**UNIVERSIDAD DE LA INTEGRACIÓN DE LAS AMÉRICAS**

**FACULTAD DE INGENIERÍA.**

**MATERIA**

**Sistemas Operativos.**

**TÍTULO**

# La seguridad del sistema operativo;

# una responsabilidad que empieza con el usuario.


**Mg. Alan Vladimir Dioses Echegaray.**

**Lucio Vera.**

**ESTUDIANTE:**

**Jannely Magalí Guillén Capdevila.**


**Asunción - Paraguay.**

**2025.**

**La seguridad del sistema operativo;**
**una responsabilidad que empieza con el usuario…**

En la era digital, donde gran parte de nuestras actividades cotidianas dependen de sistemas computacionales, la seguridad del sistema operativo se convierte en un tema fundamental. A pesar de ello, muchas veces no somos conscientes de las herramientas que tenemos a disposición para proteger nuestra información. Durante el desarrollo del Laboratorio N.º 4 de la materia Sistemas Operativos, tuve la oportunidad de experimentar directamente con funciones clave de seguridad en el sistema Windows, como la auditoría de eventos, el análisis de servicios innecesarios y la restauración del sistema. Esta experiencia me permitió comprender que el usuario cumple un rol activo en la protección de su entorno digital. Este ensayo parte de la hipótesis de que la seguridad del sistema operativo no depende únicamente de configuraciones técnicas, sino también de la actitud y responsabilidad del usuario frente al entorno informático. A continuación, se presentan argumentos que respaldan esta afirmación a través del análisis de los resultados obtenidos en el laboratorio y de información accesible en línea.

Una de las primeras actividades realizadas en el laboratorio fue la activación de la auditoría de eventos. Esta función permite al sistema operativo registrar información detallada sobre acciones que se realizan, tanto exitosas como fallidas. En mi caso, generé un intento de inicio de sesión fallido y un acceso a una carpeta sin los permisos necesarios. Inmediatamente, el Visor de eventos de Windows registró los eventos correspondientes (por ejemplo, ID 4625 y 4656), lo que demostró que el sistema estaba monitoreando cada acción.

Esta herramienta no solo sirve para detectar intrusiones o errores, sino también para tener control sobre el propio uso del sistema. Según el sitio oficial de Microsoft, el evento 4656 indica que se ha solicitado acceso a un objeto protegido, y muestra datos como el usuario, el recurso y la razón del fallo (support.microsoft.com). Gracias a esta función, comprendí que auditar no es solo “vigilar”, sino también “entender” lo que ocurre en el sistema.

Durante el laboratorio también se analizaron los servicios en ejecución en el sistema. Al abrir la consola de servicios (services.msc), identifiqué que estaban activos procesos que no eran esenciales, como “Cola de impresión” o “Windows Search”. Investigando en sitios como SoftZone, aprendí que mantener estos servicios activos sin necesidad puede aumentar la superficie de ataque y reducir el rendimiento del sistema (softzone.es).

Este hallazgo me ayudó a reflexionar sobre la importancia de conocer lo que se ejecuta en segundo plano. Desactivar servicios innecesarios no solo optimiza recursos, sino que también evita que atacantes aprovechen funciones habilitadas sin propósito. Esta parte del laboratorio me enseñó que, en seguridad, menos puede ser más, y que cada elemento activo debe tener una razón justificada.

La tercera parte del laboratorio consistió en probar la herramienta de restauración del sistema. Primero creamos un punto de restauración, luego modificamos algunos elementos visibles del escritorio (fondo de pantalla, carpetas) y finalmente activamos la restauración para volver al estado anterior. El proceso fue rápido y exitoso.

Esta función me resultó especialmente útil porque demuestra que los errores no siempre son irreversibles. Como explica el portal Windows Noticias, restaurar el sistema permite regresar a un punto anterior sin perder archivos personales, lo cual es ideal ante fallos de configuración o instalaciones problemáticas (windowsnoticias.com).

Para quienes trabajan o para quienes estudiamos con computadoras, saber que se puede volver atrás de forma segura representa una tranquilidad enorme. No se trata solo de corregir errores, sino de trabajar con confianza.

El laboratorio de seguridad del sistema operativo me permitió descubrir que la protección de un entorno informático no es algo lejano ni complicado. A través del uso de herramientas como la auditoría de eventos, el análisis de servicios innecesarios y la restauración del sistema, entendí que cuidar el sistema no es responsabilidad exclusiva del software, sino también del usuario. Estas funciones, disponibles en sistemas como Windows 10, son efectivas si se usan con criterio y constancia.

Con base en la experiencia vivida, sostengo que la seguridad del sistema operativo es una construcción diaria que se basa en la observación, la prevención y la toma de decisiones informadas. Cada vez que revisamos los eventos del sistema, desactivamos un servicio innecesario o creamos un punto de restauración, estamos fortaleciendo nuestra autonomía digital. Por ello, promover el conocimiento y uso de estas herramientas desde la educación técnica es clave para formar profesionales responsables y conscientes de su entorno digital.

## Referencias.

**Monrás, A.** (2021, aprox.). *¿Qué servicios innecesarios de Windows 10 y 11 se pueden desactivar para acelerar el sistema?* DominioGeek. Recuperado el 21 de junio de 2025, de https://dominiogeek.com/desactivar-servicios-innecesarios-windows-10/

**Windows Noticias.** (2023). *Cómo restaurar Windows 10 a un estado anterior.* https://www.windowsnoticias.com/restaurar-windows-10-a-un-punto-anterior/

**Microsoft.** (2021, September 7). *4656(S, F): A handle to an object was requested.* In *Windows 10 security auditing*. Microsoft Learn. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4656