TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

September 01, 2026

TLP AMBER BOARDROOM

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.

Actual Risk

n/a

Durante junio no se identificaron amenazas activas que permitieran establecer un nivel cuantificable de riesgo actual. Aunque permanecen hallazgos de vulnerabilidad y actividad de seguridad bajo monitoreo, los controles implementados continúan limitando la exposición observada durante el período

Accepted Risk

n/a

El análisis se mantiene enfocado en los riesgos identificados y en las condiciones observadas durante el monitore

Confidence

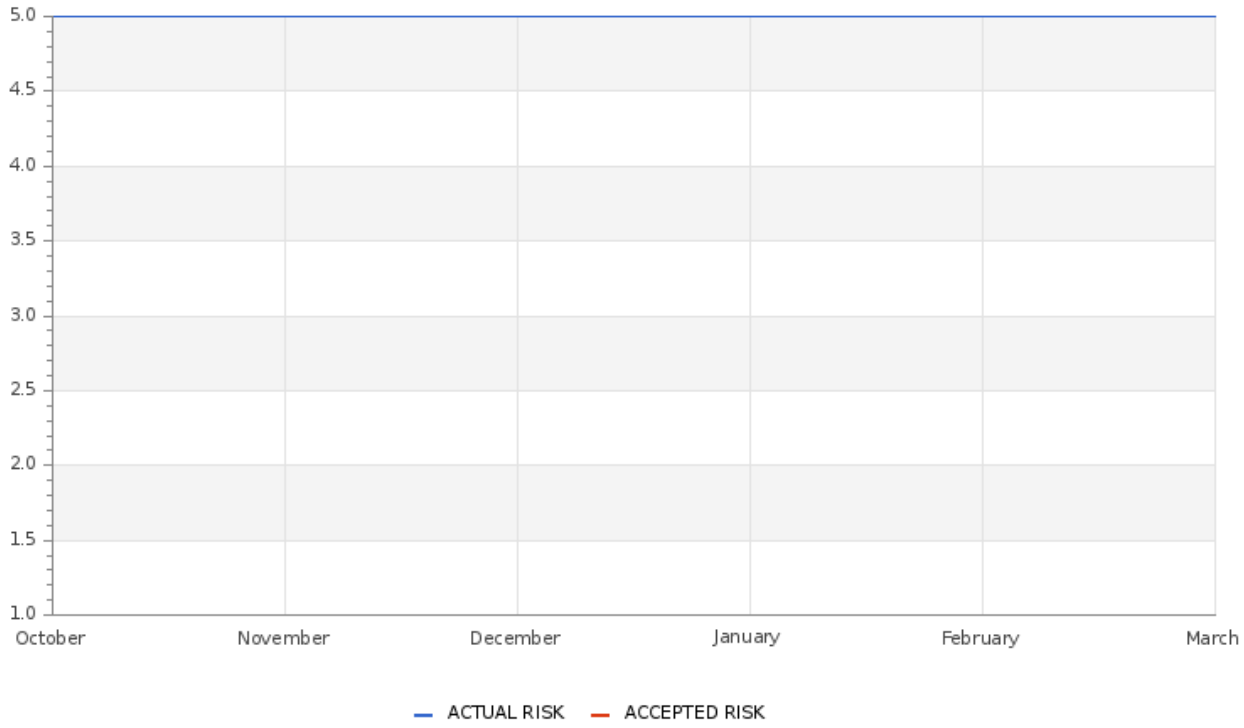
Low

El nivel de confianza se mantiene en Low, debido a que la visibilidad disponible continúa siendo parcial y no se cuenta con la integración completa de todas las fuentes necesarias para realizar una valoración integral del riesgo.

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

Organo Judicial 09/01/2026

Accepted & Actual Risk

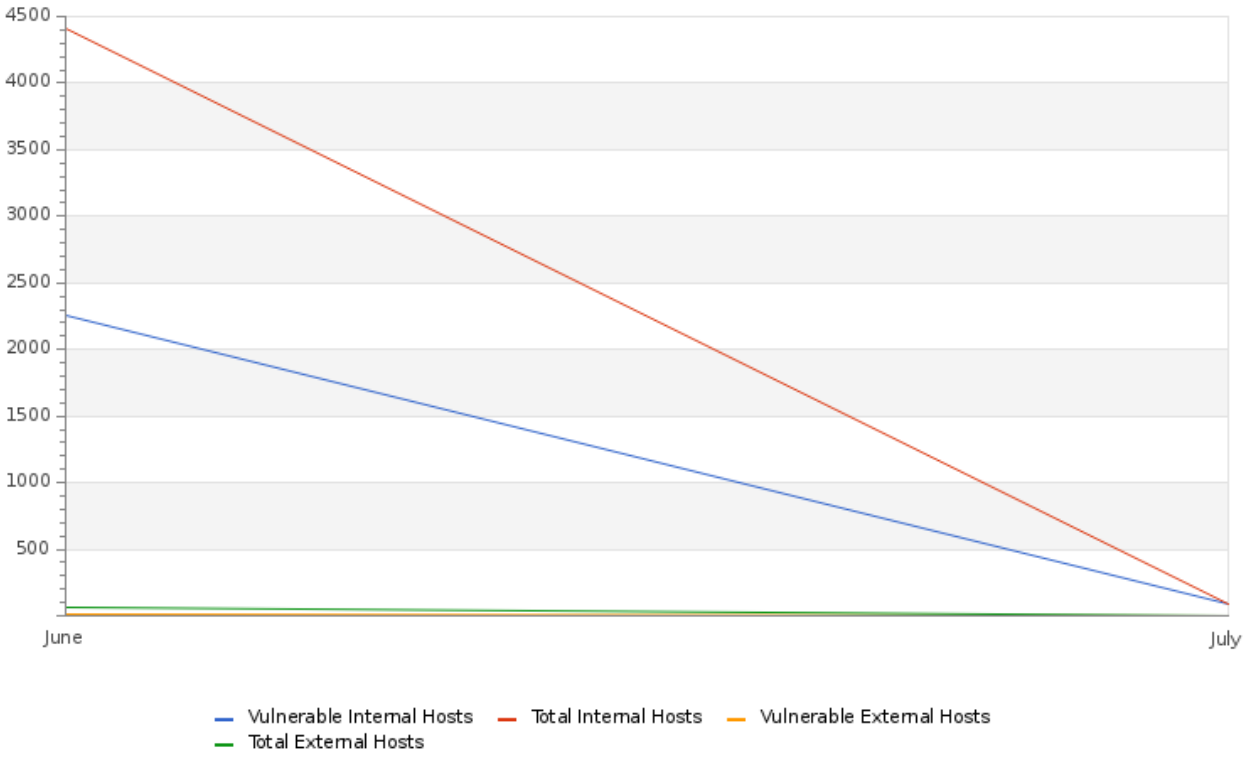


Durante junio no se registraron variaciones en los indicadores de Actual Risk y Accepted Risk
La evaluación continúa sustentándose en la información disponible a través de los servicios de monitoreo y seguridad integrados, por lo que la incorporación de nuevas fuentes de telemetría permitiría aumentar la precisión y el nivel de confianza de futuras evaluaciones.

Hosts & Vulnerable Hosts In Last 6 Months

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

Organo Judicial 09/01/2026



Durante junio de 2026, la gráfica refleja una disminución en la cantidad de hosts internos vulnerables respecto al período anterior. Como complemento a esta tendencia, el análisis mensual registró 7,072 hosts internos evaluados, de los cuales 4,298 presentaron vulnerabilidades activas.

En comparación con mayo, cuando se identificaron 7,051 hosts evaluados y 4,742 vulnerables, junio presentó una reducción de 444 hosts vulnerables, disminuyendo la proporción de sistemas afectados de aproximadamente 67.3 % a 60.8 %. Este comportamiento representa una mejora en el nivel de exposición de la infraestructura interna.

En la superficie externa se identificaron 86 activos publicados en Internet, de los cuales 18 presentaron vulnerabilidades activas, manteniéndose una exposición considerablemente menor frente al entorno interno. Se recomienda continuar el seguimiento de esta evolución y priorizar la remediación de los activos que concentran vulnerabilidades de mayor severidad.

Total Attacks Successfully Blocked

10469

Durante los últimos días de junio se registraron 10,469 ataques bloqueados por los controles de seguridad. Sin embargo, al considerar el análisis completo del mes, el servicio MSS-DDOS registró 3,795,578 eventos asociados a actividad de ataques, lo que representa un incremento aproximado del 110.13 % respecto a mayo. La actividad estuvo concentrada principalmente en las categorías Access y GeoFeed.

Los controles de seguridad implementados permitieron contener la actividad identificada, contribuyendo a reducir el riesgo de afectación sobre los servicios expuestos de la organización.

Organo Judicial 09/01/2026

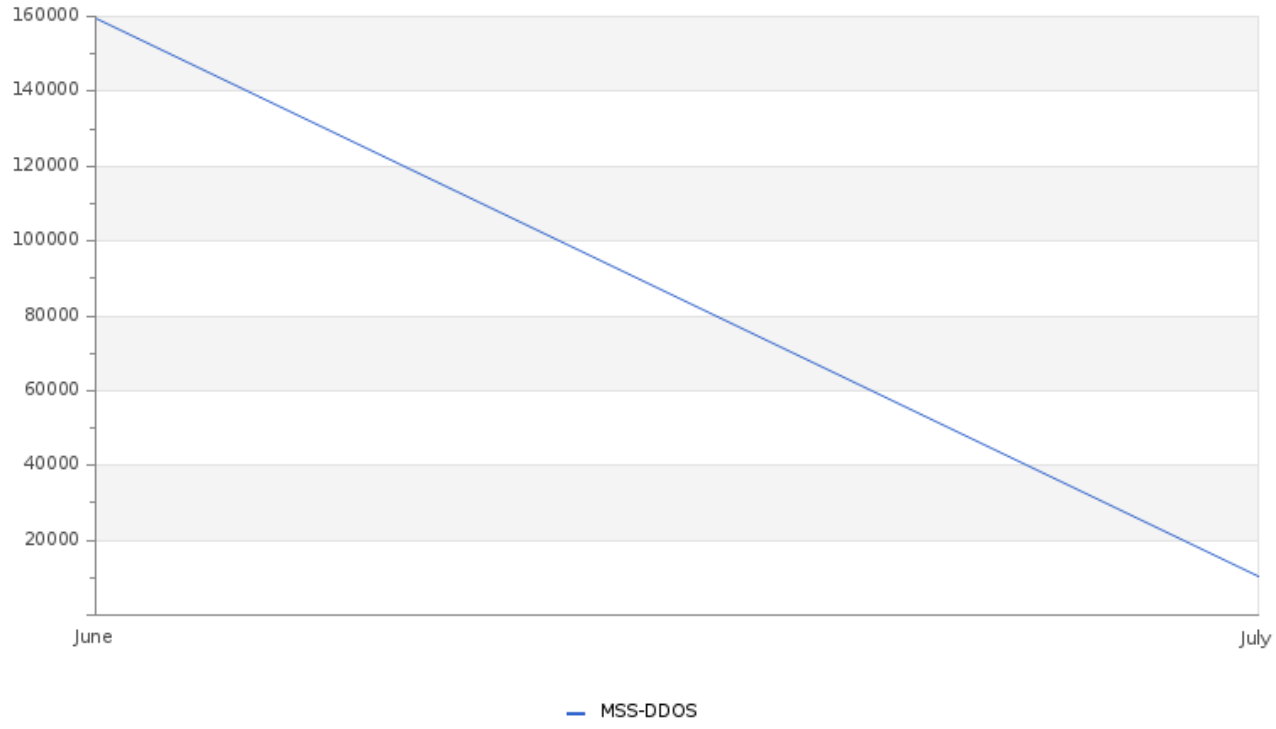
Critical Attacks Successfully Blocked

7149

Durante los últimos días de junio se registraron 7,149 ataques críticos bloqueados. No obstante, al considerar el análisis completo del mes, se identificaron 2,150,903 ataques clasificados como críticos, evidenciando una presencia significativa de actividad de alta severidad durante el período.

Los controles de protección permitieron contener estos eventos, reduciendo el riesgo de afectación sobre la disponibilidad de los servicios. Se recomienda mantener especial seguimiento sobre la evolución de los ataques críticos y sobre los activos que presenten incrementos relevantes en este tipo de actividad.

Attacks Successfully Blocked



Durante el cierre de junio se observó un repunte en la actividad asociada al servicio MSS-DDOS respecto al período anterior, manteniéndose una variación importante en el volumen de ataques dirigidos contra los servicios expuestos.

Sin embargo, al considerar el análisis consolidado del mes de junio, se identificaron 3,795,578 eventos asociados a actividad de ataques, frente a 1,801,502 registrados en mayo, lo que representa un incremento aproximado del 110.13 %. La actividad estuvo concentrada principalmente en Access, con 1,618,644 eventos, y GeoFeed, con 1,573,500 eventos.

Este comportamiento evidencia un incremento significativo de la actividad durante junio y refuerza la importancia de mantener el monitoreo continuo sobre posibles variaciones en los patrones de ataque.

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

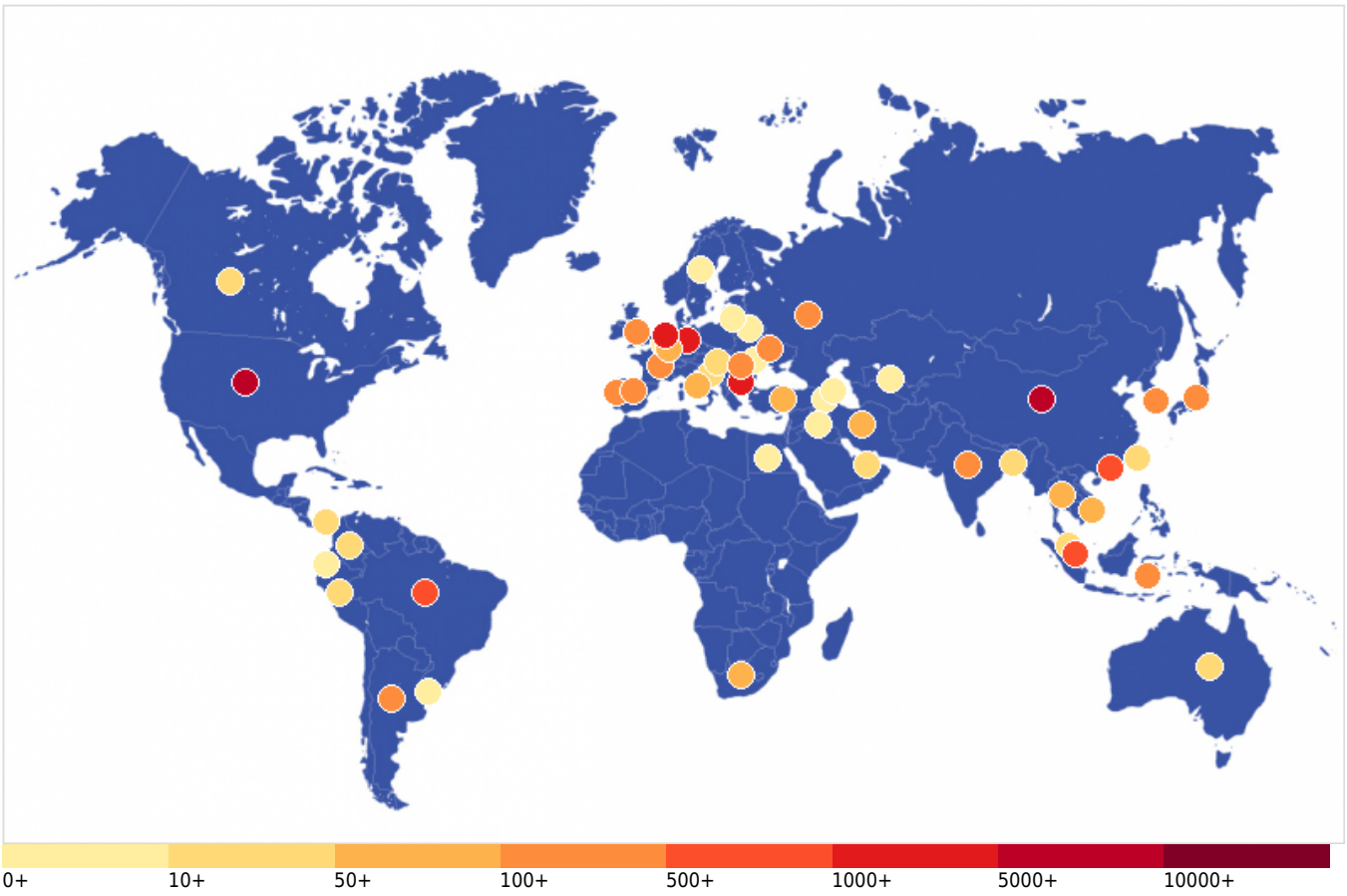
Organo Judicial 09/01/2026

Vulnerability Metric

5

Durante junio, el Vulnerability Metric disminuyó de 8 a 5 respecto al período anterior, reflejando una mejora relevante en el nivel de exposición asociado a las vulnerabilidades identificadas.
Esta reducción es consistente con la disminución observada en la cantidad de hosts vulnerables durante el período y sugiere una evolución favorable en la postura de vulnerabilidades. No obstante, se recomienda mantener la priorización de los hallazgos críticos y altos, especialmente aquellos asociados a activos de mayor relevancia para la operación.

Critical Attacks Per Country In Past Week



Andorra - 111
Argentina - 414
Armenia - 4
Australia - 41
Azerbaijan - 3
Bangladesh - 24
Belarus - 4
Belgium - 2
Bosnia and Herzegovina - 19
Brazil - 582
Bulgaria - 3072
Canada - 22
China - 5746
Colombia - 10
Ecuador - 3
Egypt - 3
France - 288
Germany - 1173
Hong Kong - 517
Hungary - 10
India - 481
Indonesia - 159
Iran - 64
Iraq - 2
Italy - 65
Japan - 229
Lithuania - 2
Luxembourg - 97
Malaysia - 39
Mauritius - 2
Moldova - 4
Netherlands - 1342
New Zealand - 34
Panama - 12
Peru - 22
Portugal - 161
Romania - 147
Russia - 225
Saint Kitts and Nevis - 57
Seychelles - 15
Singapore - 669
South Africa - 52
South Korea - 339
Spain - 390

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

Organo Judicial 09/01/2026

Sweden - 4	Taiwan - 34	Thailand - 55	Turkey - 83
Ukraine - 127	United Arab Emirates - 11	United Kingdom - 243	United States - 6024
Uruguay - 2	Uzbekistan - 9	Vietnam - 95	

Durante el período analizado se observa una distribución geográfica amplia de ataques críticos, con actividad proveniente de múltiples regiones, principalmente de Norteamérica, Europa y Asia. Este comportamiento evidencia que la exposición de los servicios publicados no se encuentra asociada a una única ubicación o fuente específica, sino a un entorno de amenazas distribuido globalmente.
La presencia simultánea de actividad desde diferentes países es consistente con comportamientos automatizados de reconocimiento, escaneo y explotación de servicios expuestos, por lo que el origen geográfico debe considerarse como un indicador complementario y no como el único criterio para determinar el nivel de riesgo.

TLP:AMBER

BOARDROOM 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