TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

July 30, 2026

TROPIGAS 07/30/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "MAYO 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

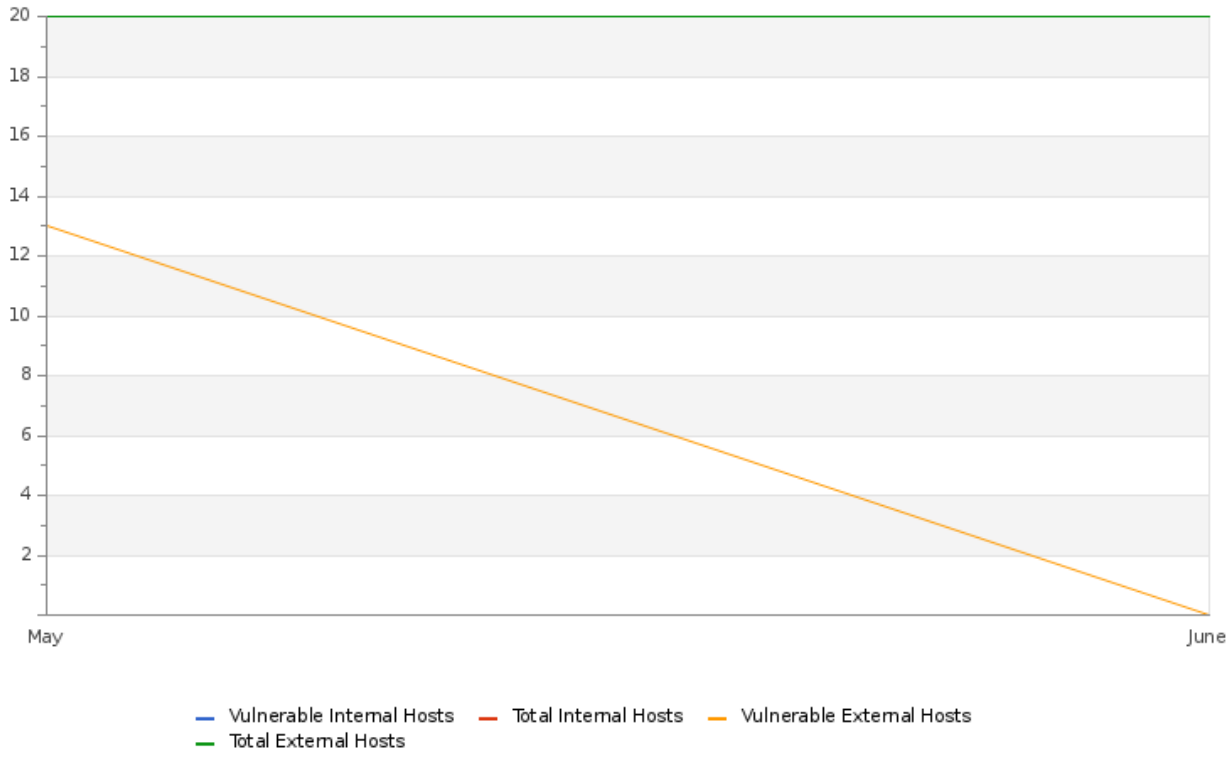
El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

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

TROPIGAS 07/30/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de mayo se evaluó un total de 20 hosts externos. En comparación con el período anterior, la cantidad de activos con vulnerabilidades identificadas se mantuvo estable en 12 hosts, lo que indica que la superficie de exposición de la organización no presentó variaciones significativas durante el período evaluado. No obstante, la identificación de vulnerabilidades en estos activos pone de manifiesto la necesidad de mantener un proceso continuo de gestión y remediación para reducir el riesgo asociado. La métrica general de vulnerabilidades se mantiene en un nivel controlado, lo que refleja la efectividad de las actividades de monitoreo y evaluación implementadas. Se recomienda continuar fortaleciendo el proceso de gestión de vulnerabilidades mediante evaluaciones periódicas, la remediación priorizada de los hallazgos de mayor criticidad y el monitoreo constante de los activos expuestos, con el objetivo de disminuir progresivamente la superficie de ataque y fortalecer la postura de seguridad de la organización.

THREATS

TROPIGAS 07/30/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Internal user deleted or moved a SoftwareMine	216
High Persistency Detection	598
Non Baselined Discovered System	233
MSS-DLP - External File access	310
Threat Intelligence Validation	17
Change in Systems Availability	2
Change in Systems Performance	3

Durante el mes de mayo se evidenció un incremento en la actividad relacionada con el monitoreo de seguridad, la protección de la información y la gestión de activos de la infraestructura tecnológica. El evento con mayor incidencia correspondió a High Persistency Detection, con un total de 598 eventos registrados, lo que refleja una elevada actividad asociada a direcciones IP con antecedentes maliciosos, intentos persistentes de reconocimiento y campañas automatizadas dirigidas contra los servicios expuestos. Adicionalmente, se registraron 310 eventos relacionados con MSS-DLP – External File Access, evidenciando accesos a archivos desde fuentes externas que requirieron validación para descartar posibles riesgos de fuga de información. Asimismo, se identificaron 233 eventos de Non Baselined Discovered System, asociados a la detección de activos no contemplados en la línea base de monitoreo, y 216 eventos correspondientes a Internal User Deleted or Moved a SoftwareMine, vinculados a cambios realizados por usuarios internos sobre archivos o recursos monitoreados. En menor proporción, se registraron 17 eventos de Threat Intelligence Validation, 3 cambios en el rendimiento de los sistemas y 2 cambios en la disponibilidad de servicios. En conjunto, estos resultados reflejan la importancia de mantener un monitoreo continuo, fortalecer la validación de eventos de persistencia y acceso a la información, y asegurar una adecuada gestión de activos para reducir la superficie de riesgo y responder oportunamente ante actividades potencialmente maliciosas.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

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

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