# **Informe de Análisis de Eventos de Seguridad en Windows**

**Fecha del Informe**: 11 de agosto de 2025  
**Analista**: Enmanuel Canelon, Analista Junior en Entrenamiento  
**Referencia del Incidente**: Análisis de Eventos 5379 - Lectura de Credenciales en Credential Manager  
**Clasificación de Severidad**: Baja (actividad rutinaria, sin evidencia inmediata de amenaza)

## **Resumen Ejecutivo**

Se analizaron 10 eventos de seguridad con Event ID 5379 registrados el 11 de agosto de 2025 a las 1:21:31 PM en el equipo "EQUIPO\_LOCAL". Estos eventos indican lecturas de credenciales almacenadas en el Credential Manager por el usuario "usuario\_prueba". Debido a limitaciones del evento, no se identificó la aplicación ni la credencial específica, pero se propone el uso de Process Monitor para mayor detalle. No se encontraron indicadores de compromiso. El análisis, realizado en 1 hora con PowerShell, refuerza habilidades en auditoría de seguridad para un rol de analista de ciberseguridad junior.

## **Metodología**

* **Herramientas utilizadas**: PowerShell (Get-EventLog -LogName Security -Newest 10); exportación a CSV (InformeSeguridad.csv).
* **Fuente de datos**: Registro de eventos de seguridad de Windows.
* **Alcance**: Eventos del 11 de agosto de 2025, enfocados en Event ID 5379.
* **Referencias**: Documentación de Microsoft sobre Event ID 5379 y Credential Manager ([learn.microsoft.com](https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/event-5379)).

## **Hallazgos**

* **Eventos identificados**: 10 eventos con Event ID 5379, todos simultáneos.
* **Detalles clave**:
  + **Usuario**: "usuario\_prueba" (Security ID: S-1-5-21-00000000-11111111-22222222-1001).
  + **Dominio**: "EQUIPO\_LOCAL".
  + **Operación**: Lectura de credenciales (%%8100).
  + **Limitaciones**: No se especifica la aplicación ni la credencial leída.
* **Resumen de eventos**:

| **TimeGenerated** | **EventID** | **Message (Resumen)** |
| --- | --- | --- |
| 8/11/2025 1:21:31 PM | 5379 | Credential Manager credentials were read by user "usuario\_prueba". |
| (Repetido para los 9 eventos restantes) |  |  |

* **Anexos**: InformeSeguridad.csv y analisis\_seguridad.ps1.

## **Análisis**

* Los eventos reflejan una operación rutinaria, probablemente desencadenada por una aplicación legítima accediendo a múltiples credenciales simultáneamente. La falta de detalles específicos es una limitación del Event ID 5379.
* **Utilidad**: Sirve como alerta inicial para monitoreo de seguridad, permitiendo identificar patrones inusuales que justifiquen investigación adicional.

## **Recomendaciones**

* **Investigación adicional**: Use Process Monitor (Sysinternals) para identificar la aplicación responsable, filtrando por accesos a "vaultcli.dll".
* **Mejoras de seguridad**: Revise Credential Manager para eliminar credenciales innecesarias; ejecute un escaneo con Windows Defender.
* **Formación**: Estudié herramientas de monitoreo avanzadas y continúe con cursos en Microsoft Learn.

## **Conclusión**

El análisis demuestra competencias en PowerShell y auditoría de eventos, clave para un analista junior. Se recomienda implementar monitoreo con Process Monitor para identificar aplicaciones específicas.

**Firma del Analista**: Enmanuel Canelon  
**Fecha**: 11 de agosto de 2025