TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

April 11, 2026

TROPIGAS 04/11/2026

TLP AMBER CISO
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

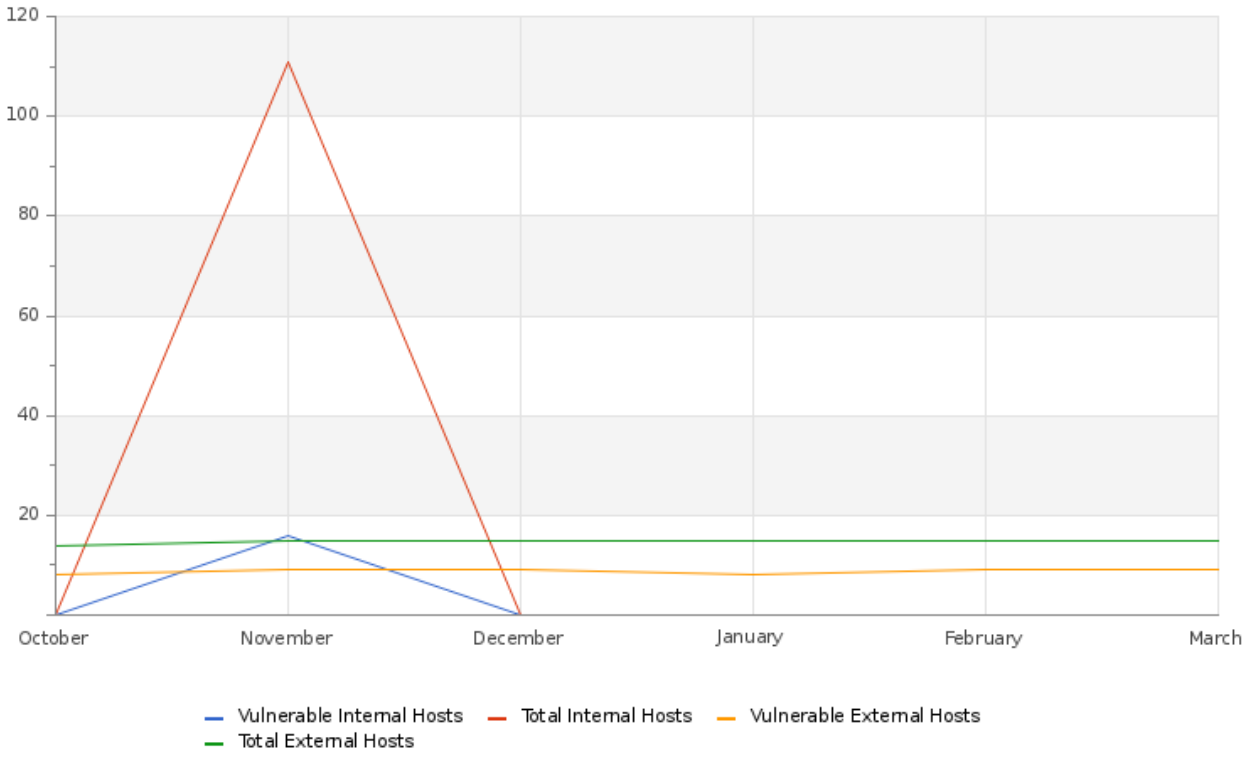
El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

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

TROPIGAS 04/11/2026

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.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	201.226.254.231	1
Current	1	

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

TROPIGAS 04/11/2026

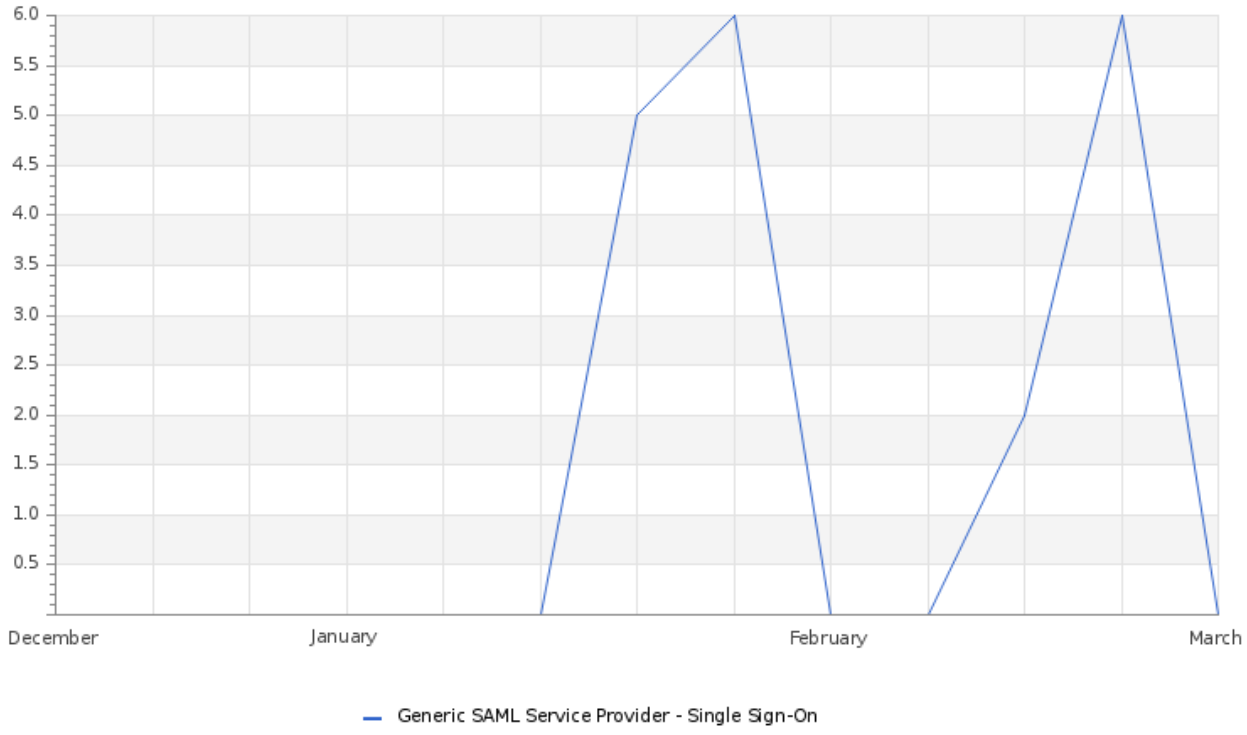
Vulnerability Metric

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.

THREATS

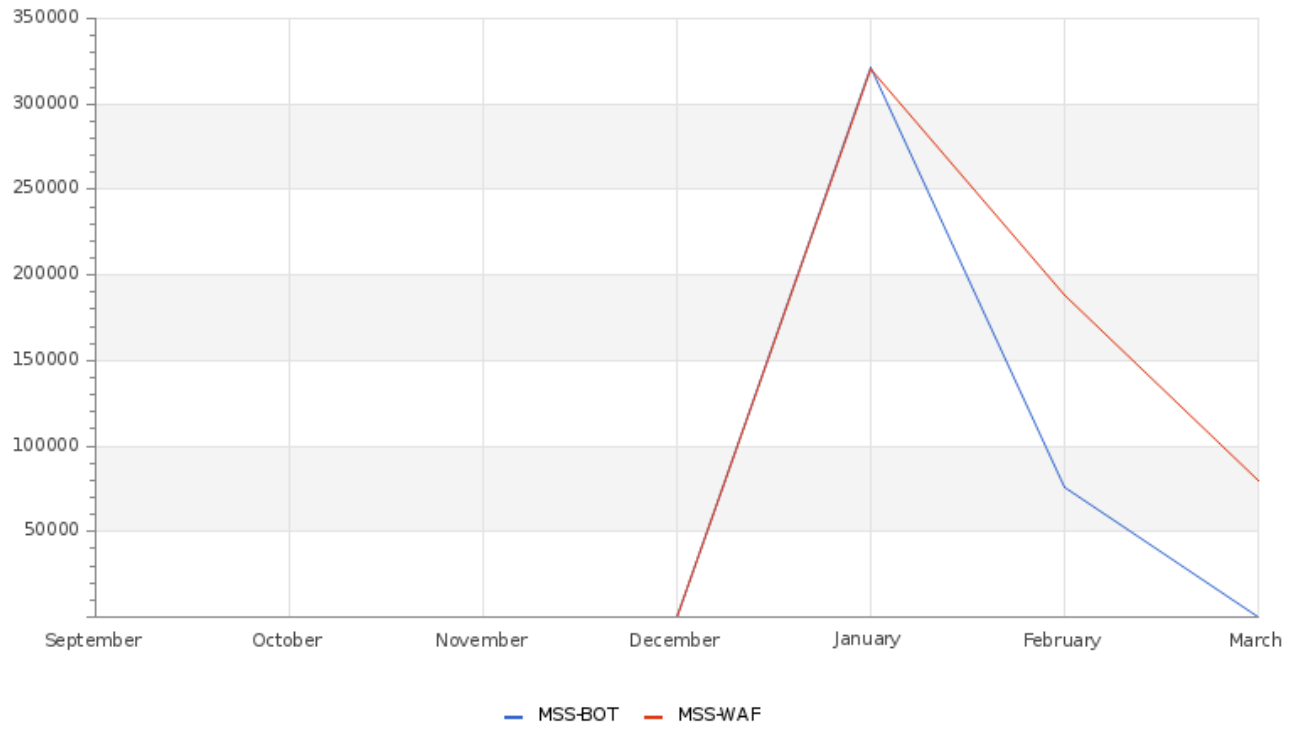
Total Number of Successful MFA authentications per application



La gráfica permite visualizar la actividad del cliente en las diferentes plataformas a las que tiene acceso. Durante el mes de noviembre, se registraron 6 accesos exitosos y 4 intentos denegados en la aplicación "Generic SAML Service Provider Single Sign-On", reflejando el nivel de interacción del usuario y la efectividad de los controles de acceso implementados.

TROPIGAS 04/11/2026

Total Attacks Successfully Blocked Per Service



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.

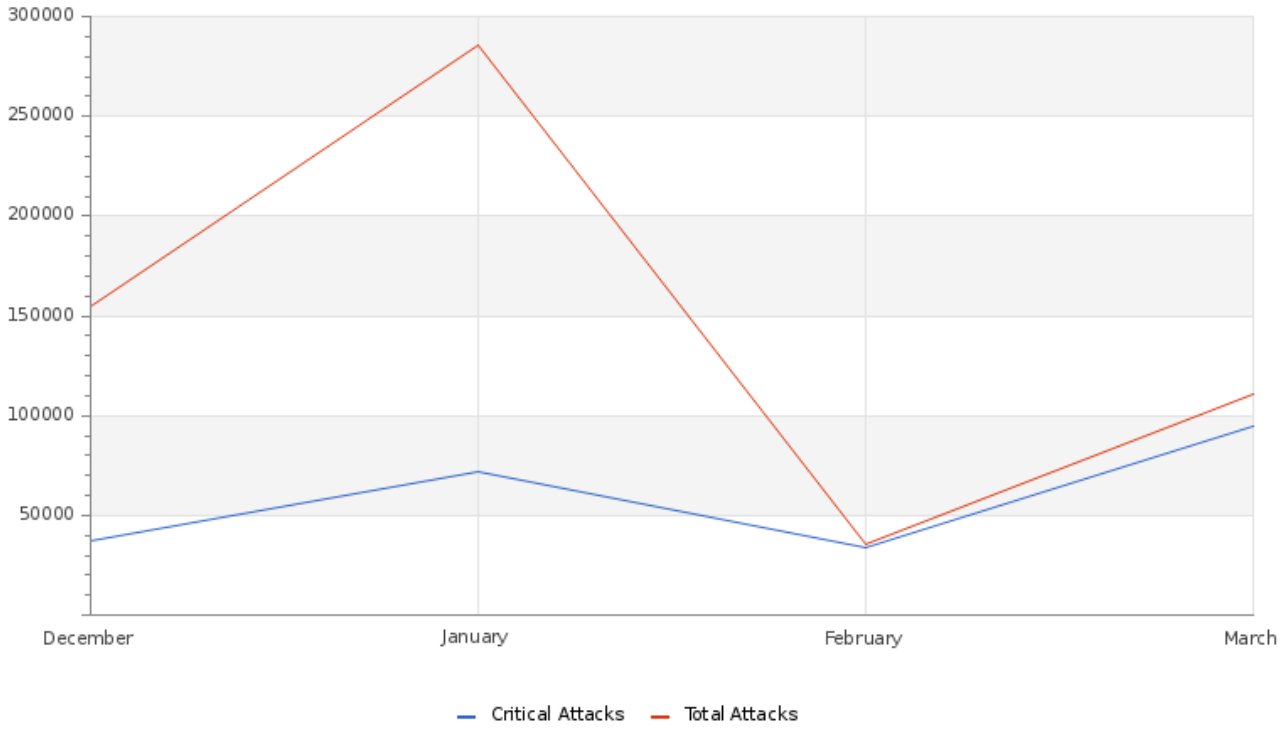
Por el contrario, MSS-WAF mantiene una presencia más constante, con una ligera tendencia al alza que sugiere intentos continuos de explotar aplicaciones web. Aunque no se observan picos pronunciados durante este mes, la actividad constante refleja un enfoque persistente en los vectores de ataque basados 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 04/11/2026

Attacks Successfully Blocked by Severity



Durante el mes de febrero se registró un total aproximado de 80,000 ataques bloqueados, evidenciando una disminución significativa en comparación con el mes de enero, donde se mitigaron aproximadamente350,000 eventos. Esta reducción refleja un comportamiento más estable del entorno y una menor actividad maliciosa durante el período evaluado.
En términos de severidad, no se identificaron incidentes críticos, manteniéndose este indicador en niveles nulos. Asimismo, la totalidad de los eventos bloqueados correspondió a amenazas de baja severidad, lo que evidencia un desempeño consistente de los controles de seguridad, permitiendo una detección oportuna y una mitigación efectiva desde etapas tempranas.

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
192.168.12.22	SSL Certificate Sensor (Port 443)	Clients	Warning		8785	2026-02-10 00:04:50	2026-03-12 14:00:06
Gateway: 10.100.40.1	SSL Certificate Sensor (Port 443)	Network Infrastructure	Warning		8785	2026-02-10 00:04:50	2026-03-12 13:59:59
192.168.12.20	SSL Certificate Sensor (Port 443)	Linux / macOS / Unix	Warning		8180	2026-02-10 00:04:50	2026-03-12 13:59:46
Probe Device	System Health	MSS-CSME-Tropigas	Warning		16	2026-03-02 13:13:09	2026-03-11 22:05:02

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

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	396,660	0	0	0	30,451

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
MSS-DLP - Abnormal activity in the file system(s)	528
BAS Web Security	9
Change in Systems Performance	1
Non Baselined Discovered System	110
Internal user deleted or moved a SoftwareMine	64
Monitoring for open ports	4
MSS-DLP - External File access	10

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.**

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