



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS
August 19, 2026



TROPIGAS 08/19/2026

TLP AMBER CISO EXECUTIVE REPORT

Este informe corresponde "JULIO 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



Total Vulnerability Counts In Current & Previous Month

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

Durante el período evaluado, el activo controller.tropigas.com.pa registró un total de 6 vulnerabilidades, representando un incremento respecto al mes anterior, en el cual no se habían identificado hallazgos. Entre las vulnerabilidades detectadas se encuentran JQuery 1.2 < 3.5.0 Multiple XSS, Web Application Potentially Vulnerable to Clickjacking, TLS Version 1.0 Protocol Detection, TLS Version 1.1 Deprecated Protocol y Web Server Allows Password Auto-Completion. Estas condiciones evidencian debilidades relacionadas con el uso de componentes web desactualizados, ausencia de controles adecuados contra ataques de Clickjacking, utilización de protocolos criptográficos obsoletos y configuraciones que podrían facilitar la exposición de credenciales. De ser explotadas, estas vulnerabilidades podrían permitir la ejecución de contenido malicioso en el navegador, manipulación de la interacción del usuario, interceptación de comunicaciones o exposición de información sensible. Se recomienda actualizar las librerías web afectadas, implementar encabezados de seguridad contra Clickjacking, deshabilitar TLS 1.0 y TLS 1.1, habilitar únicamente TLS 1.2 o TLS 1.3 y revisar las configuraciones relacionadas con el autocompletado de credenciales, manteniendo evaluaciones periódicas para reducir progresivamente la superficie de exposición del activo.



TROPIGAS 08/19/2026

Vulnerability Metric**5**

El análisis de los 19 activos evaluados durante el período evidencia que la cantidad de hosts con vulnerabilidades identificadas se mantuvo estable en 12, sin variaciones respecto al período anterior. En total, se identificaron 30 vulnerabilidades, de las cuales 22 corresponden a severidad media y 8 a severidad baja, manteniendo la métrica general de vulnerabilidades en un 5 %.

Aunque los resultados reflejan un nivel de exposición relativamente controlado y sin incremento en la cantidad de activos afectados, la permanencia de vulnerabilidades de severidad media indica que aún existen condiciones que podrían ser aprovechadas para ampliar la superficie de ataque o comprometer determinados servicios expuestos.

Por este motivo, se recomienda continuar fortaleciendo las actividades de gestión y remediación, priorizando aquellas vulnerabilidades con mayor impacto potencial sobre la infraestructura. Asimismo, resulta conveniente mantener evaluaciones periódicas de seguridad y un monitoreo continuo de los activos expuestos, con el objetivo de reducir progresivamente la exposición identificada y fortalecer la postura general de ciberseguridad de la organización.

THREATS



TROPIGAS 08/19/2026

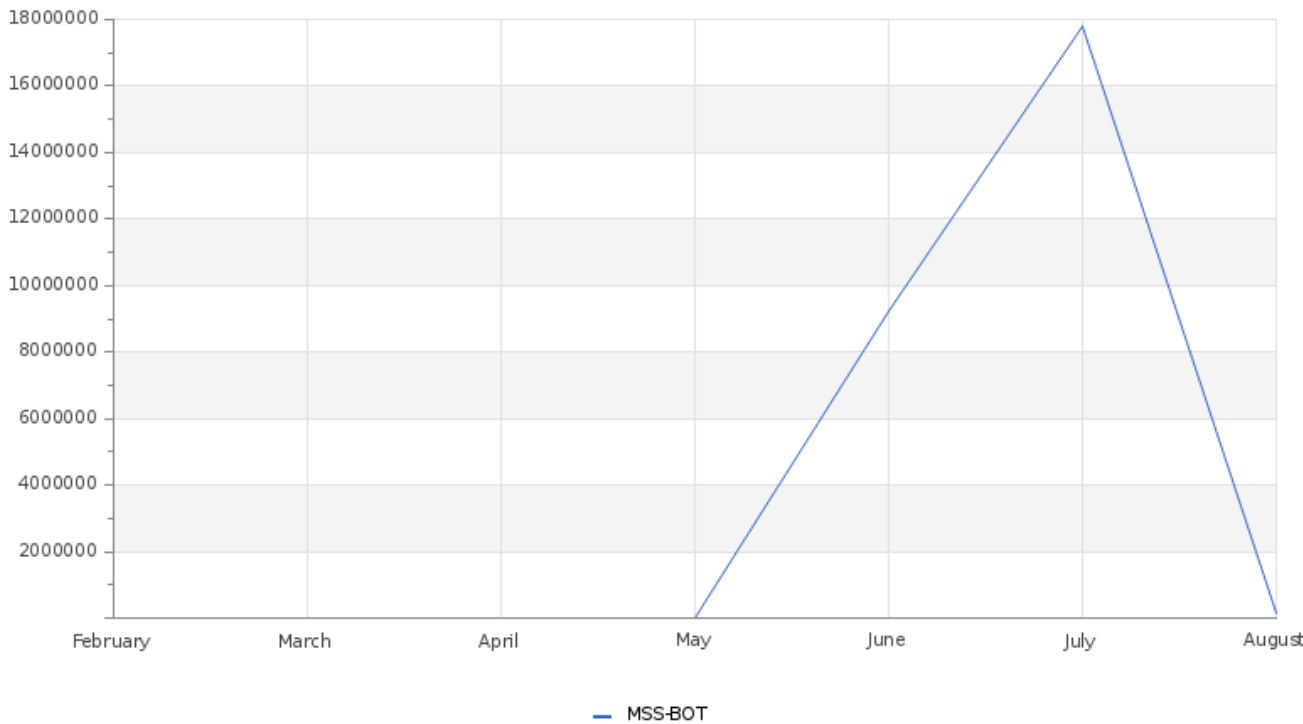
Total Number of Successful MFA authentications per application



Durante el mes de junio se registraron 5 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.

TROPIGAS 08/19/2026

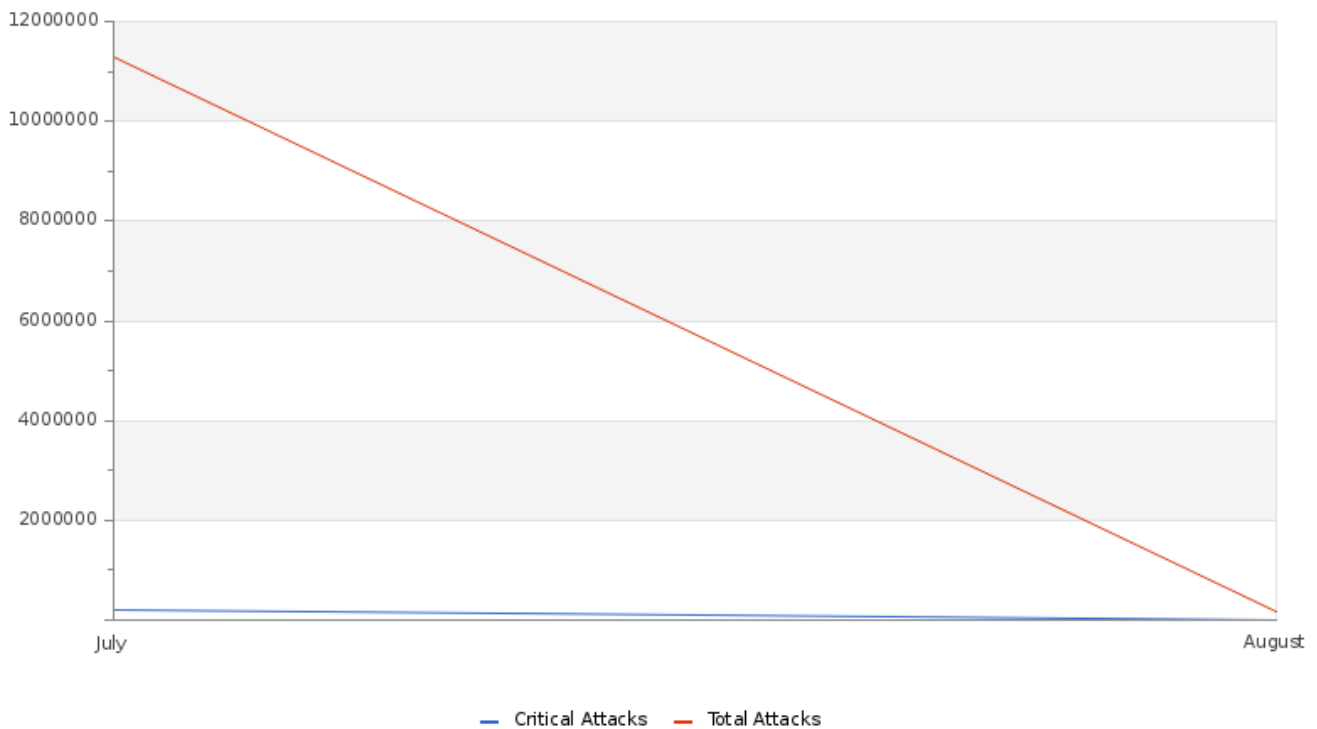
Total Attacks Successfully Blocked Per Service



Durante el mes de julio, el servicio MSS-BOT bloqueó aproximadamente 17.7 millones de ataques, evidenciando un incremento significativo en la actividad automatizada dirigida contra los servicios expuestos de la organización. Este volumen puede estar asociado con tráfico generado por bots maliciosos, actividades de reconocimiento, escaneo automatizado, intentos de enumeración y otras solicitudes masivas orientadas a identificar posibles puntos de acceso o debilidades en la infraestructura. A pesar del elevado volumen registrado, los mecanismos de protección lograron detectar y bloquear oportunamente la actividad identificada, reduciendo el riesgo de accesos no autorizados, abuso de recursos y afectaciones sobre la disponibilidad de los servicios monitoreados. En conjunto, los resultados reflejan la efectividad del servicio MSS-BOT para mitigar amenazas automatizadas y fortalecer la postura de seguridad de la organización frente a este tipo de actividad.

TROPIGAS 08/19/2026

Attacks Successfully Blocked by Severity



La gráfica presenta la tendencia de los ataques bloqueados durante los últimos 30 días y no representa el total consolidado de eventos registrados durante el mes. En ella se observa una disminución en la cantidad de ataques críticos y ataques totales hacia el cierre del período analizado; sin embargo, esta variación debe interpretarse únicamente como parte del comportamiento registrado dentro de la ventana de tiempo mostrada. Al considerar las estadísticas consolidadas del mes de julio, el servicio MSS-WAF-CLOUD bloqueó un total de 13,567,718 ataques, de los cuales 664,779 fueron clasificados como críticos. Estos resultados evidencian un volumen significativo de actividad maliciosa dirigida contra las aplicaciones web protegidas y confirman la efectividad de los mecanismos de seguridad para detectar y mitigar oportunamente los eventos identificados.

System Availability and Performance in current & previous month

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

Durante el mes de junio se registro 1 eventos de indisponibilidad de dispositivos, en comparación al 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.

TROPIGAS 08/19/2026

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		37	2026-07-02 06:14:07	2026-08-01 09:21:32
https://correo.tropigas.com.pa/	https://correo.tropigas.com.pa/	WEB SERVER	Down, Warning		4	2026-07-28 23:57:49	2026-07-29 00:27:54

El análisis correspondiente al período evaluado evidencia que la mayor concentración de eventos estuvo asociada al Probe Device del grupo MSS-CSME-Tropigas, el cual registró un total de 37 eventos mediante el sensor System Health, manteniéndose en estado Warning. La recurrencia de estas alertas indica una condición persistente sobre la salud del sistema de monitoreo, por lo que se recomienda validar el estado operativo del dispositivo y sus componentes, con el objetivo de descartar problemas de rendimiento, disponibilidad o estabilidad que puedan afectar la correcta supervisión de la infraestructura.

Adicionalmente, el servicio <https://correo.tropigas.com.pa/> registró 4 eventos mediante el sensor WEB SERVER, presentando estados Down y Warning durante el período analizado. Este comportamiento evidencia interrupciones o degradaciones puntuales en la disponibilidad del servicio de correo, las cuales podrían estar relacionadas con problemas temporales de conectividad, mantenimiento, reinicios del servicio o afectaciones a nivel del servidor web.

En conjunto, los eventos registrados reflejan la necesidad de mantener un monitoreo continuo sobre la salud del sistema de supervisión y la disponibilidad del servicio de correo, permitiendo identificar oportunamente condiciones recurrentes y aplicar acciones correctivas que contribuyan a preservar la continuidad operativa de los servicios monitoreados.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	22,008,858	0	0	0	129,604

Durante el período evaluado se registró un incremento significativo en la actividad de ataques bloqueados, destacando el servicio MSS-BOT con aproximadamente 22 millones de eventos mitigados, mientras que MSS-WAF bloqueó alrededor de 129 mil intentos de ataque. Este comportamiento evidencia una elevada presencia de tráfico automatizado, actividades de reconocimiento y solicitudes potencialmente maliciosas dirigidas contra aplicaciones y servicios expuestos a Internet. A pesar del volumen observado, los mecanismos de protección demostraron una respuesta efectiva, bloqueando oportunamente la actividad identificada y reduciendo el riesgo de afectación sobre la infraestructura monitoreada. En conjunto, los resultados reflejan la efectividad de los servicios MSS-BOT y MSS-WAF frente a amenazas automatizadas y ataques dirigidos a la capa de aplicación.

TROPIGAS 08/19/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
High Persistency Detection	320
Internal user deleted or moved a SoftwareMine	96
Non Baselined Discovered System	81
MSS-DLP - External File access	200
Change in Systems Performance	2
Change in Systems Availability	1

Durante el mes de julio se mantuvo una actividad constante 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 High Persistency Detection, con un total de 320 eventos, asociados a actividad persistente proveniente de fuentes con comportamiento potencialmente malicioso, intentos reiterados de reconocimiento y patrones automatizados dirigidos contra los servicios expuestos.

Asimismo, se registraron 200 eventos de MSS-DLP – External File Access, relacionados con accesos a archivos desde fuentes externas que requirieron validación para descartar posibles riesgos de fuga de información o accesos no autorizados. Adicionalmente, se identificaron 96 eventos de Internal User Deleted or Moved a SoftwareMine, correspondientes a modificaciones realizadas por usuarios internos sobre archivos o recursos monitoreados, y 81 eventos de Non Baselined Discovered System, asociados a la detección de activos fuera de la línea base establecida.

En menor proporción, se registraron 2 eventos de Change in Systems Performance y 1 evento de Change in Systems Availability, los cuales fueron monitoreados para verificar posibles afectaciones sobre el rendimiento y la continuidad operativa. En conjunto, los resultados de julio resaltan la importancia de mantener un monitoreo continuo sobre la actividad persistente, los accesos a información sensible y los cambios asociados a usuarios y activos, con el objetivo de reducir la superficie de riesgo y responder oportunamente ante comportamientos anómalos o potencialmente maliciosos.

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.**



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

