**PRÁCTICA N°5**

**TEMA: “MONITOREO Y ANALISIS DE EVENTOS DE SEGURIDAD”**

**1. OBJETIVOS**

1.1 Familiarizar al estudiante en la navegación y filtración de registros en el visor de eventos.

1.2 Identificar patrones de actividades sospechosas o no autorizadas.

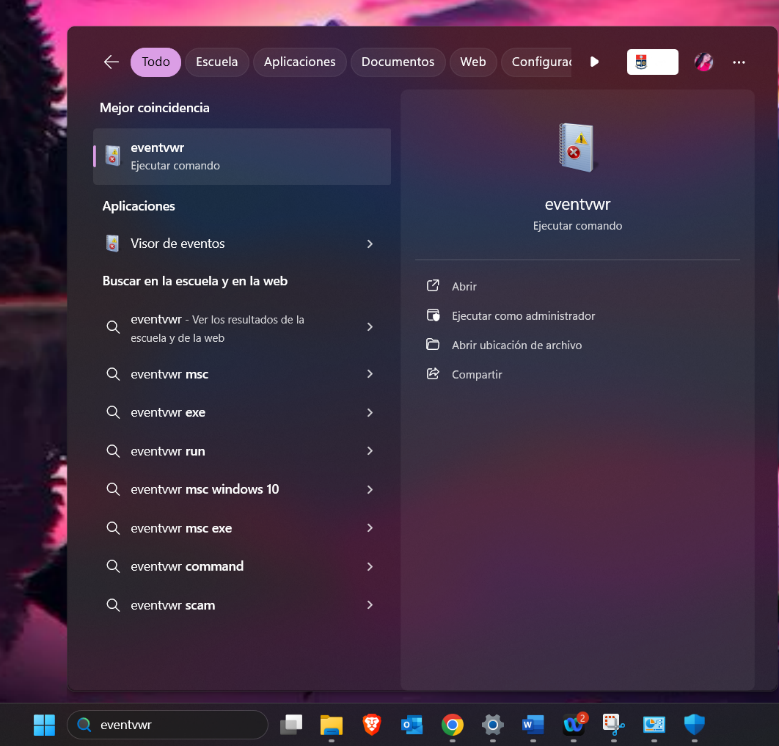
1.3 Introducir al estudiante en la propuesta de medidas correctivas y preventivas basadas en los hallazgos del análisis de logs.

**4. PRÁCTICA**

#### Acceso al Visor de Eventos

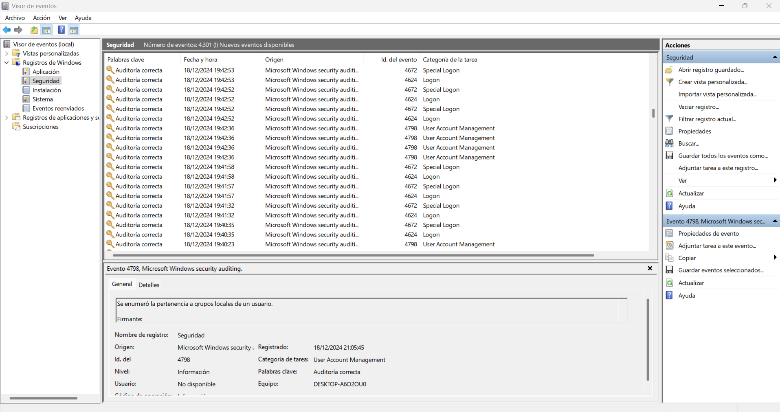
1. El proceso detallado en la Figura 1 indica la búsqueda del visor de eventos:

* Clic derecho en la barra de búsqueda de Windows > Escribir **eventvwr** y presionar Enter.



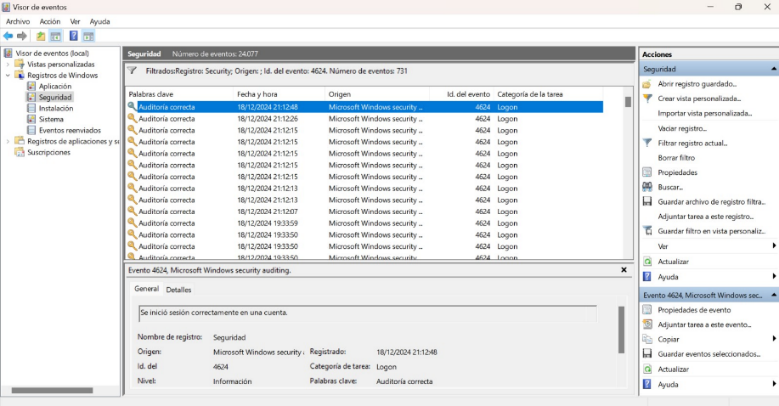
*Figura 1: búsqueda de Visor de Eventos*

1. Abrir la consola del Visor de Eventos > Registros de Windows > Seguridad, en la Figura 2, se observa los diferentes logs.

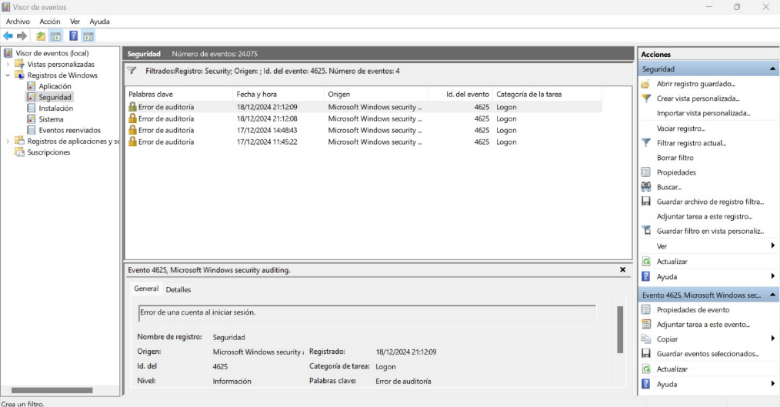


*Figura 2: Visualizador de logs*

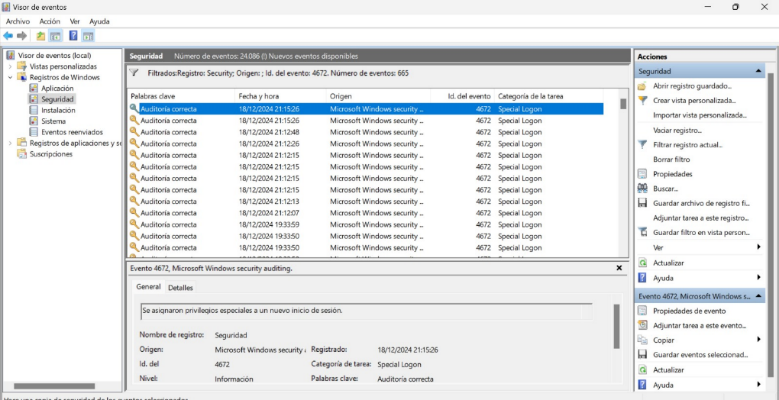
1. En el panel derecho > Filtrar registro actual, ingresar ID de evento (Figura 3 se observa el evento 4624, Figura 4 muestra el evento 4625 y en la Figura 5 indica el evento 2672).



*Figura 3: Evento 4624*



*Figura 4: Evento 4625*



*Figura 5: Evento 4672*