
TLP:AMBER

# CISO EXECUTIVE REPORT

TROPIGAS

May 14, 2026

TROPIGAS 05/14/2026

# TLP AMBER CISO
## EXECUTIVE REPORT

Este informe corresponde "ABRIL 2026" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

**SOBRE ESTE INFORME**

El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

# VULNERABILITY

# THREATS

# OPERATIONAL

### Notable Events Active For The Last Month

| Notable Event Type | How Many # |
|---|---|
| MSS-DLP - Abnormal activity in the file system(s) | 219 |
| Internal user deleted or moved a SoftwareMine | 98 |
| Monitoring for open ports | 10 |
| MSS-DLP - External File access | 119 |
| Non Baselined Discovered System | 63 |
| High Persistency Detection | 118 |
| BAS Immediate Threat | 19 |
| Notable Event Alert: Vulnerability exposure from Threat Intelligence | 1 |
| TEVR BAS Immediate Threats | 1 |
| Change in Systems Availability | 1 |

Durante el mes de abril, se produjo un notable incremento en la actividad relacionada con la seguridad de la información, el monitoreo de comportamiento y el control de activos dentro de la infraestructura tecnológica. El evento con mayor volumen correspondió a MSS-DLP - Abnormal activity in the file system(s), con un total de 219 eventos detectados, evidenciando comportamientos anómalos sobre sistemas de archivos monitoreados. Esta actividad puede estar relacionada con modificaciones inusuales, accesos no autorizados, transferencias de información sensible o ejecuciones de procesos fuera del comportamiento esperado, lo que representa un riesgo potencial para la integridad y confidencialidad de los


LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500

datos corporativos.

Además, se identificaron 119 eventos de MSS-DLP (Acceso a Archivos Externos), lo que indica accesos a archivos desde ubicaciones, usuarios o mecanismos considerados externos al comportamiento habitual definido en las políticas de seguridad. Este tipo de eventos requiere una atención especial debido a su posible relación con exposición de información sensible, intercambio no autorizado de archivos o intentos de extracción de datos.

De manera simultánea, se documentaron 117 eventos de High Persistency Detection, lo que sugiere la presencia de posibles mecanismos de persistencia dentro de los sistemas objeto de monitoreo. Estas alertas pueden estar asociadas a procesos recurrentes, tareas programadas sospechosas, ejecución continua de servicios no habituales o comportamientos compatibles con técnicas utilizadas para mantener acceso prolongado dentro de un entorno comprometido.

Por otra parte, se detectaron 98 eventos relacionados con Internal user deleted or moved a SoftwareMine, lo que evidencia acciones internas sobre recursos monitoreados, incluyendo eliminación o movimiento de componentes dentro de la infraestructura. Si bien este comportamiento puede estar asociado a actividades administrativas legítimas, también podría comprometer la trazabilidad, disponibilidad o control sobre elementos críticos si no se implementan procesos adecuados de validación y seguimiento de cambios.

Adicionalmente, se han identificado un total de 63 eventos de Non Baselined Discovered System, lo que indica la presencia de activos que no se encuentran dentro de las configuraciones base establecidas o que no están alineados con las políticas corporativas de hardening y control de inventario. Este comportamiento podría indicar una posible debilidad en la gestión de activos tecnológicos y podría incrementar la superficie de exposición frente a amenazas de seguridad.

Dentro de los eventos de menor volumen, se registraron 19 alertas de BAS Immediate Threat, 10 eventos de Monitoring for open ports, así como eventos individuales relacionados con exposición de vulnerabilidades provenientes de inteligencia de amenazas, detección inmediata de amenazas BAS y cambios en disponibilidad de sistemas. Aunque la frecuencia de estos eventos fue reducida, continúan siendo indicadores relevantes que podrían asociarse a actividades de reconocimiento, exposición de servicios o intentos iniciales de explotación.

---



---


TLP:AMBER

# CISO EXECUTIVE REPORT

## HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500