



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# CISO EXECUTIVE REPORT

TROPIGAS

May 14, 2026



TROIPIGAS 05/14/2026

# 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

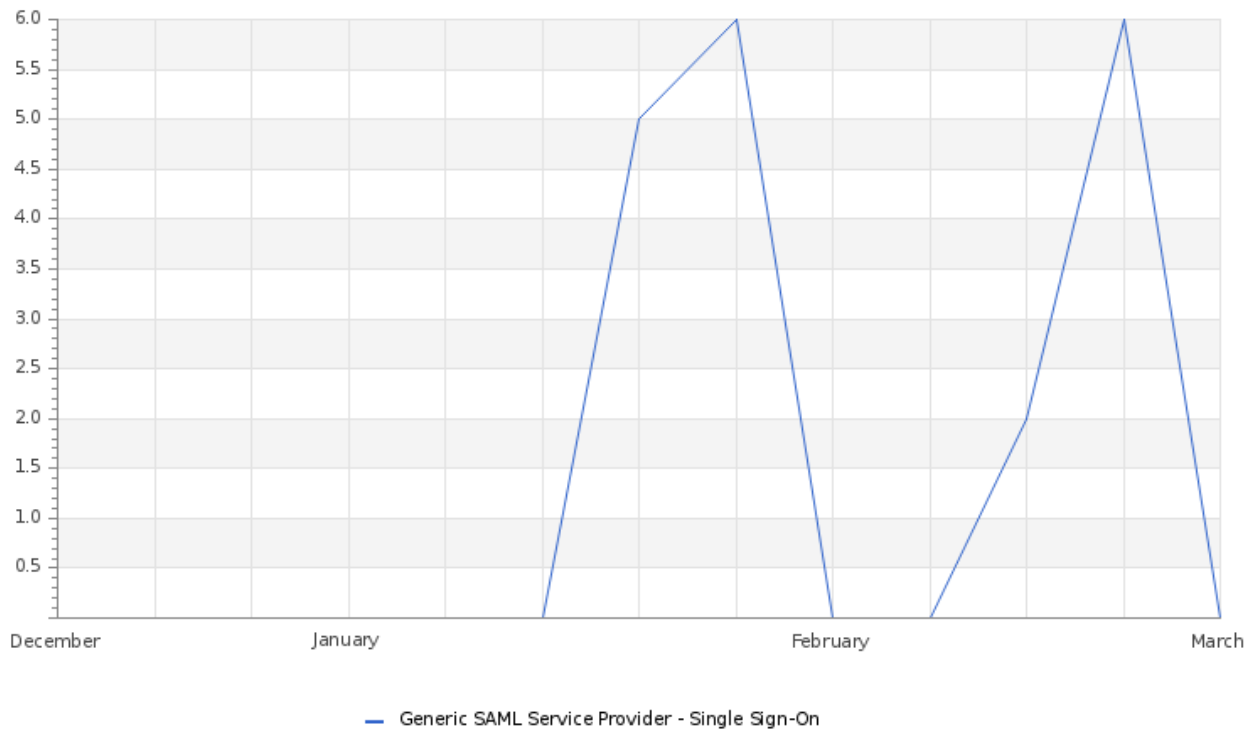
El propósito de este documento es informar sobre el estado de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

## VULNERABILITY

## THREATS

TROPIGAS 05/14/2026

### 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.

TROIIGAS 05/14/2026

## 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

El análisis correspondiente al período evaluado evidencia la generación sostenida de alertas asociadas al monitoreo de certificados SSL/TLS sobre servicios expuestos mediante el puerto 443 en activos críticos de la infraestructura. Los dispositivos 192.168.12.22, Gateway: 10.100.40.1 y 192.168.12.20 registraron eventos a través del sensor “SSL Certificate Sensor (Port 443)”, todos clasificados bajo estado Warning, indicando anomalías relacionadas con la gestión criptográfica de los servicios HTTPS publicados.

Las alertas detectadas pueden estar asociadas a certificados expirados o próximos a su vencimiento, inconsistencias en la cadena de confianza (CA), algoritmos criptográficos obsoletos, errores en la validación del Common Name (CN) o Subject Alternative Name (SAN), así como configuraciones TLS inseguras o incompletas. Este tipo de condición puede impactar directamente la disponibilidad, integridad y confiabilidad de las comunicaciones cifradas, además de incrementar la superficie de exposición frente a ataques de interceptación, degradación criptográfica o pérdida de confianza por parte de clientes y servicios consumidores.

En términos de criticidad acumulada, el activo 192.168.12.22 presentó el mayor volumen de eventos con un total de 8,785 registros desde el 10 de febrero de 2026, seguido por el host 192.168.12.20 con 8,180 eventos. Asimismo, el Gateway 10.100.40.1 reflejó igualmente 8,785 eventos asociados a componentes de infraestructura de red, lo que podría representar un riesgo operativo significativo en caso de que los certificados afectados pertenezcan a servicios productivos, plataformas corporativas o recursos accesibles externamente.

## 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

El análisis correspondiente al período evaluado evidencia que la capa MSS-BOT se consolidó como el principal mecanismo de defensa frente a actividades automatizadas y tráfico malicioso, registrando un total de 396,660 ataques bloqueados exitosamente. Este volumen representa la mayor concentración de eventos detectados dentro de las capas de seguridad monitoreadas, lo que sugiere una alta actividad relacionada con bots automatizados, intentos de scraping, reconocimiento, abuso de aplicaciones web o campañas automatizadas dirigidas contra los servicios expuestos.

Asimismo, la capa MSS-WAF reportó el bloqueo de 30,451 ataques, reflejando una actividad constante orientada a la explotación de aplicaciones web y posibles intentos de acceso no autorizado, validación de vulnerabilidades o ejecución de patrones maliciosos sobre los recursos publicados. La correcta actuación de esta capa demuestra la efectividad de las reglas de protección y mitigación implementadas para salvaguardar los entornos web críticos.

TROPIGAS 05/14/2026

# OPERATIONAL

## Notable Events Active For The Last Month

Notable Event Type	How Many #
MSS-DLP - Abnormal activity in the file system(s)	603
BAS Web Security	9
Change in Systems Performance	1
Non Baselined Discovered System	164
Internal user deleted or moved a SoftwareMine	99
Monitoring for open ports	10
MSS-DLP - External File access	119
High Persistency Detection	117
BAS Immediate Threat	19
Notable Event Alert: Vulnerability exposure from Threat Intelligence	1
TEVR BAS Immediate Threats	1
Change in Systems Availability	1

Durante el período en cuestión, se ha identificado una actividad considerable relacionada con eventos de seguridad, monitoreo operativo y control de activos dentro de la infraestructura tecnológica. El evento con mayor recurrencia correspondió a MSS-DLP - Abnormal activity in the file system(s), con un total de 603 registros, lo que evidencia comportamientos anómalos asociados al acceso, modificación, movimiento o manipulación de archivos dentro de sistemas monitoreados. Esta actividad puede estar relacionada con transferencias no autorizadas, cambios masivos en información sensible, ejecución de procesos inusuales o posibles intentos de exfiltración de datos, lo que representa un riesgo relevante para la integridad y confidencialidad de la información corporativa.

Asimismo, se detectaron 164 eventos de Non Baselined Discovered System, lo que indica la presencia de activos que no cumplen con las configuraciones base definidas o que no han sido correctamente integrados dentro de los procesos de control e inventario corporativo. Este comportamiento constituye una debilidad significativa desde la perspectiva de la gestión de activos, el refuerzo de la seguridad y el cumplimiento de las políticas de seguridad, lo que potencialmente aumenta la superficie de exposición frente a amenazas internas o externas.

En lo que respecta a las actividades asociadas a la persistencia y los accesos externos, se han registrado un total de 119 eventos de MSS-DLP - External File Access y 117 eventos de High Persistency Detection. Estos indicadores podrían estar relacionados con accesos recurrentes a archivos sensibles, mecanismos de persistencia no habituales, ejecución sostenida de procesos o comportamientos potencialmente vinculados a actividades maliciosas avanzadas dentro del entorno monitoreado. La combinación de ambos tipos de eventos subraya la importancia de mantener una supervisión continua sobre los usuarios, los procesos y los sistemas que tienen acceso a información crítica.

Adicionalmente, se identificaron 99 eventos relacionados con Internal user deleted or moved a SoftwareMine, lo que refleja acciones internas de modificación o desplazamiento de recursos monitoreados. Aunque este tipo de actividad puede corresponder a tareas administrativas legítimas, también podría representar riesgos asociados a alteraciones no autorizadas, pérdida de trazabilidad o eliminación accidental de componentes críticos.

Por otro lado, se registraron eventos de menor volumen, pero igualmente relevantes desde el punto de vista de seguridad,

TROPIGAS 05/14/2026

incluyendo 19 eventos de BAS Immediate Threat, 10 eventos de Monitoring for open ports, 9 eventos de BAS Web Security, así como eventos individuales relacionados con exposición de vulnerabilidades provenientes de inteligencia de amenazas, cambios en disponibilidad de sistemas y variaciones en el rendimiento operacional. Aunque su frecuencia fue reducida, este tipo de alertas puede representar indicadores tempranos de exposición, degradación operacional o intentos de explotación sobre servicios tecnológicos.

**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.

