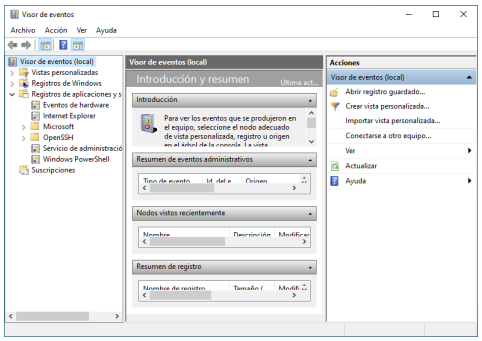
Tema VII Ejercicio II: El Visor de Eventos

Nicolás A. Ortega Froysa

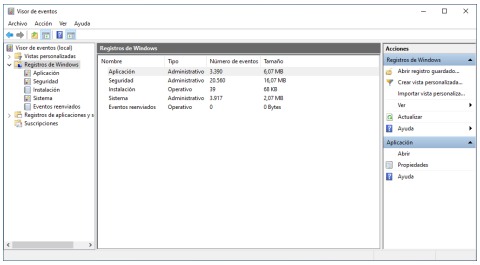
19 de febrero de 2022

Índice

1. Introducción



(a) Visor de Eventos.



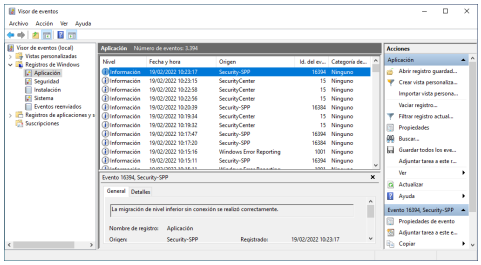
(b) Registros de Windows.

Figura 1: Vista inicial del visor de eventos.

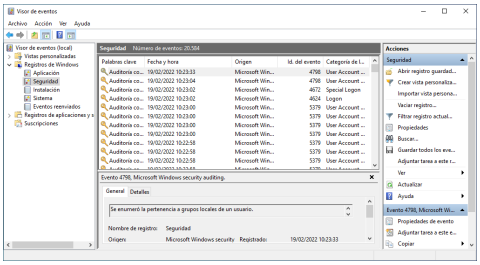
El *Visor de Eventos* es una herramienta que nos provee Windows para poder facilitar la tarea de monitorizar nuestra máquina, o incluso varias máquinas. Podemos encontrarlo simplemente buscando en el *menú de Inicio* por su nombre: «visor de eventos». Esto nos abrirá una ventana como la que vemos en la figura 1a. Si nos vamos al apartado en el menú a la izquierda que dice «Registros de Windows» podemos ver un resumen de los sucesos que han ocurrido en nuestra máquina (figura 1b), aunque sean tan sólo estadísticas simples.

Nos encontramos en el menú a la izquierda que podemos ver varios registros. Cada uno de estos registros contiene eventos divididos en categorías. Podemos acceder a los siguientes registros:

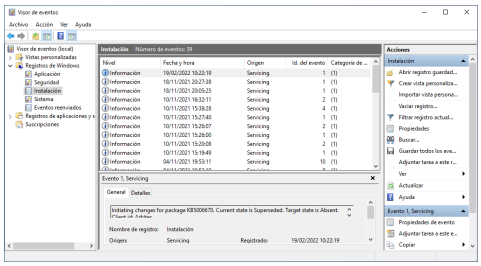
- **Sucesos de aplicación:** los eventos que han disparado de las aplicaciones (figura 2a).
- **Sucesos de seguridad:** se trata de eventos tratando con uso de acciones privilegiadas y auditorías programadas (figura 2b).
- **Sucesos de instalación:** todo evento relacionado con la instalación y actualización de *software* en el sistema (figura 2c).
- **Sucesos de sistema:** se tratan de eventos provocados por el sistema, generalmente tienen que ver con servicios de Windows (figura 2d).
- **Eventos reenviados:** actualmente este registro está vacío, ya que lo tenemos que configurar (figura 2e). Este registro sirve para acumular eventos de otros sitios que queremos acumular. Lo usaremos luego cuando tratemos las suscripciones.



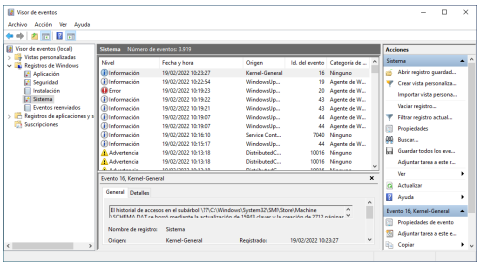
(a) Sucesos de aplicación.



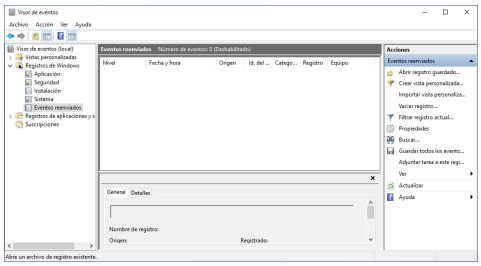
(b) Sucesos de seguridad.



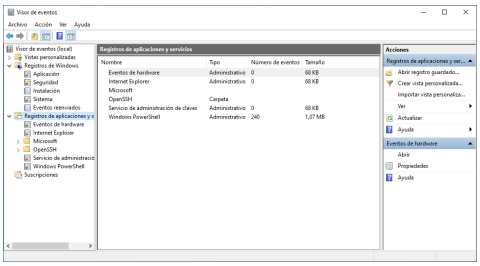
(c) Sucesos de instalación.



(d) Sucesos de sistema.



(e) Eventos reenviados.



(f) Registros de aplicaciones.

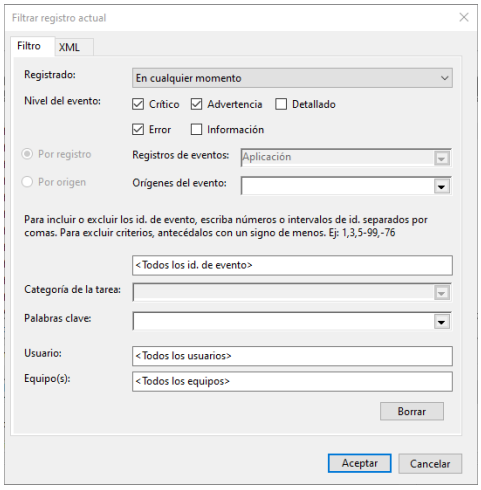
Figura 2: Registros del visor de eventos.

- **Registros de aplicaciones:** para los eventos que pertenecen a aplicaciones concretas, podemos verlos en este apartado para cada aplicación en particular (figura 2f).

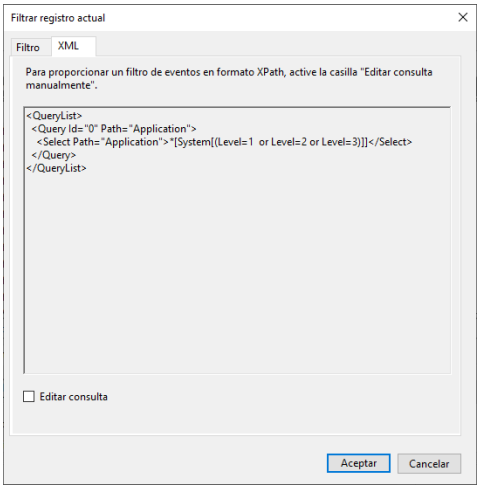
2. Filtrando Eventos

Generalmente ver absolutamente todas los sucesos, aunque estén discriminados por tipo, puede ser una tarea bastante tedioso. Para solucionar esto podemos hacer uso de la filtración de sucesos que nos provee el *Visor de Eventos*. E.g. si sólo queremos aquellos sucesos que sean errores o advertencias (es decir, que no sean informativas), nos sería útil un filtro para que sólo veamos aquellos sucesos que nos interesen o que requieran nuestra atención.

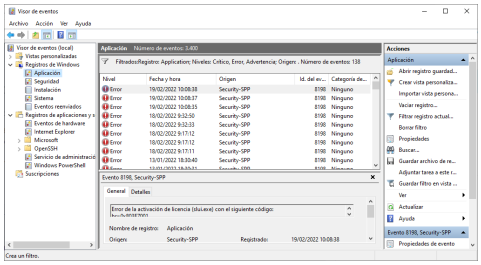
Para crear un filtro nuevo, entramos en el registro que nos interesa y



(a) Ventana de configuración del filtro.



(b) Configuración del filtro en XML.



(c) Vista de registro filtrado.

Figura 3: Configuración del filtro.

buscamos en el menú de acciones disponible a la derecha el elemento que dice «Filtrar registro actual...». Esto nos abrirá una nueva ventana para configurar nuestro filtro (figura 3a). Esto nos provee varias opciones principales para configurar nuestro filtro:

- **Registrado:** el tiempo en el cual el evento ha sido registrado.
- **Nivel del evento:** el nivel de prioridad que tiene el evento.
- **Registros de eventos:** el registro existe del que se filtrarán los eventos; en nuestro caso como filtramos el registro de «Aplicación», este campo ya no se puede editar.

También podemos ver que existe una pestaña que se denomina «XML». Aquí podemos encontrar la misma configuración de nuestro filtro, pero definido por medio de código XML (figura 3b). Este código lo podemos editar manualmente si no queremos usar el interfaz de la pestaña de «Filtro».

Cuando le damos al botón de «Aceptar», nos mostrará una nueva vista filtrada con nuestro filtro que acabamos de definir (figura 3c). Si queremos desactivar el filtro, tan sólo tenemos que pulsar sobre la acción en el menú a la derecha, «Borrar filtro».

3. Programación de Tareas

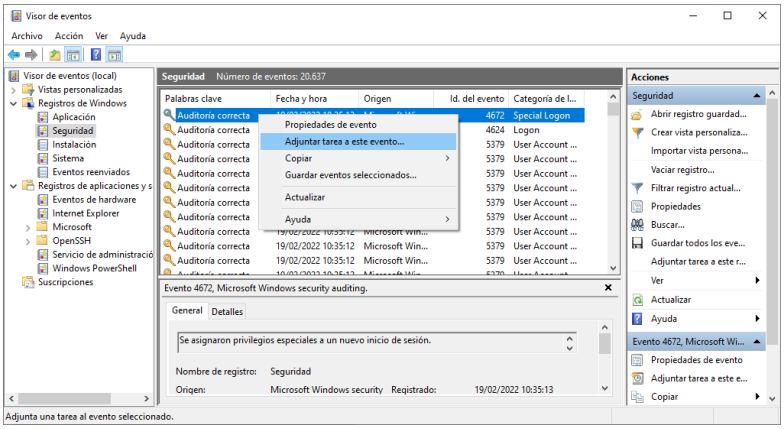


Figura 4: Adjuntar una tarea a un evento.

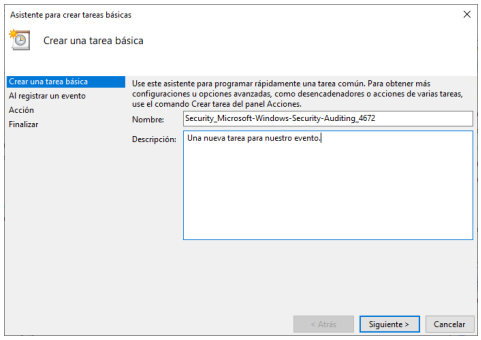
El visor de eventos también nos facilita programar tareas en reacción a ciertos eventos. Esto puede ser algo útil si queremos que nos notifique si ocurre un suceso específico. Para administración de sistemas, esto sería un sistema bastante útil. Para esto, pulsamos el botón derecho del ratón sobre el evento al que queremos adjuntar una tarea, y pulsamos la opción de «Adjuntar tarea a este evento...» (figura 4).

Al pulsar el botón se abrirá una ventana nueva para la configuración de nuestra acción. El proceso se divide en varios pasos:

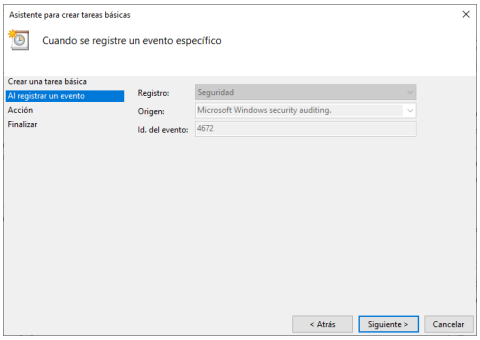
1. Asignamos un nombre y (de forma opcional) una descripción a nuestra tarea (figura 5a)

2. Seleccionamos el evento que disparará nuestra tarea (figura 5b). En nuestro caso, como ya lo seleccionamos al abrir esta ventana, no es necesario definirlo.

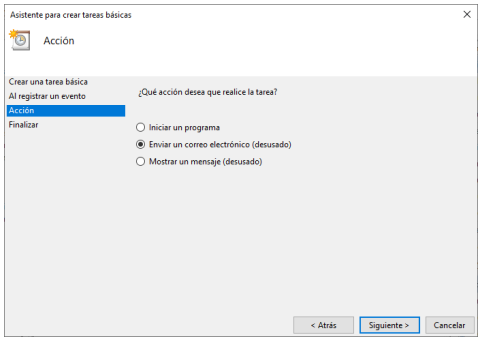
3. Seleccionar el tipo de acción que se realizará cuando se dispara el evento (figura 5c). Nosotros vamos a usar correo electrónico, aunque actualmente dice que está «desusado», por lo tanto luego no nos permitirá crear la tarea, mas el proceso sigue siendo igual.



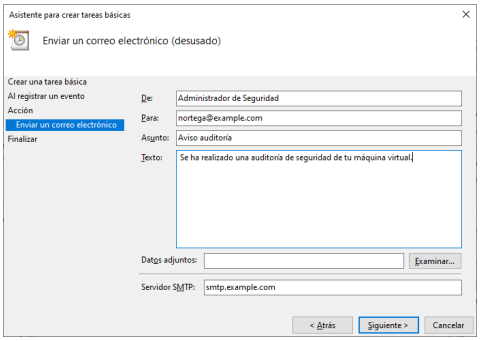
(a) Nombrar tarea.



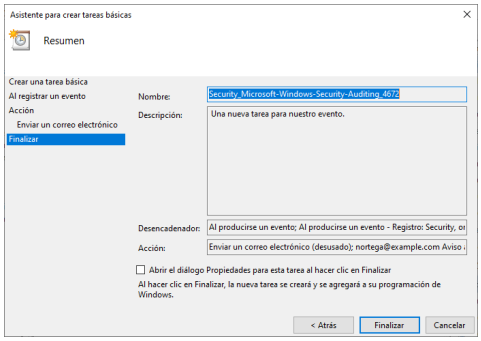
(b) Seleccionar evento.



(c) Seleccionar acción.



(d) Configurar acción.



(e) Resumen de tarea.

Figura 5: Configuración de una tarea nueva.

a) Definimos los detalles del correo que se enviará (figura 5d).

4. Nos muestra un resumen de lo que hemos configurado (figura 5e).

Al llegar a este último paso pulsamos «Finalizar» para crear la tarea. Aunque, como mencionamos antes, no nos dejará ya que la acción de enviar un correo esta en «desuso».

4. Suscripciones

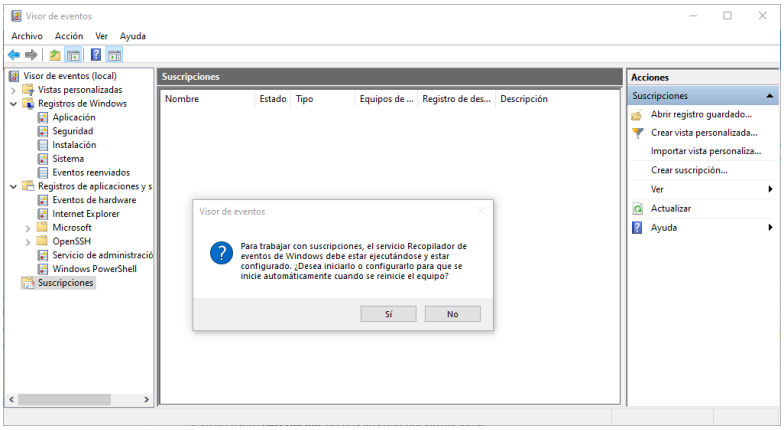


Figura 6: Habilitar recopilador de eventos de Windows.

Si estamos trabajando con varios equipos, lo más útil es la opción de usar suscripciones, ya que éstas nos permiten recibir todo tipo de sucesos filtrados de varias máquinas. Para administrar nuestras suscripciones nos vamos al apartado del menú izquierdo que dice «Suscripciones». Al pulsarlo, nos mostrará un aviso diciendo que para usar las suscripciones tenemos que habilitar un servicio de Windows denominado «Recopilador de eventos de Windows» (figura 6). Para continuar, simplemente le decimos que «Sí».

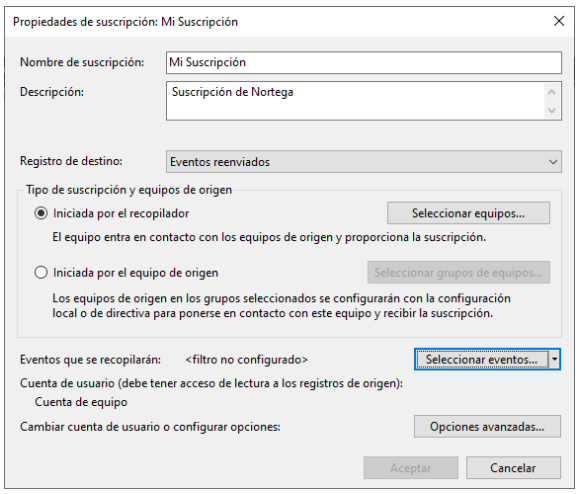


Figura 7: Creación de una nueva suscripción.

Cuando ya está habilitado, podemos crear una nueva suscripción seleccionando el elemento en el menú de acciones derecho denominado «Crear

suscripción...». Esto nos abrirá una nueva ventana donde podemos configurar nuestra suscripción (figura 7). Aquí tenemos varias opciones para la configuración de nuestra suscripción:

- **Nombre y descripción:** nos sirve para definir e identificar nuestra suscripción.
- **Registro de destino:** precisamente aquel registro vacío que vimos en la primera sección es el registro que usamos aquí: el registro de «Eventos reenviados».
- **Selección de equipos:** podemos escoger los equipos (remotos) que queremos monitorizar con esta suscripción.
- **Selección de eventos:** escogemos un filtro, con una interfaz igual a la del segundo apartado, para los eventos a los que nos queremos suscribir.

Con todo esto configurado podemos darle a «Aceptar» y nos creará una nueva suscripción.

5. Derechos de Autor y Licencia