**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.

**3. REACTIVOS**

¿Cuál es el propósito principal del monitoreo de eventos de seguridad en un sistema operativo?

1. Mejorar el rendimiento del sistema.
2. Detectar y responder a incidentes de seguridad.
3. Mejorar la apariencia de la interfaz de usuario.
4. Minimizar el uso de memoria.

¿Qué tipo de eventos deberían ser monitoreados para detectar intentos de acceso no autorizado?

1. Eventos de inicio de sesión y cierre de sesión.
2. Errores de red.
3. Actualizaciones de software.
4. Modificaciones en el sistema operativo.

¿Qué categoría de eventos en el Visor de Eventos de Windows está relacionada con la seguridad del sistema?

1. Aplicación.
2. Sistema.
3. Seguridad.
4. Configuración.

Al revisar los registros de eventos de seguridad, ¿qué tipo de actividad indicaría un posible intento de phishing o ataque similar?

a) Un cambio en la configuración de la pantalla.

b) Varias fallas de inicio de sesión seguidas por un inicio exitoso.

c) Actualizaciones de software en el sistema.

d) Conexiones a servicios de redes sociales.

¿Qué herramienta es comúnmente utilizada para analizar y visualizar los registros de eventos en un sistema Windows?

a) Microsoft Excel.

b) Visor de Eventos.

c) PowerShell.

d) Task Manager.