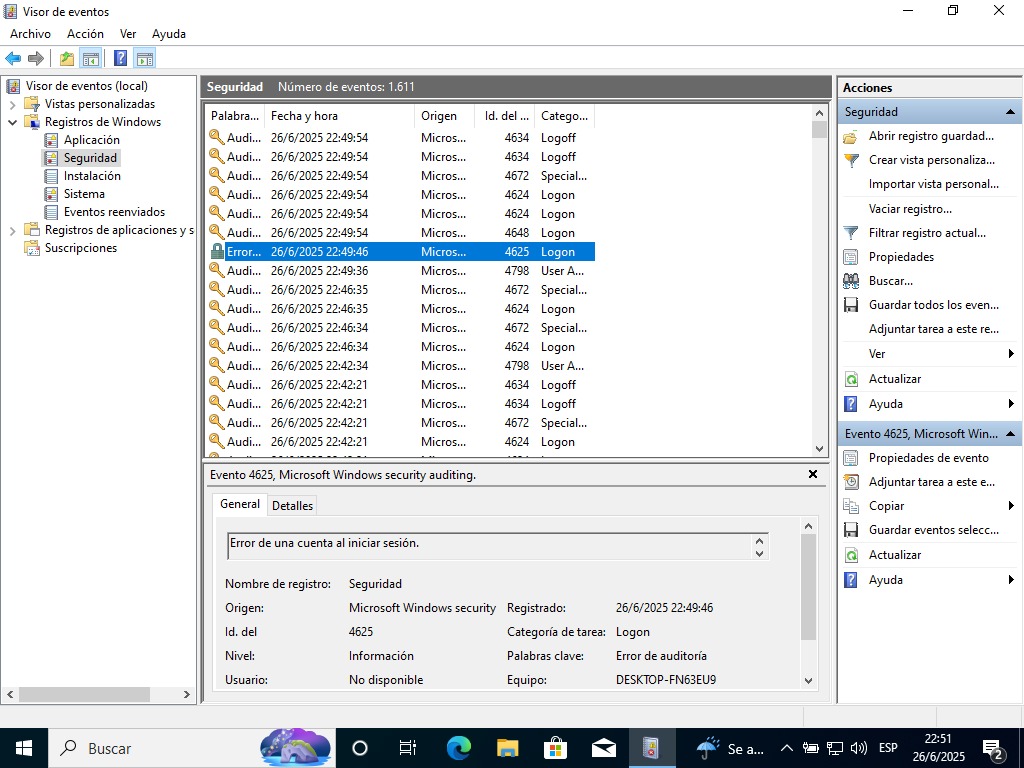
**Laboratorio 4: Seguridad del SistemaAuditoria de Seguridad**

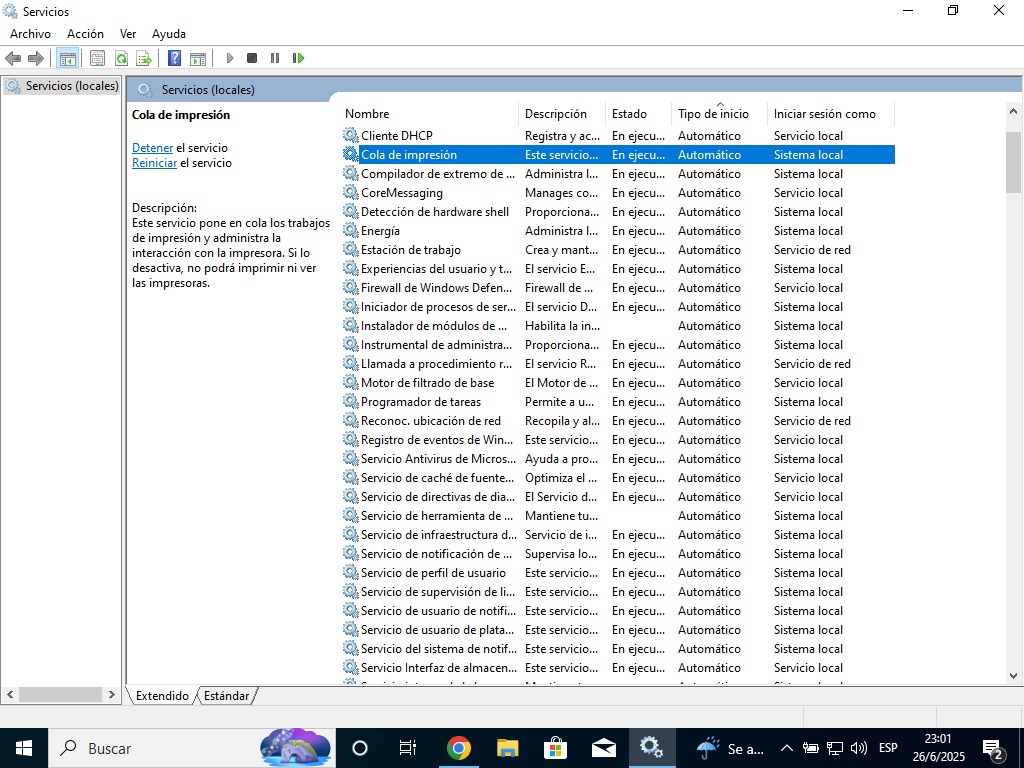
**Alumno:** Marcos Daniel Morel Granada

Se habilitó el registro de eventos de seguridad en Windows con el propósito de capturar sucesos relevantes, como accesos rechazados e intentos fallidos de inicio de sesión. Para comprobar que el sistema registraba correctamente estos eventos, se realizaron pruebas controladas y luego se revisaron los resultados en el Visor de eventos.

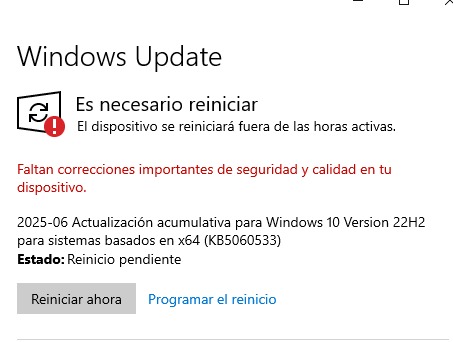


Intento de inicio de sesión fallido

**Análisis de Vulnerabilidades**

Este laboratorio se enfoca en las herramientas de seguridad del SO.

“Cola de impresión” podría ser un riesgo porque cuando está corriendo es una posible puerta de entrada para un ataque



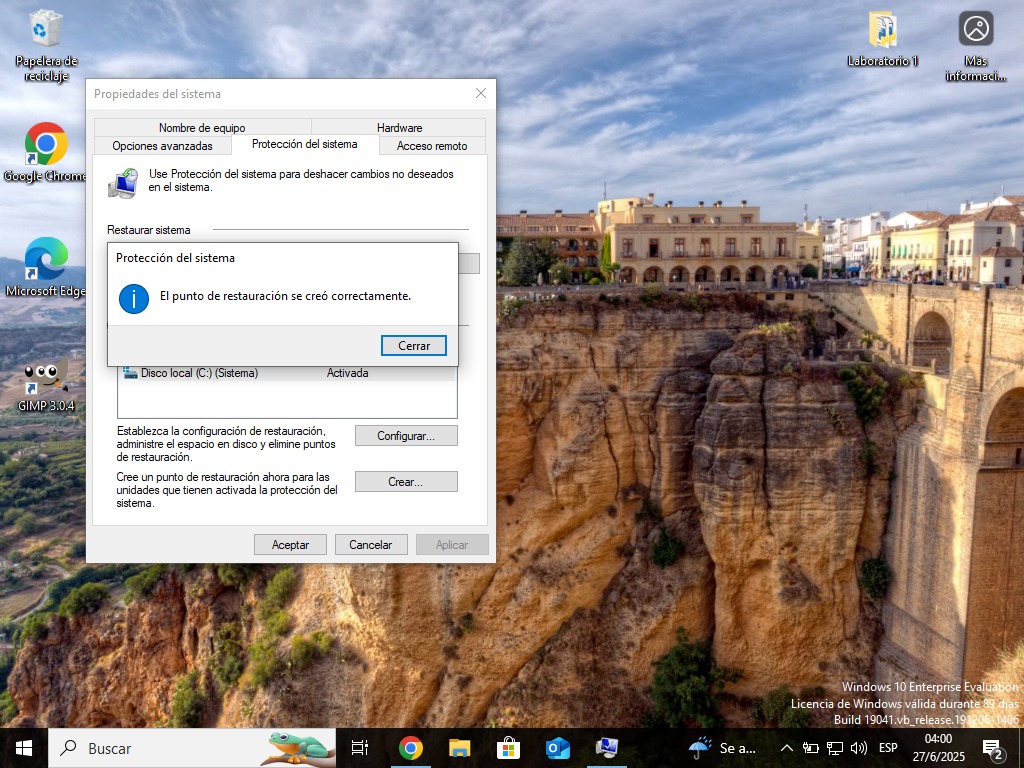
Un sistema desactualizado es una de las mayores vulnerabilidades

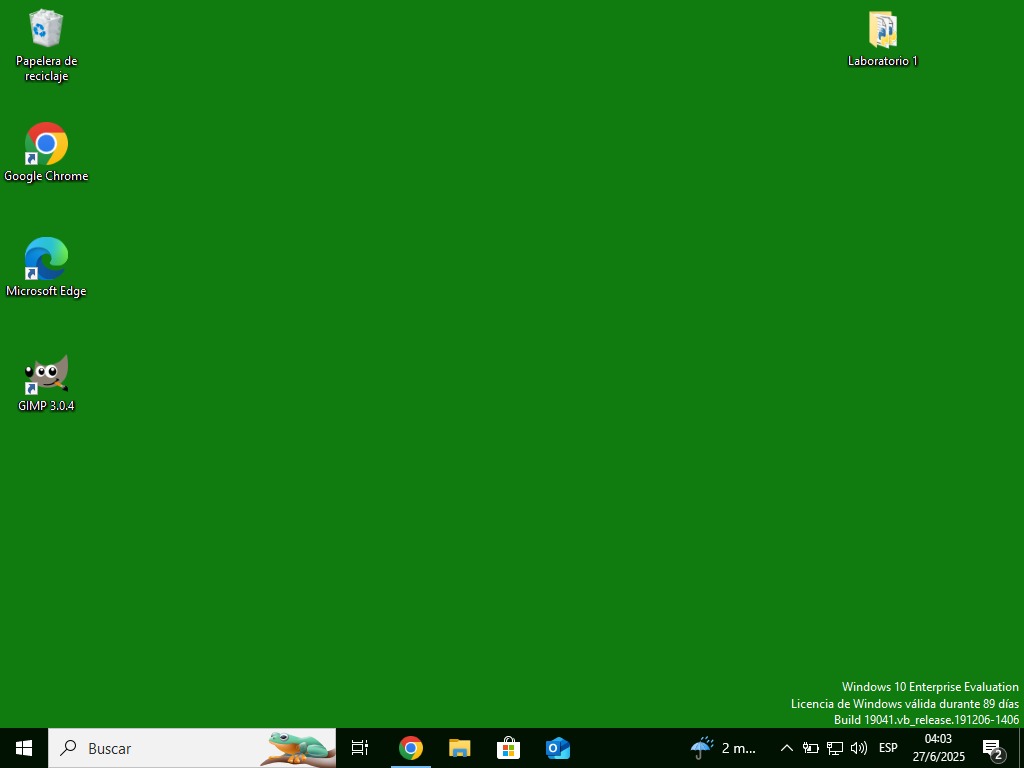
**Respaldo y Recuperación**

Antes de realizar modificaciones en el sistema, se generó un punto de restauración en Windows como medida preventiva, permitiendo revertir el estado del sistema si surgiera algún inconveniente.

**Creación del Punto de Restauración**

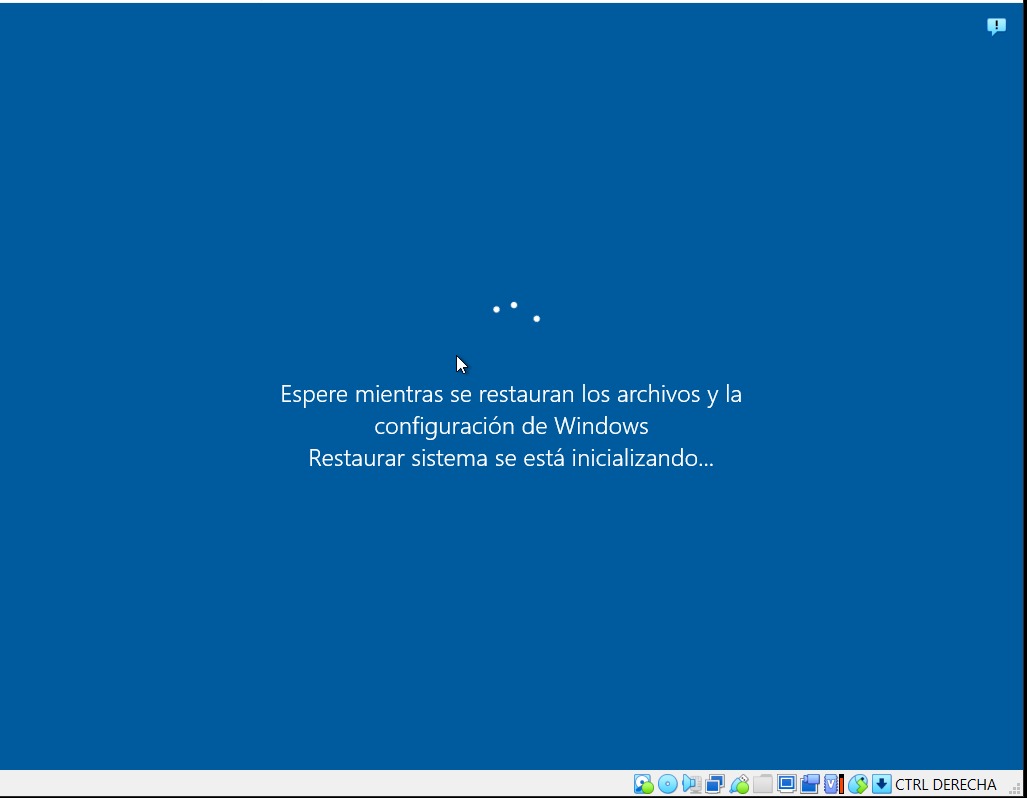
A través de la opción Protección del Sistema, se creó manualmente un punto de restauración. El procedimiento fue rápido, tomando unos 3 minutos. Al finalizar, se confirmó que el punto quedó correctamente registrado y disponible para su uso en caso necesario.





Cambio de fondo antes de iniciar la restauración

Creación de punto de restauración



Inicio de restauración

Windows restaurado

**Conclusión**

Este laboratorio permitió analizar los mecanismos de seguridad integrados en Windows 10, demostrando que:

1. **Los logs de eventos** registran eficientemente actividades críticas (como intentos fallidos de inicio de sesión), siendo una herramienta clave para auditorías.
2. **Los puntos de restauración** son vitales para recuperar el sistema ante cambios no deseados, aunque requieren configuración previa (*Protección del sistema activada*).
3. **Las actualizaciones pendientes y servicios innecesarios** representan riesgos de seguridad, evidenciando la importancia del mantenimiento preventivo.

**Recomendación**:

* Activar la **protección del sistema** y crear puntos de restauración antes de instalar software o realizar cambios críticos.
* Revisar periódicamente el **Visor de eventos** para detectar accesos sospechosos.