacion: estos son los eventos generados por las aplicaciones que los usuarios ejecutan para su desempeño, actualmente la inmensa mayoría son de nivel información, el último ha sido en fecha y hora: 06/06/2025 10:23:45



y hay algunos sospechosos de nivel error como este de la aplicacion ShellExperienceHost.exe del día y hora: 05/06/2025 11:05:39, con esta descripción:

El programa ShellExperienceHost.exe versión 10.0.26100.3912 dejó de interactuar con Windows y se cerró. Para ver si hay más información disponible sobre este problema, comprueba el historial de problemas en el panel de control de Seguridad y mantenimiento.

3. Explica cómo pueden utilizarse estos registros para:  
 - Auditar el uso del sistema: Para Auditar un registro, hay que trazar el error con el programa, la fecha y hora indicada, el nivel, el usuario y comprobar que es un evento autorizado para el usuario, y no es erróneo, en la pestaña detalles se ve todo el requistro, si es un usuario autorizado para derlo, claro.

- Detectar fallos o accesos indebidos.

Para ello debemos conocer la politica de seguridad de la empresa, donde debe estar la lista de usuarios autorizados para las distintas aplicaciones, y servicios, se debe mantener los accesos a las aplicaciones actualizados para los usuarios de forma casi instantanea,

Por ejemplo, en caso de que un usuario intente ejecutar un programa para el que no esta autorizado debe registrarse el intento, y deben realizarse las acciones de la politica de seguridad de la empresa, que deben ser registrar dicho acceso, y avisar al usuario de que no está autorizado para lo que sea que esté intentando hacer, si aun así se repite el intento, ya se deben tomar otras medidas

- Evaluar el estado general del sistema operativo.

Para evaluar el estado general del sistema operativo, en el visor de eventos se ven los programas que estan instalados pero en mejor usar el monitor de rendimientos, donde se ve la telemetria de memoria, uso de disco y cpu, uso de wifi, etc, si se ve consumo muy alto de cpu, hay que analizar a que sedebe dicho consumo, para ver so es un proceso normal o un evento extraordinario, y evaluar su peligrosidad, recomendando en este caso contactar con el usuario y con la persona responsible de sistemas en la empresa para tomar las medidas oportunas, y modificar/actualizar la politica de uso del material informatico, si es necesario