**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.

**2. PREPARATORIO**

2.1 Consultar que es un log o registro de eventos en un sistema operativo?

2.2 Investigar que es un visor de eventos en Windows y cómo se accede a él?

2.3 Enumerar las categorías principales del registro en el visor de Eventos y su descripción? (mínimo 3).

2.4 Enumerar ejemplos de eventos que pueden auditarse y su importancia? (mínimo 3).