TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

August 06, 2026

TROPIGAS 08/06/2026

TLP AMBER CISO
EXECUTIVE REPORT

Este informe corresponde "JUNIO 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

Hosts & Vulnerable Hosts In Last 6 Months

Durante el mes de junio se evaluó un total de 19 hosts externos, observándose un ligero incremento en la cantidad de activos con vulnerabilidades identificadas, al pasar de 12 a 13 hosts respecto al período anterior. Este comportamiento refleja una variación moderada en la superficie de exposición de la organización, derivada de la identificación de nuevos hallazgos de seguridad durante las evaluaciones realizadas. Aunque el aumento es limitado, pone de manifiesto la necesidad de mantener un proceso continuo de gestión de vulnerabilidades para evitar un incremento progresivo del riesgo. En este contexto, se recomienda priorizar la remediación de las vulnerabilidades detectadas según su nivel de criticidad, realizar evaluaciones periódicas de seguridad y mantener un monitoreo constante de los activos expuestos. Estas acciones contribuirán a reducir la superficie de ataque, fortalecer la postura de ciberseguridad de la organización y minimizar la probabilidad de explotación de vulnerabilidades por parte de actores maliciosos.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	201.226.254.249	0
Current	3	

Durante el mes de junio, el activo 201.226.254.249 registró un total de 3 vulnerabilidades asociadas a la configuración de los servicios criptográficos. Los hallazgos identificados corresponden a SSL Certificate Cannot Be Trusted, SSL Self-Signed Certificate y TLS Version 1.1 Deprecated Protocol, los cuales evidencian debilidades en los mecanismos de autenticación y cifrado utilizados por el servicio. Estas condiciones pueden impedir la validación adecuada de la identidad del servidor y permitir el uso de protocolos criptográficos obsoletos, incrementando el riesgo de ataques de interceptación de comunicaciones (Man-in-the-Middle) y reduciendo el nivel de protección de la información transmitida. Se recomienda reemplazar el certificado autofirmado por uno emitido por una Autoridad Certificadora (CA) confiable, deshabilitar el soporte para TLS 1.1 y habilitar únicamente versiones seguras del protocolo, como TLS 1.2 o TLS 1.3, además de mantener un proceso continuo de evaluación y remediación para fortalecer la postura de seguridad del activo.

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

TROPIGAS 08/06/2026

Vulnerability Metric

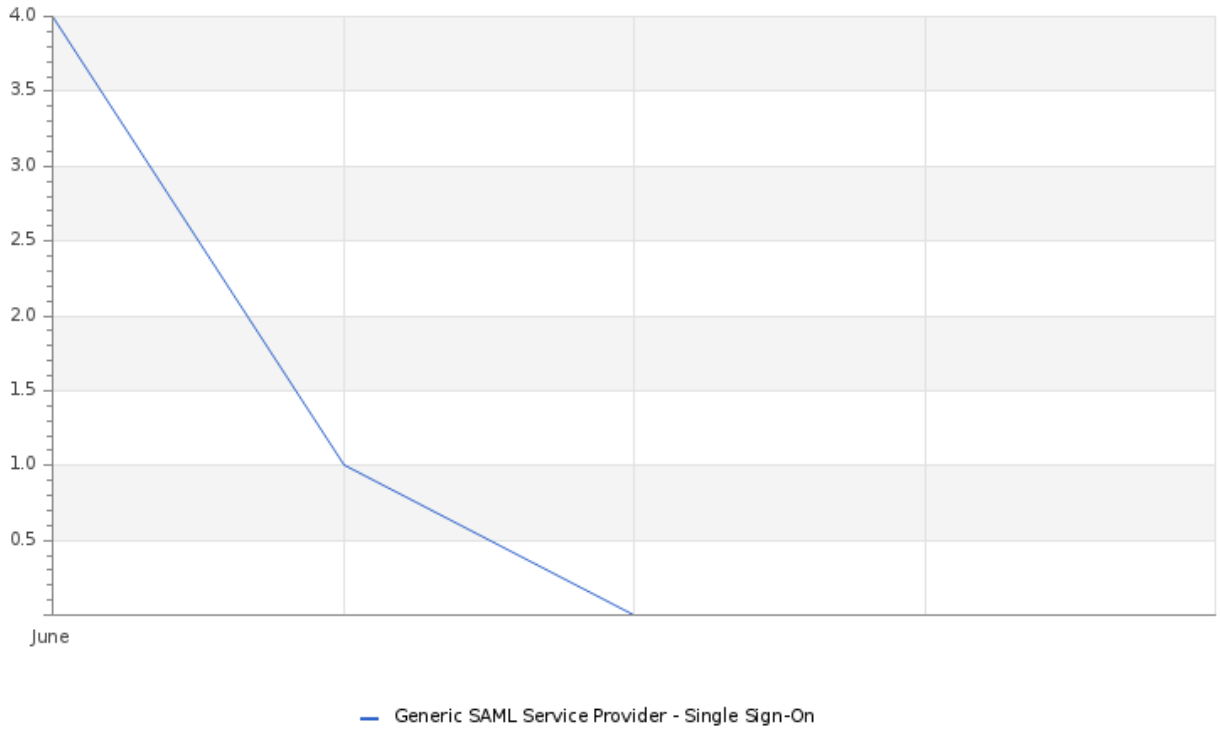
7

El análisis de los 19 activos evaluados durante el mes evidencia un ligero incremento en la superficie de exposición, al registrarse un aumento de 12 a 13 hosts con vulnerabilidades identificadas respecto al período anterior. En total, se detectaron 15 vulnerabilidades, distribuidas en 12 de severidad media y 3 de severidad baja, lo que sitúa la métrica general de vulnerabilidades en un 7%. Aunque este porcentaje refleja una postura de riesgo moderada y un nivel de exposición relativamente controlado, el incremento en la cantidad de activos afectados evidencia la necesidad de reforzar las actividades de gestión de vulnerabilidades. En este contexto, se recomienda priorizar la remediación de las vulnerabilidades de severidad media, complementar estas acciones con evaluaciones periódicas de seguridad y mantener un monitoreo continuo de los activos expuestos. Estas medidas contribuirán a reducir la superficie de ataque, fortalecer la postura de ciberseguridad de la organización y disminuir la probabilidad de explotación de vulnerabilidades por parte de actores maliciosos.

THREATS

TROPIGAS 08/06/2026

Total Number of Successful MFA authentications per application

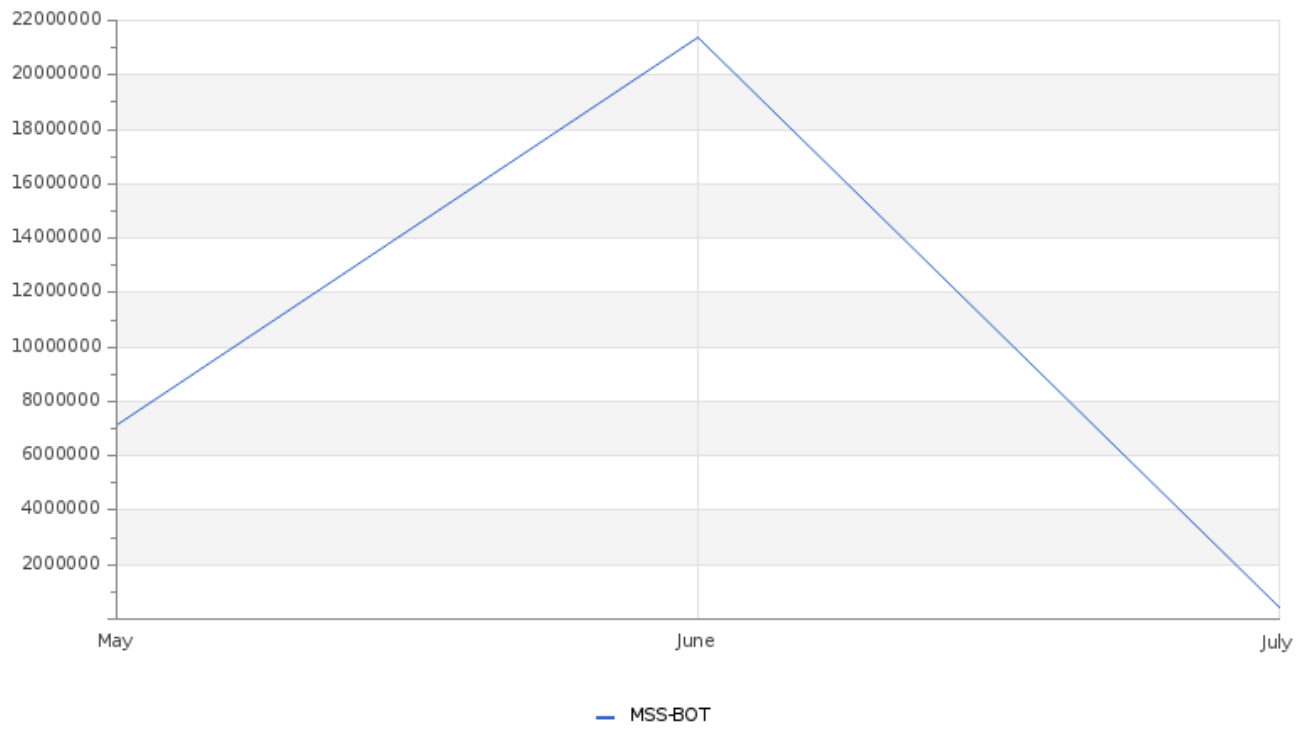


Durante el mes de junio se registraron 4 autenticaciones MFA exitosas correspondientes a la aplicación Generic SAML Service Provider – Single Sign-On. La actividad observada evidencia el uso del mecanismo de autenticación multifactor para el acceso a la plataforma, fortaleciendo los controles de identidad 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 08/06/2026

Total Attacks Successfully Blocked Per Service

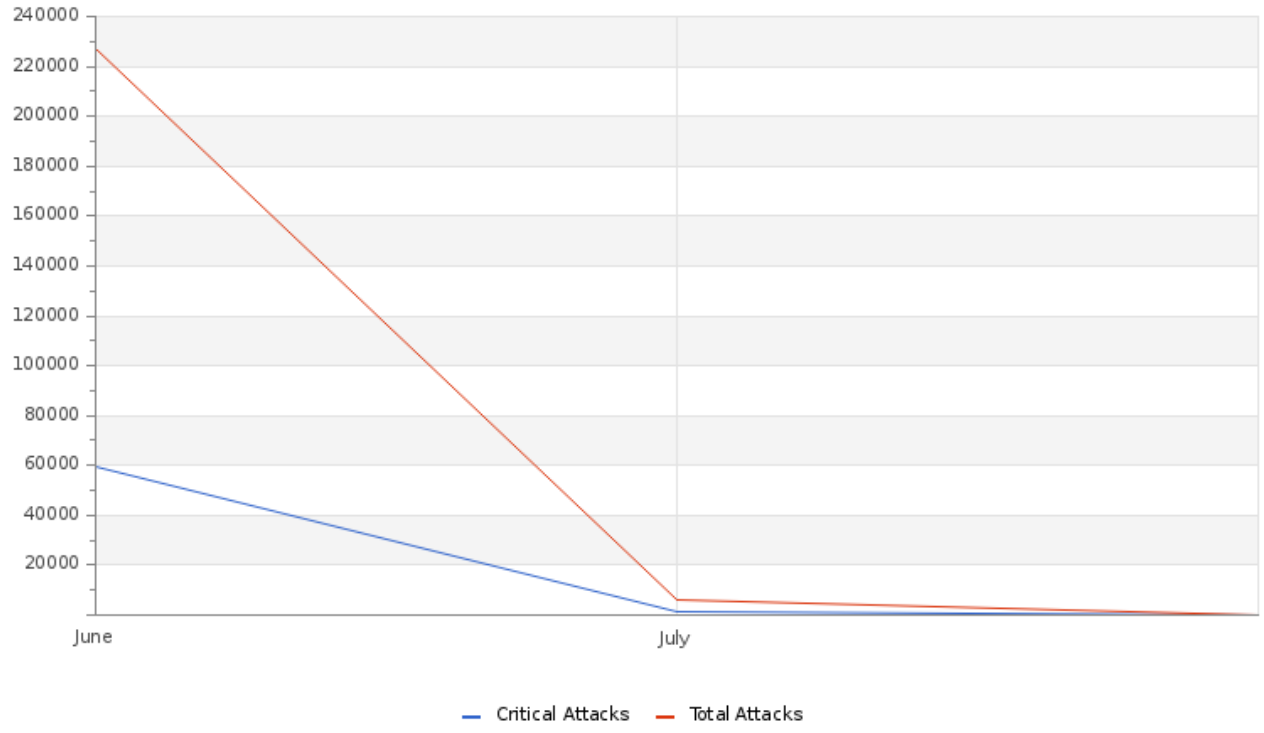


Durante el mes de junio, el servicio MSS-WAF-CLOUD bloqueó un total de 2,483,937 ataques, evidenciando un elevado nivel de actividad maliciosa dirigida contra las aplicaciones web publicadas en Internet. Este volumen incluye intentos automatizados de explotación, reconocimiento, escaneo, abuso de aplicaciones y otros patrones de ataque identificados por los mecanismos de protección del WAF. La mitigación continua de estos eventos demuestra la efectividad del servicio para filtrar tráfico malicioso, preservar la disponibilidad de las aplicaciones y fortalecer la postura de seguridad de la organización frente a amenazas dirigidas a la capa de aplicación

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

TROPIGAS 08/06/2026

Attacks Successfully Blocked by Severity



}La gráfica presenta la tendencia de los ataques bloqueados durante los últimos 30 días y no representa el total de eventos registrados en el mes. En ella se observa una disminución progresiva tanto de los ataques críticos como de los ataques totales hacia el cierre del período analizado. Sin embargo, al considerar las estadísticas consolidadas del mes de junio, el servicio MSS-WAF-CLOUD bloqueó un total de 2,483,937 ataques, de los cuales 66,936 fueron clasificados como críticos. Estos resultados evidencian la alta actividad maliciosa registrada durante junio y la efectividad del servicio para detectar y mitigar oportunamente amenazas dirigidas contra las aplicaciones web protegidas.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	5	1
Critical Device Outages	0	0

Durante el mes de junio se registraron 5 eventos de indisponibilidad de dispositivos, en comparación con 1 evento observado durante el período anterior. Aunque se evidenció un incremento en la cantidad de interrupciones detectadas por la plataforma de monitoreo, no se registraron indisponibilidades críticas, lo que indica que los eventos identificados no alcanzaron un nivel de severidad capaz de comprometer significativamente la continuidad de los servicios monitoreados. No obstante, resulta recomendable analizar las causas de las interrupciones registradas y mantener un monitoreo continuo de la infraestructura, con el fin de identificar tendencias, prevenir recurrencias y garantizar la estabilidad y disponibilidad de los servicios.

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

TROPIGAS 08/06/2026

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		38	2026-06-02 07:41:08	2026-07-01 06:10:45
https://correo.tropigas.com.pa/	https://correo.tropigas.com.pa/	WEB SERVER	Down, Warning		5	2026-06-23 14:34:33	2026-06-23 15:15:25
201.226.254.225	Ping v2	WEB SERVER	Down		3	2026-06-13 04:05:32	2026-06-23 15:10:15
201.226.254.228	Ping v2	WEB SERVER	Down		2	2026-06-23 14:45:06	2026-06-23 14:50:20
Probe Device	Probe Health	MSS-CSME-Tropigas	Down		1	2026-06-25 12:28:02	2026-06-25 12:28:02
201.226.254.228	SSL Certificate Sensor (Port 443)	WEB SERVER	Warning		1	2026-06-23 15:10:33	2026-06-23 15:10:33
201.226.254.228	SSL Security Check (Port 443)	WEB SERVER	Down		1	2026-06-23 15:09:06	2026-06-23 15:09:06
201.226.254.236	Ping v2	WEB SERVER	Down		1	2026-06-23 14:45:06	2026-06-23 14:45:06

El análisis correspondiente al período evaluado evidencia que la mayor concentración de eventos estuvo asociada al monitoreo de la salud de la infraestructura, destacando el Probe Device del grupo MSS-CSME-Tropigas, el cual registró 38 eventos mediante el sensor System Health con estado Warning. La recurrencia de estas alertas sugiere la necesidad de revisar el estado operativo del sistema de monitoreo y validar que sus componentes funcionen de manera estable para garantizar la correcta supervisión de los servicios.

Adicionalmente, se registraron eventos de indisponibilidad sobre el servicio https://correo.tropigas.com.pa/, detectados por el sensor WEB SERVER, así como alertas Ping v2 en los activos 201.226.254.225, 201.226.254.228 y 201.226.254.236, clasificadas con estado Down. Estos eventos podrían estar asociados a interrupciones temporales de conectividad, reinicios programados, mantenimientos o afectaciones puntuales en la disponibilidad de los servicios, por lo que resulta recomendable validar su causa y confirmar que no hayan impactado la operación normal de la infraestructura.

Asimismo, el activo 201.226.254.228 presentó eventos relacionados con los sensores SSL Certificate Sensor (Port 443) y SSL Security Check (Port 443), los cuales evidencian la necesidad de verificar la configuración y el estado de los certificados digitales utilizados por el servicio HTTPS. La revisión periódica de estos componentes resulta fundamental para garantizar la disponibilidad del servicio y mantener un nivel adecuado de seguridad en las comunicaciones cifradas.

En conjunto, los eventos registrados reflejan la importancia de mantener un monitoreo continuo sobre la disponibilidad de los servicios, la conectividad de los activos y el estado de los certificados digitales, permitiendo identificar oportunamente condiciones que puedan afectar la continuidad operativa y la postura de seguridad de la infraestructura monitoreada.

TROPIGAS 08/06/2026

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	10,369,733	0	0	0	1,649,002

Durante el período evaluado se registró un total de 12,018,735 ataques bloqueados por las capas de seguridad implementadas en la infraestructura del cliente. El servicio MSS-BOT concentró la mayor actividad, mitigando 10,369,733 eventos, lo que evidencia una elevada presencia de tráfico automatizado asociado a bots maliciosos, campañas de reconocimiento y solicitudes dirigidas contra los servicios expuestos a Internet. Por su parte, MSS-WAF bloqueó 1,649,002 intentos de ataque orientados a la capa de aplicación, contribuyendo a prevenir posibles intentos de explotación de vulnerabilidades y accesos no autorizados a las aplicaciones web. En conjunto, los resultados demuestran la eficacia de los controles de seguridad implementados para detectar y mitigar oportunamente las amenazas identificadas, fortaleciendo la protección de los servicios expuestos y contribuyendo a mantener la disponibilidad, integridad y seguridad de la infraestructura monitoreada.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
MSS-DLP - External File access	274
High Persistency Detection	528
Internal user deleted or moved a SoftwareMine	151
Non Baselined Discovered System	166
Change in Systems Availability	1
Change in Systems Performance	2

Durante el mes de junio se observó una actividad constante relacionada con el monitoreo de seguridad, la protección de la información y la gestión de activos dentro de la infraestructura tecnológica. El evento con mayor incidencia correspondió a MSS-DLP – External File Access, con un total de 246 eventos registrados, reflejando accesos a archivos desde fuentes externas que requirieron validación para descartar posibles riesgos de fuga de información o accesos no autorizados. Asimismo, se identificaron 495 eventos de High Persistency Detection, asociados a actividad persistente proveniente de direcciones IP con antecedentes maliciosos, intentos reiterados de reconocimiento y campañas automatizadas dirigidas contra los servicios expuestos. Adicionalmente, se registraron 155 eventos de Non Baselined Discovered System, relacionados con la detección de activos fuera de la línea base de monitoreo, y 151 eventos de Internal User Deleted or Moved a SoftwareMine, correspondientes a modificaciones realizadas por usuarios internos sobre archivos o recursos monitoreados. En menor proporción, se presentaron 2 eventos de Change in Systems Performance y 1 evento de Change in Systems Availability, los cuales fueron monitoreados para verificar su impacto sobre la continuidad operativa. En conjunto, estos resultados resaltan la importancia de mantener un monitoreo continuo, fortalecer los controles de protección de la información y asegurar una adecuada gestión de activos, con el fin de 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