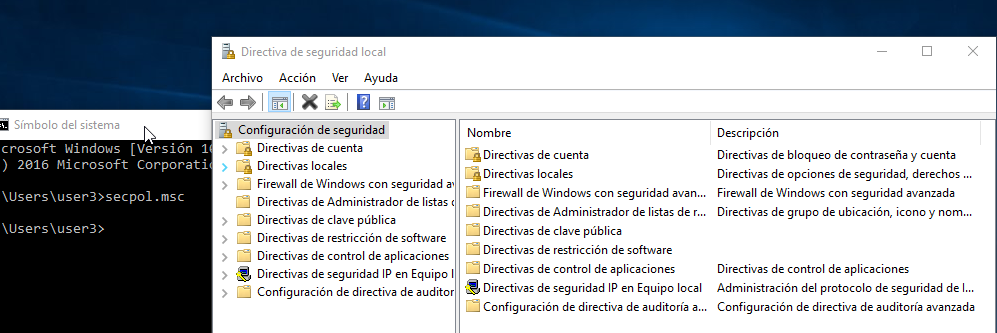
**Eventos de Seguridad.**

**1**

**Auditar el acceso a objetos**

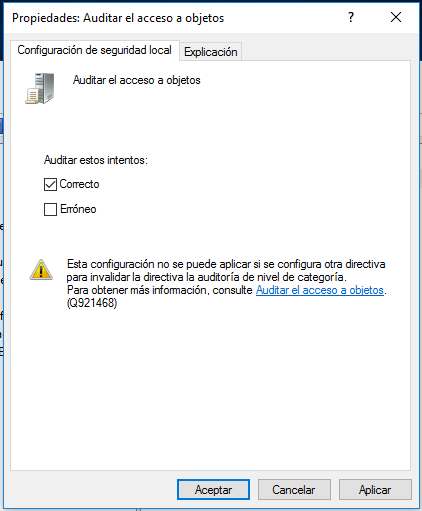
**1.1.-** Para acceder a las directivas de seguridad local ejecutamos el comando secpol.msc

**Directiva de grupo** es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. En otras palabras, la Directiva de Grupo, en parte, controla lo que los usuarios pueden y no pueden hacer en un sistema informático

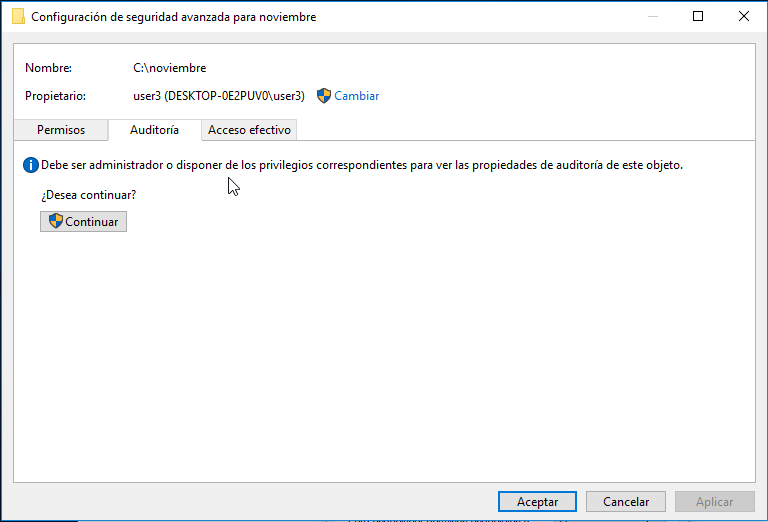


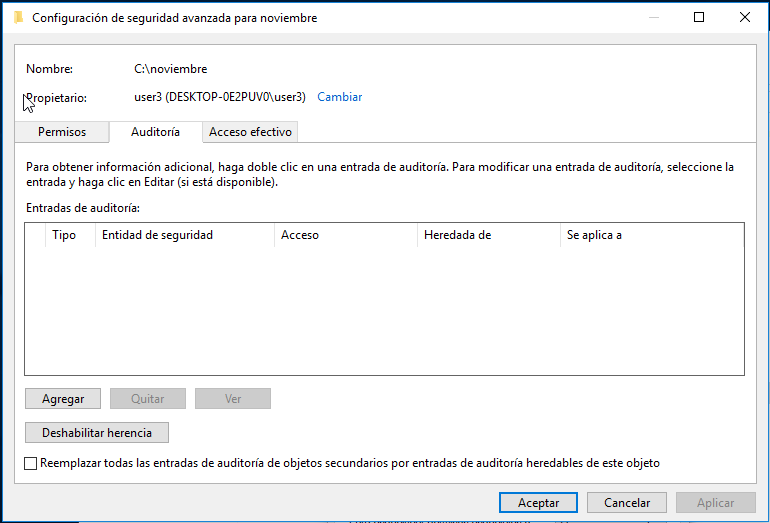
Directivas de Seguridad Local -> Directivas locales -> Directiva de auditorías -> auditar acceso a objetos.

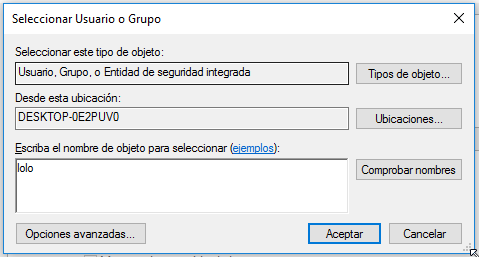
**1.2.-** Vamos a auditar los **accesos correctos y reiniciamos**

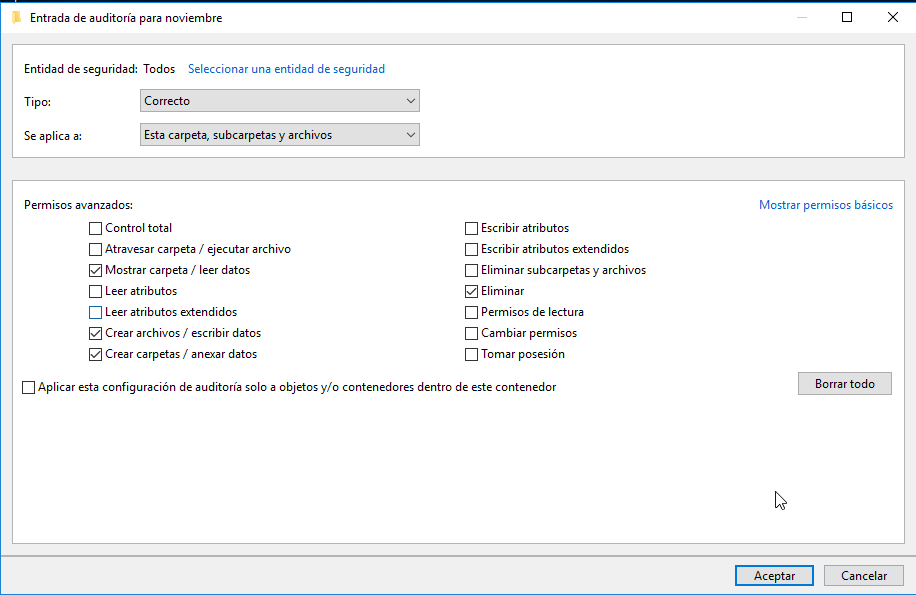


**1.3.** Escogemos la carpeta a auditar utilizando el botón derecho del ratón. Vamos a propiedades -> pestaña de seguridad -> opciones avanzadas -> auditoría y agregamos los usuarios a auditar en el acceso a la carpeta. Nosotros elegimos lolo ( o cualquier usuario de nuestro sistema).



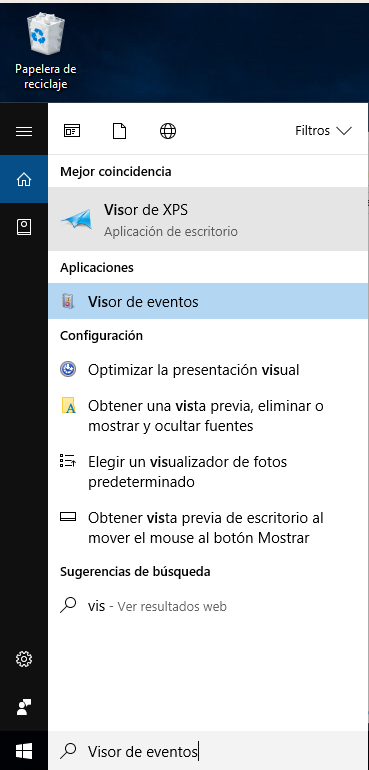


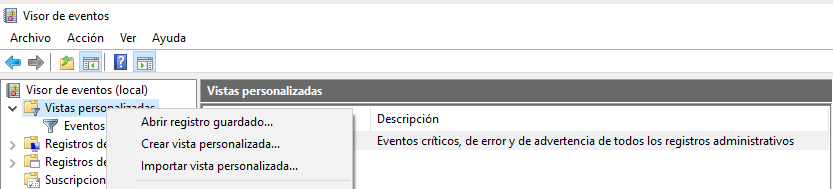


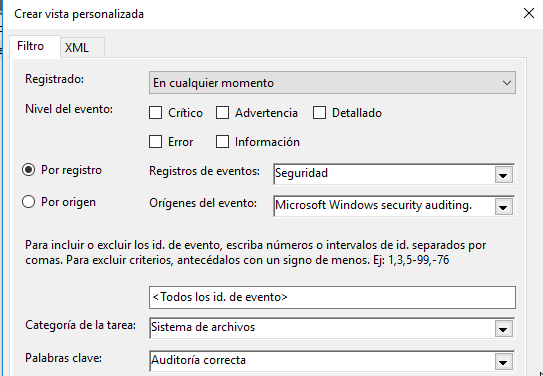


Nos vamos a permisos avanzados -> Y las acciones a auditar son los accesos correctos a Mostar carpeta/leer datos, Crear archivos/escribir datos, Crear carpetas/anexar datos, Eliminar.

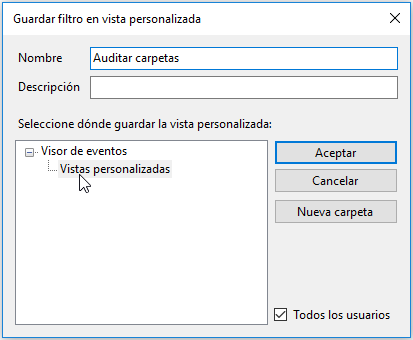
**1.4.-** Luego abrimos el visor de eventos y creamos una vista personalizada.





En filtro -> registro de eventos de Seguridad. En orígenes de evento elegimos auditoría de seguridad de Microsoft Windows (Microsoft Windows Security auditing). En categoría de la tarea elegimos Sistemas de archivos. En palabra clave ponemos auditoria correcta.

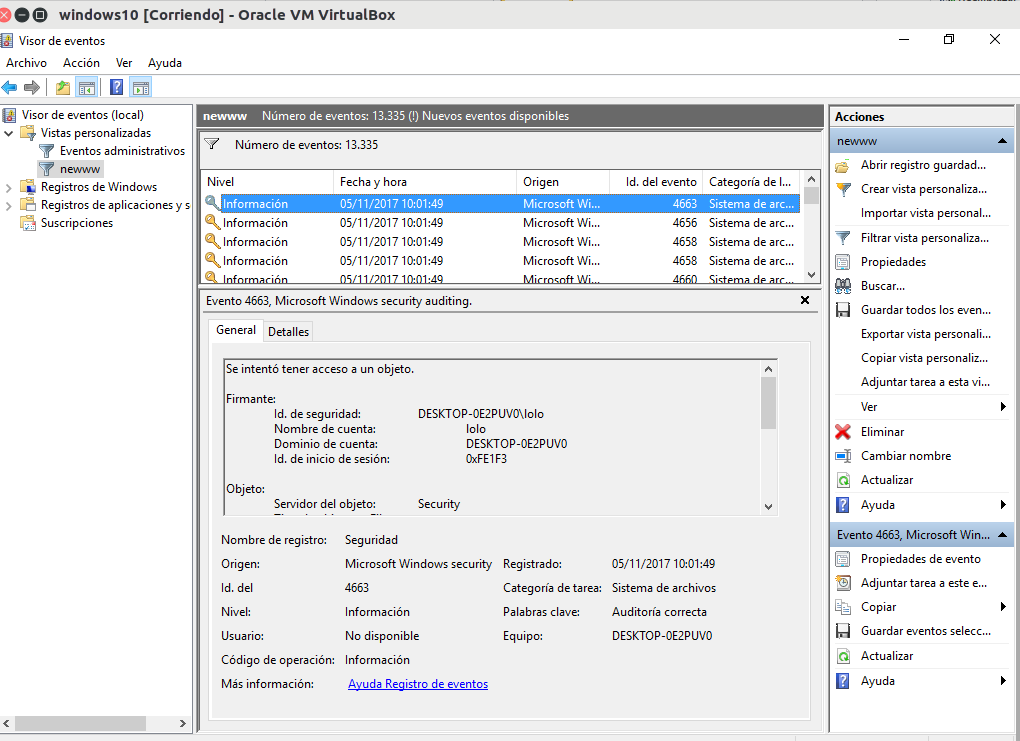
Como nombre le ponemos Auditar carpeta

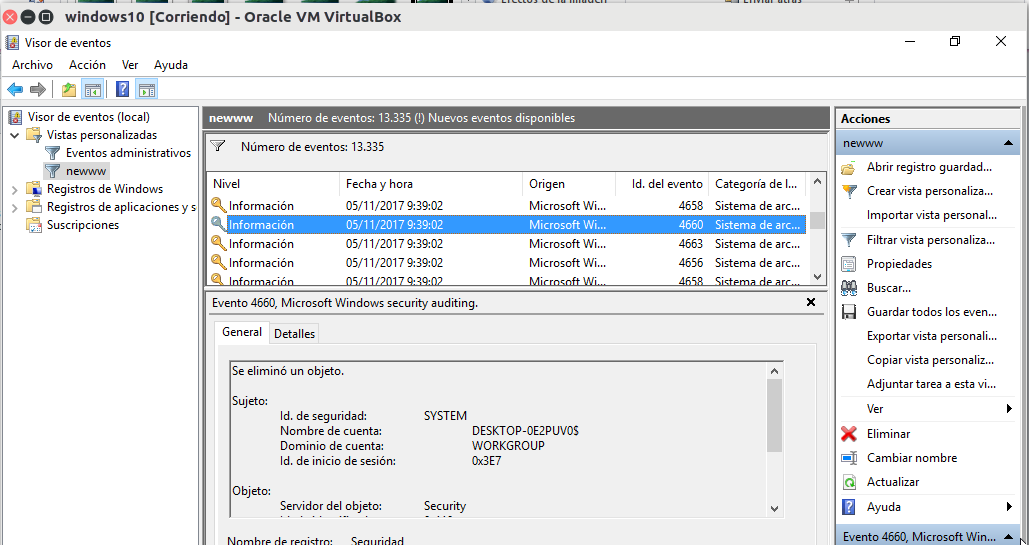


**1.5.-** Cambiamos de usuario y accedemos a la carpeta . Luego salimos de la carpeta y la borramos.

**1.6.-** De vuelta al administrador vemos que la carpeta se ha borrado. Abrimos el visor de eventos y vamos a la vista personalizada creada antes.

**1.7.-** En la pantalla de la vista damos al botón actualizar y vemos nuevos eventos. Buscamos el código **4663** que indica que un usuario accedió a un objeto y **4660** que indica que un usuario ha borrado la carpeta.





Listado de eventos relacionados con la seguridad y relacionados con la auditoría

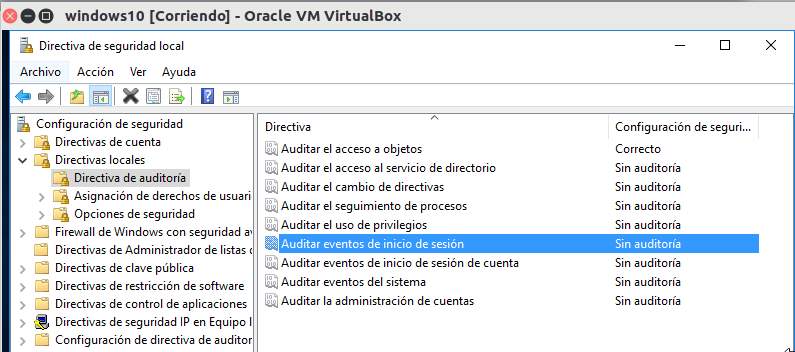
https://support.microsoft.com/es-es/kb/977519

**2**

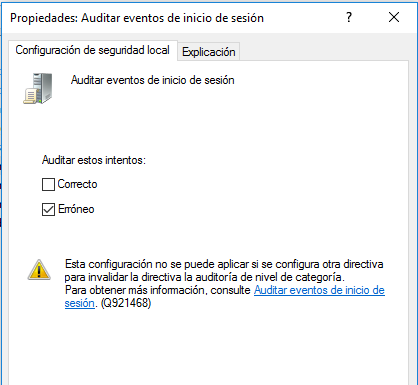
**Intentos de autenticación que no han tenido éxito**

**2.1.-** Para acceder a las directivas de seguridad local ejecutamos el comando secpol.msc

Directivas de Seguridad Local -> Directivas locales -> Directiva de auditorías -> auditar acceso a objetos.



**2.2.-** Vamos a auditar los **accesos erroneos y reiniciamos**

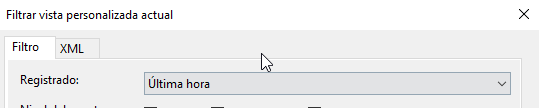
****

En este caso particular, buscamos intentos de autenticación que no han tenido éxito. Para lograrlo, será muy útil saber que el identificador de este tipo de eventos es el 4625.

**2.3.-** Creamos una vista personalizada

**2.4.-** Vamos a indicar el periodo de tiempo en el que queremos centrar la búsqueda. Para lograrlo, disponemos de una lista desplegable.El último elemento de la lista nos permite establecer un Intervalo personalizado. Es decir, podremos fijar la fecha y hora en la que comienza y en la que acaba el intervalo de tiempo en el que queremos centrarnos.

**En nuestro ejemplo, nos limitaremos a última hora .**

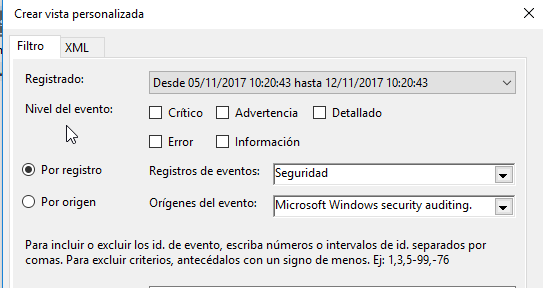


**2.5.-** Debajo del intervalo, incluiremos el *Nivel del evento*. Aquí indicaremos si buscamos eventos críticos, de advertencia, etc. *(Clasificación de la gravedad del evento)*

**Si lo dejamos en blanco, serán tenidos en cuenta todos.**

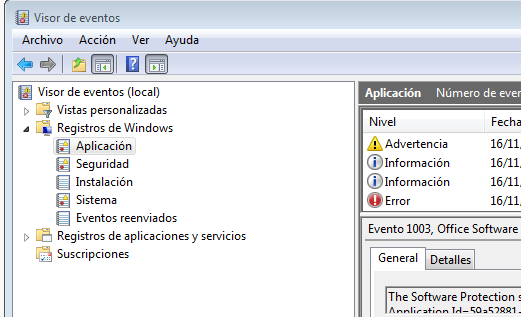
**2.6.-** Indicamos como se busca el evento: *Por registro*, podremos señalar a qué subcategoría pertenecen los eventos, dentro de las categorías *Registros de Windows* y *Registros de aplicaciones y servicios*.

**Pondremos todos los eventos relacionados con la subcategoría Seguridad y por origen , elegiremos Microsoft Windows security auditing.**



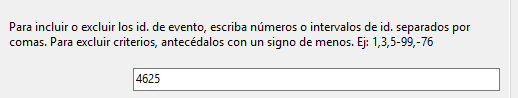
* Aplicación: Aquí anotan sus eventos las aplicaciones y los servicios que no forman parte del sistema
* Seguridad: Incluye la información de los eventos relacionados con la seguridad del sistema.
* Instalación: Donde se anotan la información de los eventos relativos a la configuración de roles y características.
* Sistema: Contiene información relativa a los eventos del sistema y de sus componentes.
* Eventos reenviados: Contiene información reenviada por otros sistemas de la red.

**Aquí los tenemos todos sin filtrar**



Si es por origen le indicamos, qué parte del sistema ha ocasionado el evento (por ejemplo, el *spooler* de impresión).Al elegir el origen, se asigna de forma automática el valor adecuado en la subcategoría *Por registro*, sustituyendo a la que pudiéramos haber elegido en el punto anterior.

**2.7.-** En el siguiente cuadro de texto, podemos restringir los identificadores que serán tenidos en cuenta para la vista. Para conseguirlo, tenemos varias opciones:

* Si necesitamos un único identificador, escribimos su número (por ejemplo: 4625).
* Si queremos incluir varios identificadores, los separamos por comas (por ejemplo: 4624, 4625).
* Para incluir un rango, escribimos el primero y el último de los repositorios que necesitamos incluir, separados por un guión (por ejemplo: 4650-4655).
* También podemos incluir todo lo anterior, escribiendo identificadores individuales o rangos separados por comas (por ejemplo: 4698, 4700-4702, 4650-4655).
* Incluso podemos eliminar un identificador en particular, de un rango dado, precediéndolo de un signo menos (Por ejemplo: 4698-4702, -4699).

**En nuestro ejemplo, nos limitaremos al identificador 4625.**

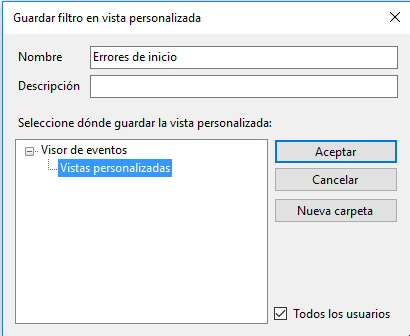
**2.8.-** Categoría de la tarea y seleccionar las que deseemos. (área general de la funcionalidad del proveedor de eventos. Tiene sentido , si vamos a auditar acceso a carpetas la categoría es Sistema de archivos, si vamos a auditar acceso de usuarios la categoría es Inicio de Sesión…)

**Nosotros seleccionamos la categoría Inicio de sesión.**

**2.9.-** Otro aspecto que podemos utilizar en nuestra vista personalizada es el filtro por Palabras clave

**En este caso, haremos clic sobre la casilla correspondiente a Error de auditoría**

**2.10.-** Aceptamos y guardamos como errores de inicio.



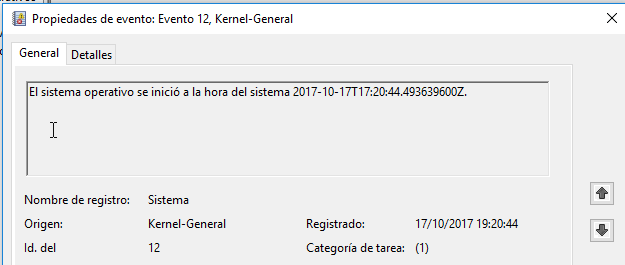
**2.11.-** Por último intentamos entrar con un usuario y ponemos mal la contraseña, luego entramos con el administrador y vemos el visor de sucesos

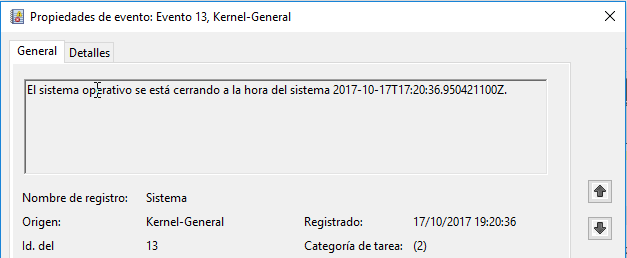
**3**

**Auditar los inicios apagados y suspensiones del sistema**

Existe la consulta del ***Visor de Eventos*** para saber si alguien ha tocado tu equipo cuando tu no estabas. Esta consulta no es otra más que la de los ***eventos de inicio y apagado del sistema***, algo bastante significativo que puede ayudarte a saber si alguien está intentando hacer algo malo mientras tú no estás.

Los eventos que se generan son fácilmente reconocibles, ya que tanto el de arranque del sistema, como el de apagado se generan en la **categoría Kernel General**, tal y como puede verse en las siguientes capturas.

**ID: 12 Encendido**



**ID: 13 Apagado**

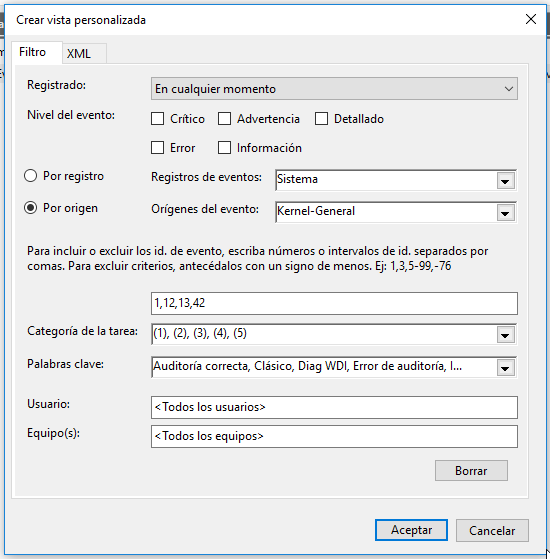
Suspender la sesión, o hibernar la computadora, es decir, bajar la pantalla del portátil o seleccionar las opciones de suspensión o hibernación. En ese caso el evento está en la categoría **Kernel-Power** y lleva el número ***42***.

Y. Si queremos saber por tanto si alguien ha encendido el equipo en nuestra ausencia, habría que controlar también si lo ha vuelto a reanudar. Para controlar esto, lo más sencillo es revisar el evento 1, ya que cuando el equipo deja la suspensión, lo primero que hace el sistema operativo es poner correctamente la hora del sistema.

**Vista del Visor de Eventos**

20. En conclusión, monitorizando en el Visor de Eventos los sucesos 1,12,13 y 42 se puede conocer si alguien ha encendido el equipo cuando nosotros no estábamos.

**Primeramente se debe habilitar la política “auditar eventos del sistema” mediante la consola secpol.msc**

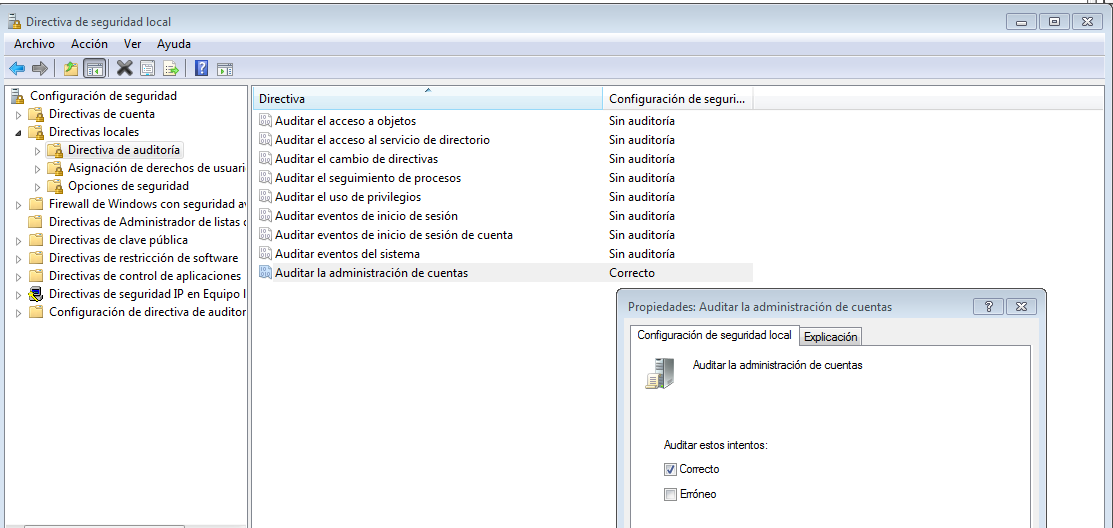


**4**

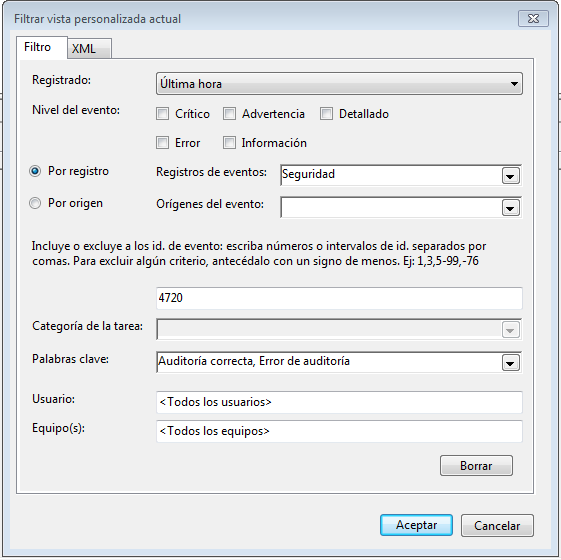
**Auditar administración de cuentas de usuario**

**4.1.-** Para acceder a las directivas de seguridad local ejecutamos el comando secpol.msc

**Directivas de Seguridad Local -> Directivas locales -> Directiva de auditorías -> auditar administración de cuentas.** (después reiniciar)

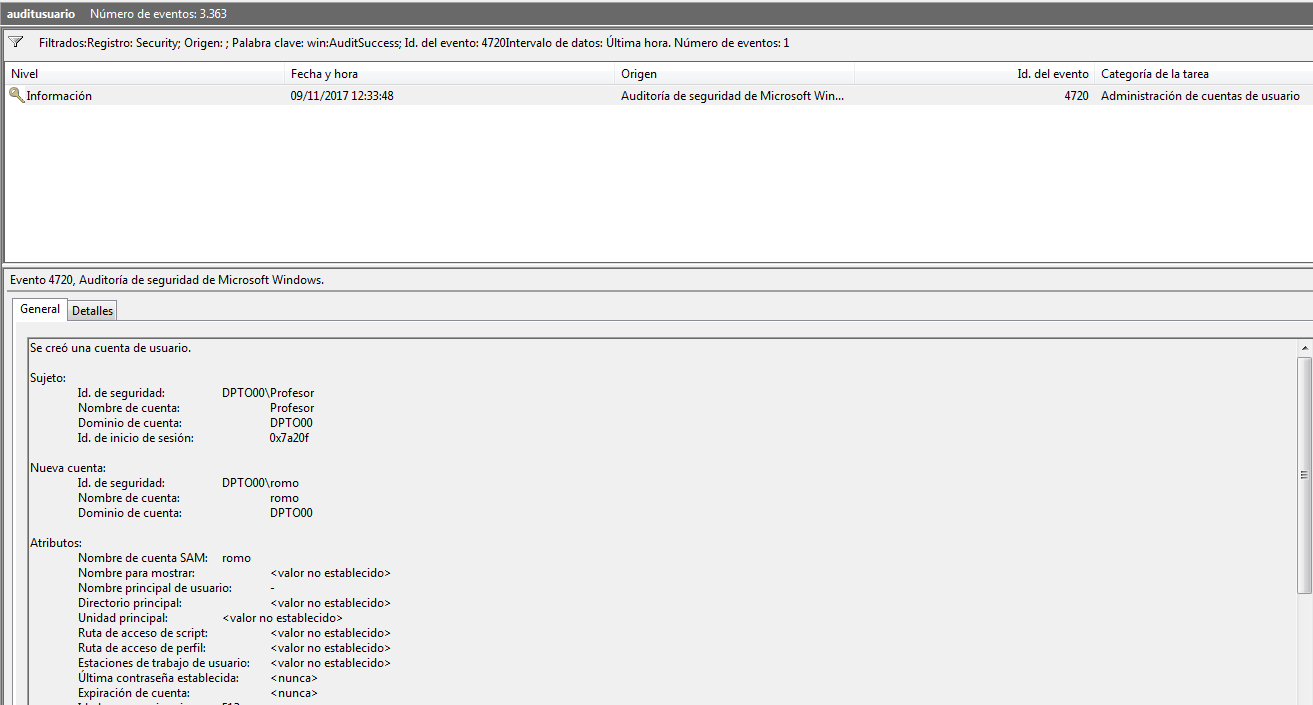


**4.2.- Configurar la vista para auditar la creación correcta de usuarios**



4.3.- Crear un usuario

4.4.- Comprobar la vista



4.5.- Control de deshabilitado de cuentas de usuarios

