TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

August 18, 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

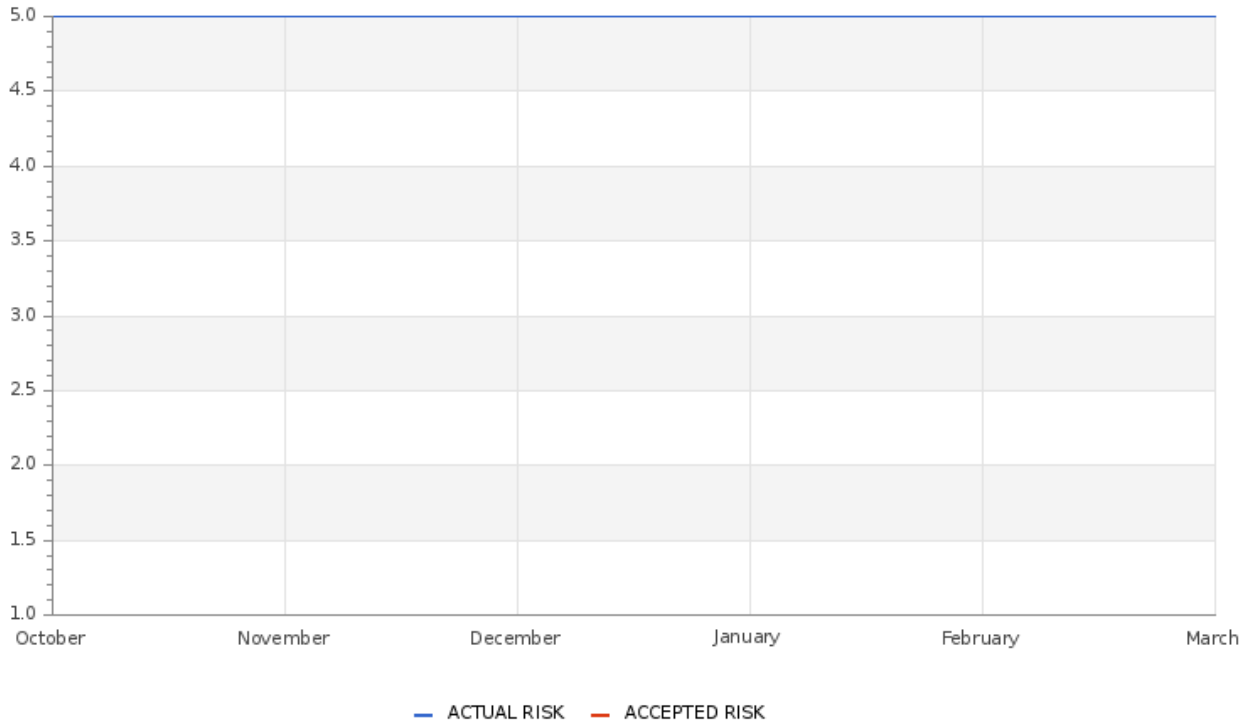
Low

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 08/18/2026

Accepted & Actual Risk

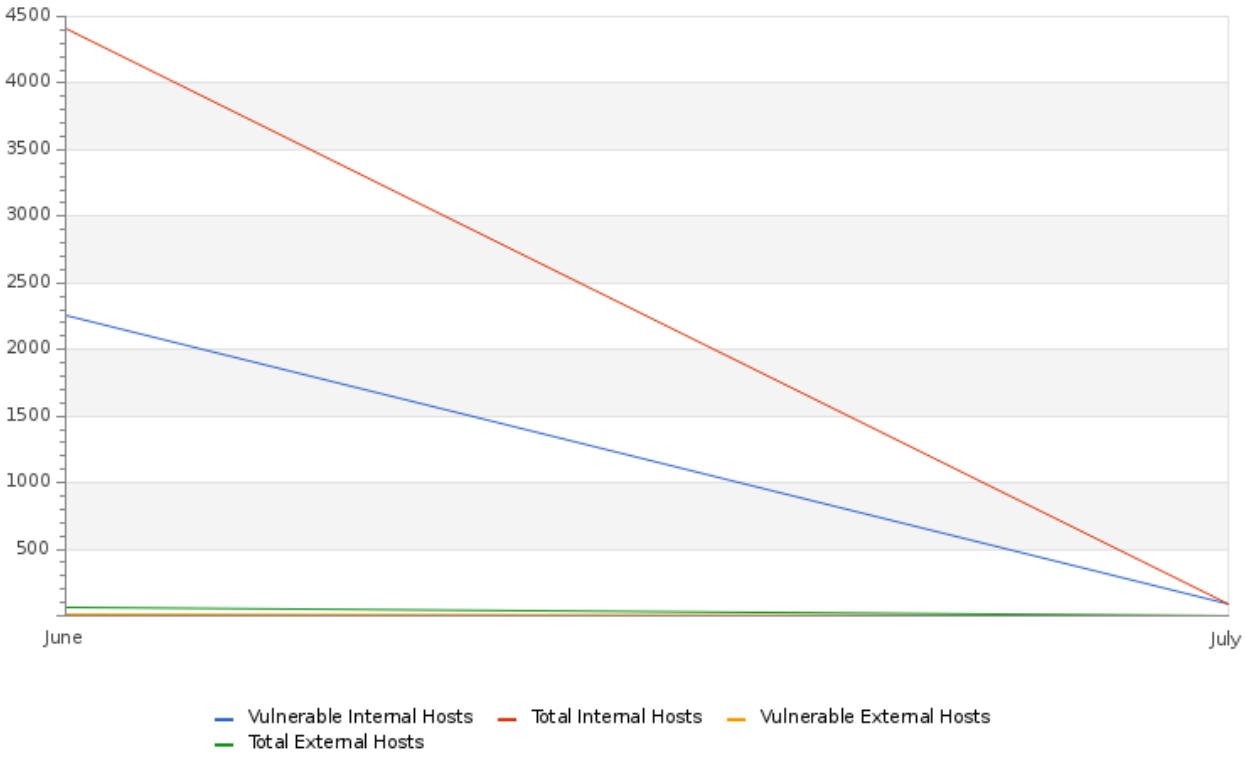


Durante junio no se registraron variaciones en los indicadores de Actual Risk y Accepted Risk
La evaluación continúa sustentándose en la información disponible a través de los servicios de monitoreo y seguridad integrados, por lo que la incorporación de nuevas fuentes de telemetría permitiría aumentar 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 08/18/2026



Entre marzo y junio de 2026, la evolución de los activos internos muestra una reducción progresiva de la exposición después del nivel más alto registrado en marzo. En junio se evaluaron 6,990 hosts internos, de los cuales 4,280 presentaron vulnerabilidades.
Frente a mayo, cuando se identificaron 4,715 hosts vulnerables, junio registró una disminución de 435 activos vulnerables, a pesar de que la cantidad total de sistemas evaluados aumentó ligeramente. Este comportamiento representa una mejora en la proporción de activos internos vulnerables durante el período.
La superficie externa continúa representando una proporción considerablemente menor frente al entorno interno, por lo que la principal concentración de exposición permanece dentro de la infraestructura interna. Se recomienda mantener el seguimiento de esta tendencia y priorizar los activos que concentran vulnerabilidades de mayor severidad.

Total Attacks Successfully Blocked

10469

Durante junio, los controles de seguridad mantuvieron una capacidad activa de detección y contención frente a la actividad maliciosa observada, contribuyendo a reducir la posibilidad de afectaciones sobre los servicios y activos de la organización.

El comportamiento registrado confirma que continúan presentándose intentos dirigidos contra distintos componentes de la infraestructura, por lo que resulta importante mantener el monitoreo continuo y la revisión periódica de los controles implementados para responder oportunamente ante variaciones en el panorama de amenazas.

Organo Judicial 08/18/2026

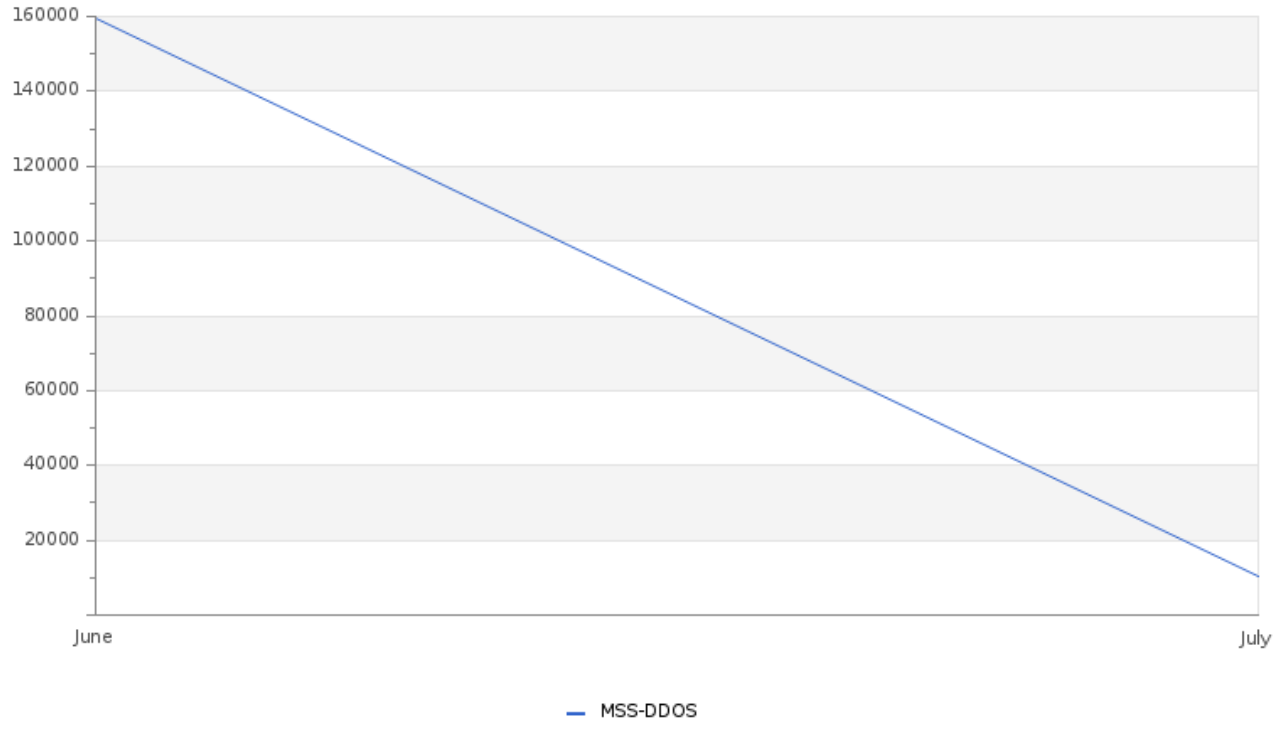
Critical Attacks Successfully Blocked

7149

Durante el período también se identificó una presencia relevante de actividad clasificada como crítica, lo que evidencia que parte de los intentos detectados presentó un nivel de severidad elevado y requirió la intervención de los mecanismos de protección.

La contención de este tipo de eventos contribuye a disminuir el riesgo sobre activos y servicios de mayor relevancia. Por ello, se recomienda mantener especial seguimiento sobre los patrones asociados a ataques críticos, particularmente cuando se observen cambios en los activos objetivo, las fuentes de origen o los tipos de actividad detectada.

Attacks Successfully Blocked



Durante junio se observó un repunte en la actividad DDoS respecto a mayo, luego de la disminución registrada en el período anterior. Aun así, el nivel de actividad permaneció por debajo de los valores observados durante marzo y abril, evidenciando un comportamiento fluctuante en los intentos dirigidos contra los servicios expuestos.
Los mecanismos de protección continuaron detectando y mitigando esta actividad, contribuyendo a reducir el riesgo de afectaciones sobre la disponibilidad de los servicios institucionales. La variación observada confirma la necesidad de mantener capacidades especializadas de monitoreo y mitigación, especialmente ante incrementos repentinos que puedan representar cambios en la presión ejercida sobre la infraestructura pública.
En términos generales, el comportamiento de junio refleja que la amenaza DDoS continúa activa y requiere seguimiento constante, aun cuando la intensidad varíe entre períodos.

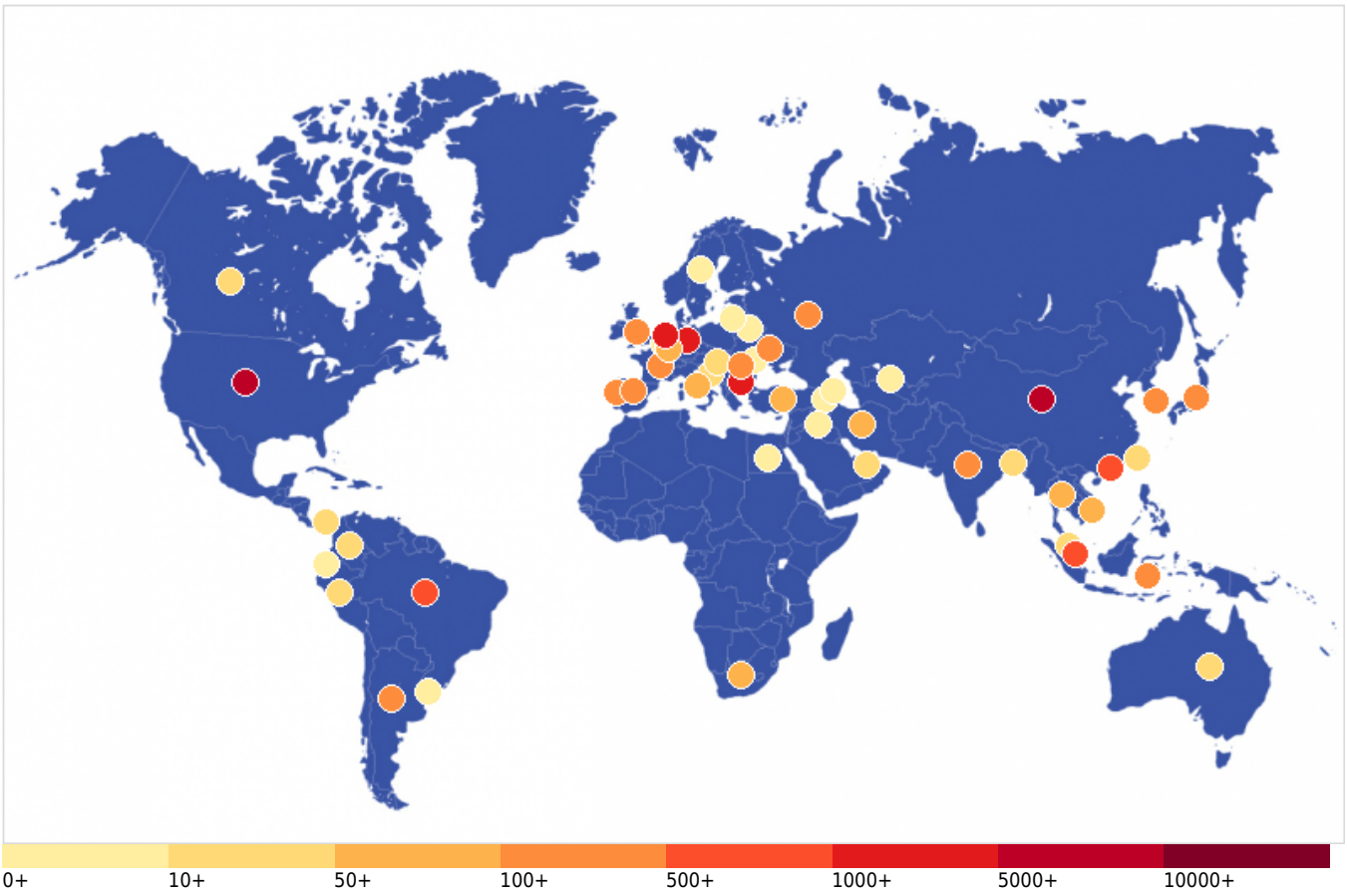
Organo Judicial 08/18/2026

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

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 = 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

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