

TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

November 11, 2026



©2023. GLESEC. All Rights Reserved.

TROPIGAS 11/11/2026

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.

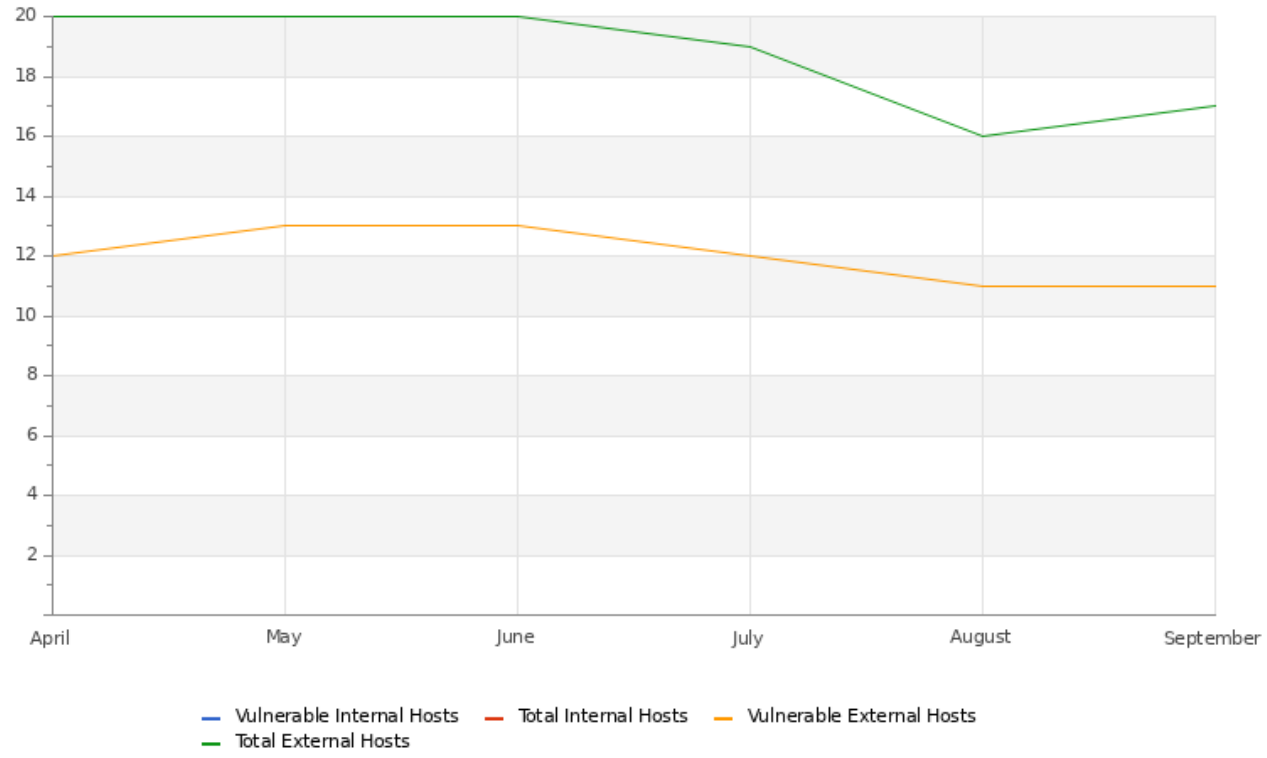
VULNERABILITY

©2023. GLESEC. All Rights Reserved.

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

TROPIGAS 11/11/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante los últimos seis meses se observa una reducción reciente tanto en la cantidad de sistemas descubiertos como en los hosts con vulnerabilidades. Para agosto, se identificaron 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas. Asimismo, la tendencia de vulnerabilidades muestra un total de 25, distribuidas en 17 de severidad media y 8 de severidad baja, sin identificarse vulnerabilidades de severidad alta o crítica. Esta evolución refleja una disminución de las vulnerabilidades externas identificadas; sin embargo, la permanencia de vulnerabilidades medias y bajas en los activos identificados requiere mantener las acciones de remediación y seguimiento para continuar disminuyendo la superficie de ataque.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 11/11/2026

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	controller.tropigas.com.pa	0
Current	5	

Durante el período evaluado, el activo "controller.tropigas.com.pa" registró un total de 5 vulnerabilidades, representando una disminución respecto al mes anterior, en el cual se habían identificado 6 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.

Vulnerability Metric

8

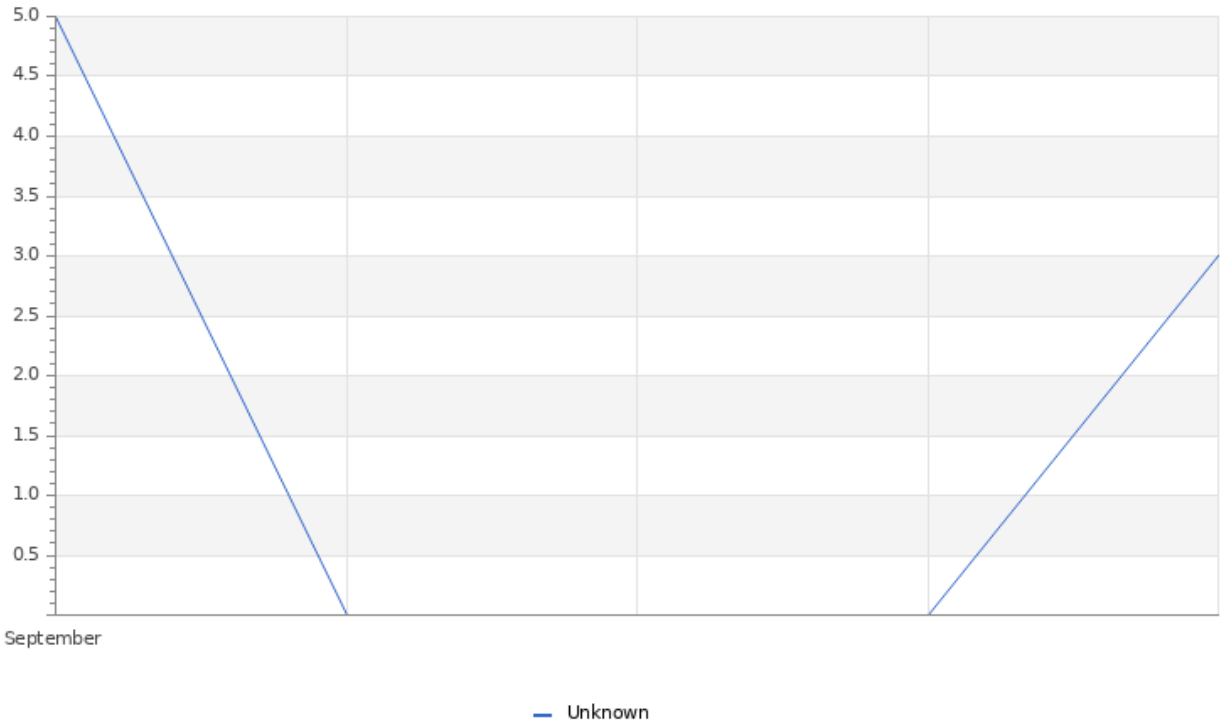
El análisis de la superficie externa identificó 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, con un total de 25 vulnerabilidades externas: 17 de severidad media y 8 de severidad baja, sin hallazgos críticos ni altos. Las principales debilidades están relacionadas con configuraciones de servicios web, protocolos criptográficos obsoletos, certificados digitales y exposición de información. Entre los hallazgos identificados, la vulnerabilidad ICMP Timestamp Request Remote Date Disclosure presentó la mayor recurrencia, siendo detectada en cinco activos. Aunque estos hallazgos no presentan una criticidad elevada de manera individual, su presencia puede ampliar la superficie de ataque y proporcionar información útil para actividades de reconocimiento, por lo que se recomienda fortalecer las configuraciones de seguridad de los servicios web, actualizar los protocolos criptográficos, mantener los certificados digitales vigentes y restringir la exposición innecesaria de información.

THREATS

©2023. GLESEC. All Rights Reserved.

TROPIGAS 11/11/2026

Total Number of Successful MFA authentications per application



Durante el mes de agosto 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.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	2	0
Critical Device Outages	0	0

Durante el mes de agosto se registraron 2 eventos de indisponibilidad de dispositivos, en comparación con 1 evento registrado en el período anterior, lo que representa un incremento en la cantidad de interrupciones detectadas por la plataforma de monitoreo. Aunque se evidenció un aumento en las interrupciones registradas, no se presentaron 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.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 11/11/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
201.226.254.228	SSL Certificate Sensor (Port 443)	WEB SERVER	Warning		6198	2026-09-09 18:15:12	2026-10-01 08:57:03
www.tropigas.com.pa	www.tropigas.com.pa	Network Discovery	Down		62	2026-09-03 23:33:08	2026-09-04 02:03:38
Probe Device	System Health	MSS-CSME-Tropigas	Warning		52	2026-09-01 07:05:34	2026-10-01 07:41:49
Probe Device	Probe Health	MSS-CSME-Tropigas	Down		3	2026-09-14 06:06:04	2026-09-22 08:12:05
https://correo.tropigas.com.pa/	https://correo.tropigas.com.pa/	WEB SERVER	Warning		2	2026-09-01 23:54:24	2026-09-01 23:59:25

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	31,235,138	0	0	0	78,912

Durante el período evaluado, se observa una actividad significativa de ataques gestionados por las diferentes capas de seguridad, con mayor presencia de eventos asociados a MSS-BOT y MSS-WAF. En este indicador, los 31,235,138 eventos registrados por MSS-BOT corresponden a un valor acumulado, mientras que los 78,912 eventos de MSS-WAF reflejan la actividad registrada durante los últimos días del período. Estos resultados evidencian una presencia sostenida de tráfico automatizado y solicitudes potencialmente maliciosas dirigidas contra las aplicaciones y servicios expuestos, las cuales fueron identificadas y bloqueadas por los controles de seguridad implementados.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

TROPIGAS 11/11/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
High Persistency Detection	115
Internal user deleted or moved a SoftwareMine	72
Non Baselined Discovered System	106
MSS-DLP - External File access	68
Change in Systems Performance	3
Change in Systems Availability	12

Durante el mes de agosto 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 115 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 106 eventos de Non Baselined Discovered System, asociados a la detección de activos fuera de la línea base establecida. Adicionalmente, se identificaron 72 eventos de Internal User Deleted or Moved a SoftwareMine, correspondientes a modificaciones realizadas por usuarios internos sobre archivos o recursos monitoreados, y 68 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.

En menor proporción, se registraron 12 eventos de Change in Systems Availability y 3 eventos de Change in Systems Performance, los cuales fueron monitoreados para verificar posibles afectaciones sobre la continuidad operativa y el rendimiento de la infraestructura. En conjunto, los resultados de agosto 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.**

©2023. GLESEC. All Rights Reserved.

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.

©2023. GLESEC. All Rights Reserved.

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