TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

September 02, 2026

TROPIGAS 09/02/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "AGOSTO 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

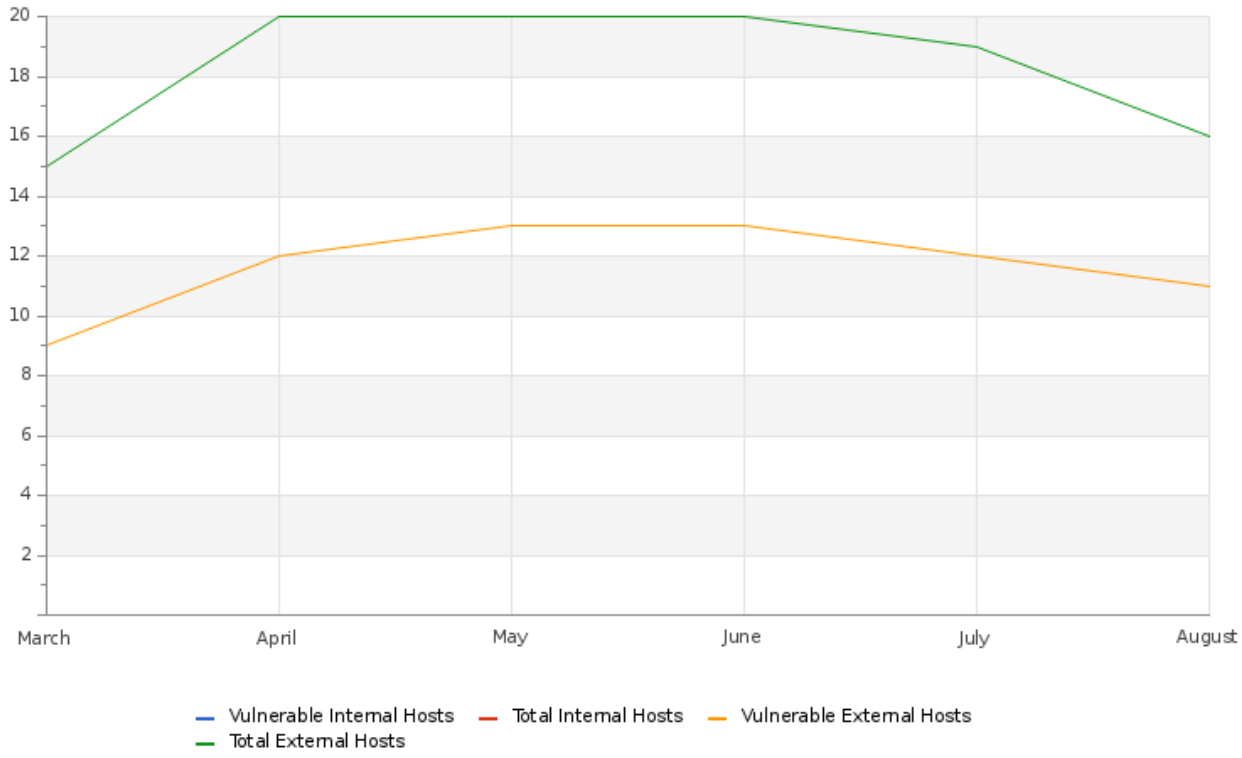
El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

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

TROPIGAS 09/02/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante los últimos meses, la métrica muestra la evolución de los sistemas externos identificados y de los hosts con vulnerabilidades. Entre julio y agosto, los sistemas identificados pasaron de 19 a 16, mientras que los hosts con vulnerabilidades pasaron de 12 a 11. Para agosto, 11 de los 16 sistemas identificados presentaron vulnerabilidades. La comparación refleja una disminución en la cantidad de sistemas expuestos y una ligera reducción en los hosts con vulnerabilidades respecto al período anterior. Se recomienda mantener el seguimiento continuo de los activos expuestos y continuar con las acciones de remediación sobre las vulnerabilidades identificadas.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	controller.tropigas.com.pa	0
Current	6	

Durante agosto de 2026, el activo controller.tropigas.com.pa registró un total de 5 vulnerabilidades, en comparación con las 6 vulnerabilidades identificadas en julio, reflejando una disminución de 6 a 5 vulnerabilidades entre ambos períodos. Entre los hallazgos identificados se encuentran el uso de protocolos criptográficos obsoletos como TLS 1.0 y TLS 1.1, una versión vulnerable de jQuery asociada a múltiples vulnerabilidades XSS, la ausencia de controles de seguridad frente a ataques de Clickjacking y configuraciones que permiten el autocompletado de contraseñas en la aplicación web. Se recomienda mantener el seguimiento de estos hallazgos y priorizar las acciones de remediación correspondientes, especialmente aquellas relacionadas con protocolos obsoletos y componentes de software vulnerables, con el objetivo de reducir la exposición y fortalecer la seguridad del activo.

TROPIGAS 09/02/2026

Vulnerability Metric

8

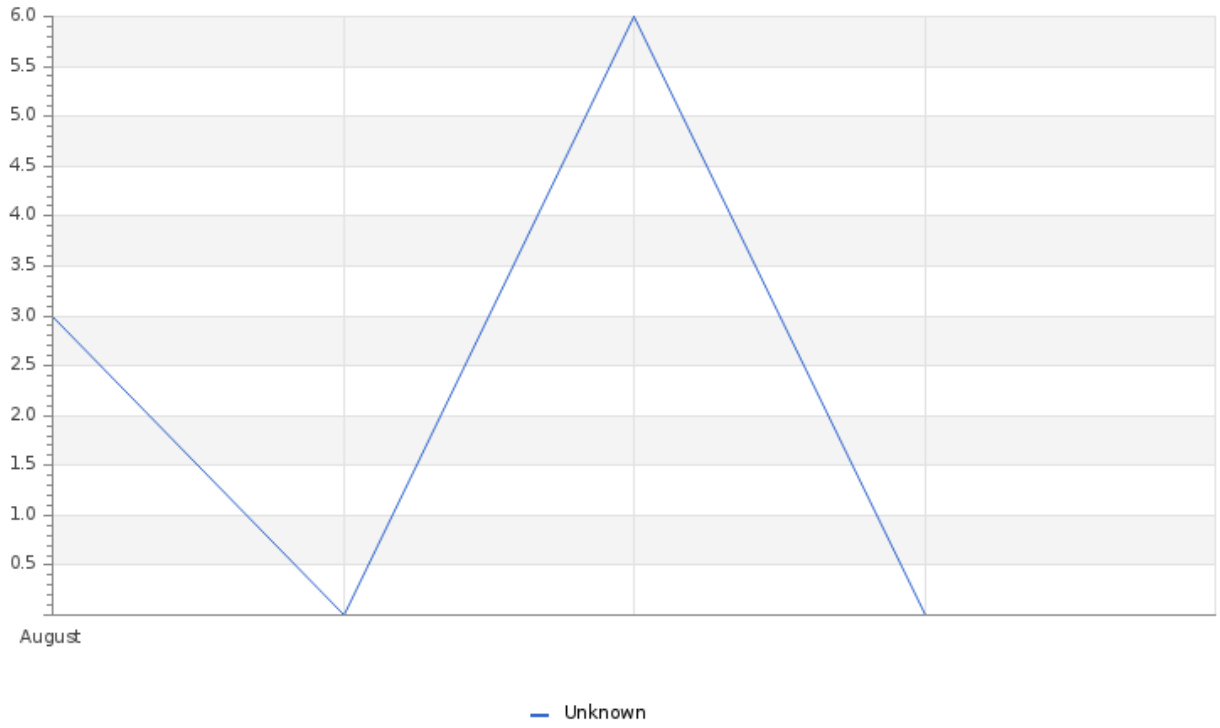
Para el período de agosto de 2026, el análisis de la superficie externa identificó 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, con un total de 25 vulnerabilidades: 17 de severidad media y 8 de severidad baja, sin hallazgos críticos ni altos. Las principales debilidades identificadas durante el período están relacionadas con configuraciones de seguridad web y mecanismos criptográficos, incluyendo ausencia de HSTS, uso de protocolos TLS obsoletos como TLS 1.1, certificados SSL autofirmados, no confiables o próximos a expirar, así como soporte de suites criptográficas asociadas a SWEET32 y divulgación de información de Microsoft Exchange.

Los resultados de agosto muestran una reducción en la cantidad de sistemas expuestos y vulnerabilidades activas respecto al período anterior, aunque persisten oportunidades de fortalecimiento principalmente en las configuraciones SSL/TLS, cabeceras de seguridad y divulgación de información. Por lo anterior, se recomienda mantener el seguimiento continuo de los activos expuestos y las acciones de remediación sobre los hallazgos identificados, priorizando aquellos que puedan incrementar la exposición del entorno.

THREATS

TROPIGAS 09/02/2026

Total Number of Successful MFA authentications per application

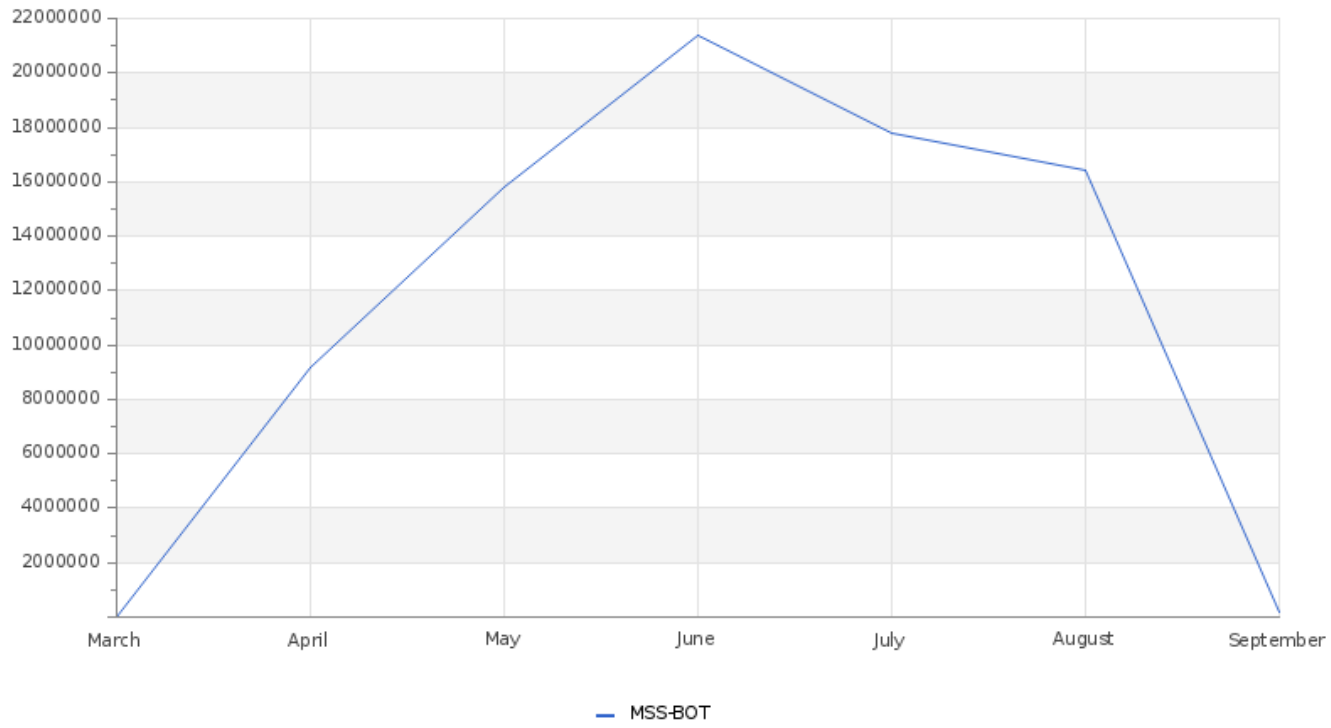


Durante el mes de agosto de 2026 se registraron 9 autenticaciones MFA exitosas correspondientes a la aplicación Generic SAML Service Provider – Single Sign-On. La actividad observada evidencia el uso del mecanismo de autenticación multifactor para el acceso a la plataforma, fortaleciendo los controles de identidad y reduciendo el riesgo de accesos no autorizados. La implementación de MFA constituye una medida de seguridad fundamental para proteger los recursos corporativos, ya que incorpora una capa adicional de verificación durante el proceso de autenticación y contribuye a reforzar la seguridad de los accesos a las aplicaciones monitoreadas.

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

TROPIGAS 09/02/2026

Total Attacks Successfully Blocked Per Service

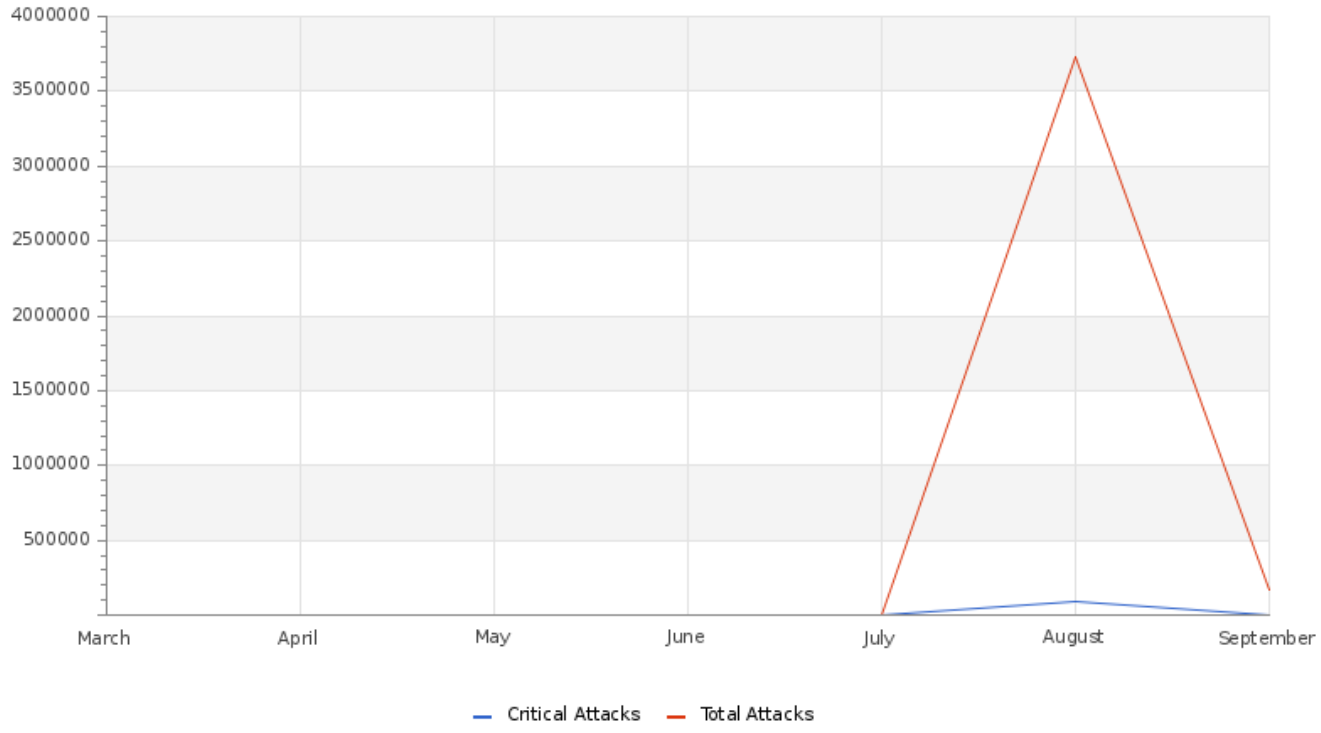


Durante el mes de agosto se registraron 16,422,735 eventos asociados a BOT, frente a 17,641,812 registrados en julio, lo que representa una disminución aproximada del 6.9 %. La actividad observada corresponde a eventos identificados por los mecanismos de protección contra tráfico automatizado. La disminución observada refleja una menor cantidad de eventos asociados a BOT durante agosto; sin embargo, los mecanismos de protección continuaron identificando y gestionando el tráfico automatizado dirigido contra las aplicaciones y servicios protegidos.

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

TROPIGAS 09/02/2026

Attacks Successfully Blocked by Severity



En términos generales, agosto presentó una disminución significativa en la actividad de ataques respecto a julio. Los ataques totales disminuyeron de 6,028,677 a 545,594 (-90.95 %), mientras que los ataques críticos pasaron de 591,415 a 469,845 (-20.58 %). Sin embargo, los eventos críticos representaron una mayor proporción del total, pasando de 9.81 % en julio a 86.11 % en agosto. Esta variación estuvo principalmente influenciada por la ausencia de eventos de Large File Download, que en julio concentró 5,247,013 eventos. Se recomienda mantener el seguimiento sobre los eventos críticos y los patrones de ataque identificados.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	1	1
Critical Device Outages	0	0

Durante el mes de agosto se registró 1 evento de indisponibilidad de dispositivos, manteniendo el mismo nivel observado durante julio. No se registraron indisponibilidades críticas, por lo que se recomienda mantener el monitoreo de la infraestructura y dar seguimiento a las causas de la interrupción para prevenir posibles recurrencias.

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

TROPIGAS 09/02/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Probe Device	System Health	MSS-CSME-Tropigas	Warning		41	2026-08-02 07:50:27	2026-09-01 07:05:34
Probe Device	Probe Health	MSS-CSME-Tropigas	Down		4	2026-08-06 08:20:27	2026-08-12 22:06:44

Se identificaron eventos de estado Warning en System Health y 4 eventos de indisponibilidad (Down) asociados a Probe Health durante agosto.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	34,478,082	0	0	0	68,834

Durante agosto, MSS-BOT registró 16,422,735 eventos asociados a tráfico automatizado, mientras que MSS-WAF registró 545,594 ataques bloqueados, de los cuales 469,845 fueron clasificados como críticos. La actividad observada evidencia una mayor concentración de eventos en los mecanismos de protección contra tráfico automatizado durante el período.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
High Persistency Detection	79
Non Baselined Discovered System	55
MSS-DLP - External File access	117
Internal user deleted or moved a SoftwareMine	78
Change in Systems Availability	1
Change in Systems Performance	2

Durante el mes de agosto se mantuvo una actividad relacionada con el monitoreo de seguridad, la protección de la información y la supervisión de activos dentro de la infraestructura tecnológica. El evento con mayor incidencia correspondió a MSS-DLP – External File Access, con 117 eventos, seguido de High Persistency Detection, con 79 eventos, e Internal User Deleted or Moved a SoftwareMine, con 78 eventos. Asimismo, se registraron 55 eventos de Non Baselined Discovered System, asociados a la detección de activos fuera de la línea base establecida.

En menor proporción, se identificaron 2 eventos de Change in Systems Performance y 1 evento de Change in Systems Availability. En conjunto, los resultados de agosto resaltan la importancia de mantener el monitoreo sobre los accesos a información, la actividad persistente y los activos detectados fuera de línea base.

TROPIGAS 09/02/2026

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