
TLP:AMBER

# BOARDROOM EXECUTIVE REPORT

TROPIGAS

May 07, 2026

TROPIGAS 05/07/2026

# TLP AMBER BOARDROOM

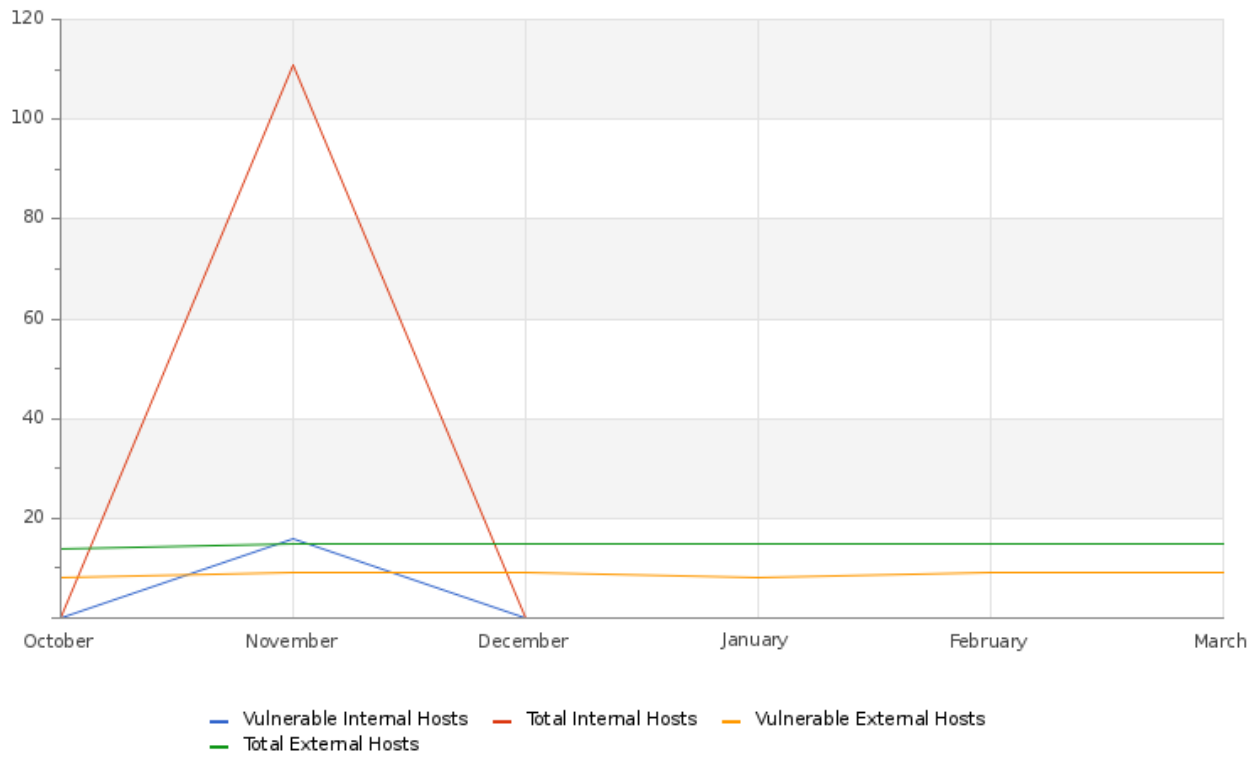
## EXECUTIVE REPORT

Este informe corresponde "FEBRERO 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.

### Hosts & Vulnerable Hosts In Last 6 Months




Durante el mes de septiembre, el número total de hosts externos se ha mantenido estable en 15 a lo largo de los últimos tres meses. En contraste, la cantidad de hosts con vulnerabilidades ha presentado un leve incremento, pasando de 8 a 9. Este comportamiento indica que, aunque la infraestructura se mantiene constante, existe una ligera variación en el nivel de exposición que debe ser atendida. Aun así, las medidas de seguridad implementadas continúan mostrando efectividad en la contención de riesgos. Se recomienda mantener un monitoreo continuo y reforzar las prácticas de gestión de vulnerabilidades, con el fin de identificar oportunamente posibles debilidades y reducir el impacto de riesgos potenciales en el entorno.


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

TROPIGAS 05/07/2026

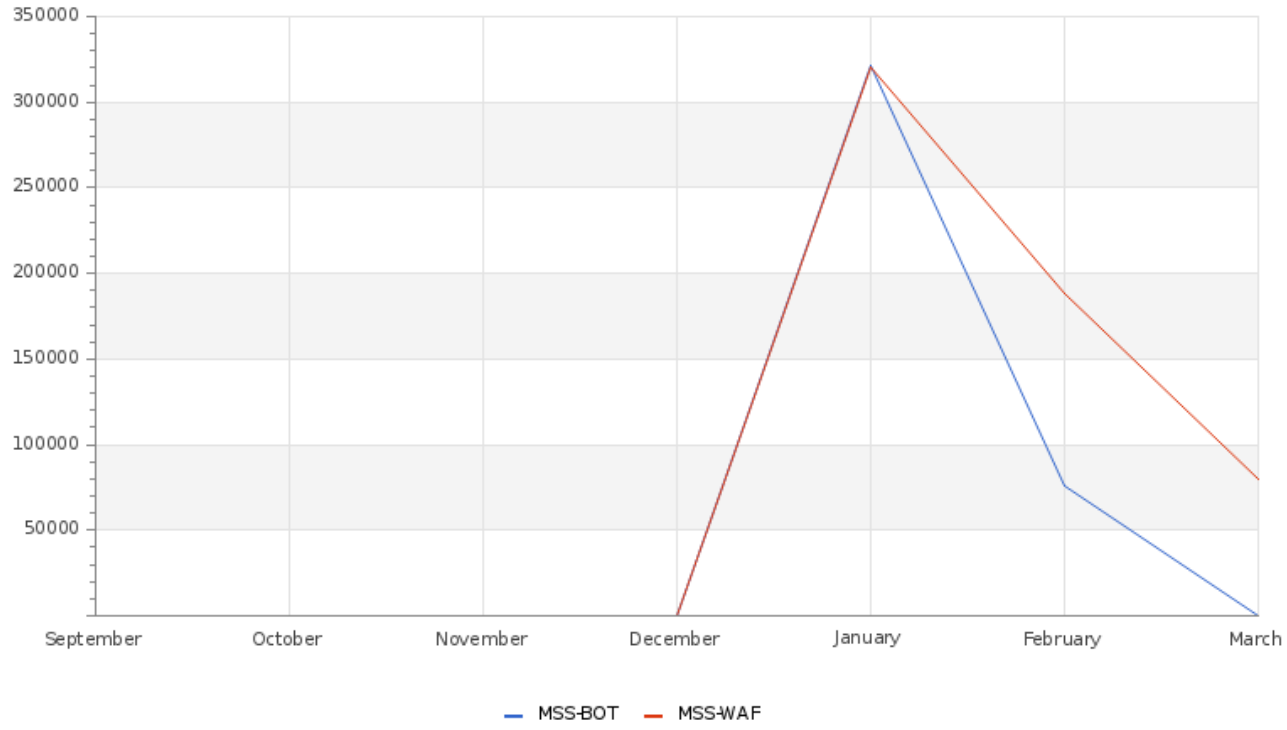
## Total Attacks Successfully Blocked

# 527938

Durante el período evaluado, se bloquearon exitosamente 527,938 intentos de ataque, lo que representa un incremento significativo en comparación con el mes anterior. Este aumento refleja una mayor actividad maliciosa en el entorno durante el período analizado. No obstante, los controles de seguridad demostraron un desempeño sólido, manteniendo su eficacia de forma consistente y asegurando un nivel adecuado de protección frente a las amenazas identificadas.

---

## Attacks Successfully Blocked




En febrero, el número de ataques bloqueados muestra una tendencia relativamente estable, con fluctuaciones moderadas a lo largo del mes. La actividad de MSS-BOT parece haberse reducido significativamente en comparación con períodos anteriores, lo que indica que el pico de intentos de automatización maliciosa fue temporal y que, desde entonces, ha remitido a niveles más bajos.

Por el contrario, MSS-WAF mantiene una presencia más constante, con una ligera tendencia al alza que sugiere intentos continuos de explotar aplicaciones web. Aunque no se observan picos pronunciados durante este mes, la actividad constante refleja un enfoque persistente en los vectores de ataque basados en la web.

Febrero representa un periodo de estabilización, en el que los volúmenes de ataques se mantienen controlados pero continuos. Este comportamiento pone de relieve la importancia de mantener una supervisión activa y controles de seguridad por capas para abordar de forma eficaz las amenazas actuales y en constante evolución.

---


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

TROPIGAS 05/07/2026

## Vulnerability Metric

# 5

El análisis de los 15 hosts registrados en la organización durante el mes evaluado muestra una variación controlada en el número de activos vulnerables, con un incremento de 8 a 9 equipos afectados. En total, se identificaron 16 vulnerabilidades de severidad media y 9 de nivel bajo, lo que sitúa la métrica general de vulnerabilidades en un 5%. Este resultado refleja un nivel de exposición relativamente bajo y gestionable; sin embargo, evidencia la necesidad de mantener y fortalecer las prácticas de gestión de vulnerabilidades. Se recomienda continuar priorizando la remediación de hallazgos de mayor impacto, así como sostener un monitoreo constante que permita reducir progresivamente la superficie de riesgo y asegurar la protección de la infraestructura tecnológica.

---

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

# BOARDROOM 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