TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

September 01, 2026

Organo Judicial 09/01/2026

TLP AMBER BOARDROOM

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.

Actual Risk

n/a

Durante julio no se contó con un nivel cuantificable de riesgo actual en el indicador. No obstante, el análisis del período mantuvo bajo seguimiento vulnerabilidades críticas y altas, actividad asociada al servicio MSS-DDOS y alertas identificadas mediante MSS-EDR

Accepted Risk

n/a

El riesgo aceptado se mantuvo sin un valor cuantificable durante julio. El análisis continúa enfocado en los riesgos identificados y en las condiciones observadas mediante los diferentes servicios de monitoreo, manteniendo el seguimiento sobre los activos y tecnologías con mayor nivel de exposición.

Confidence

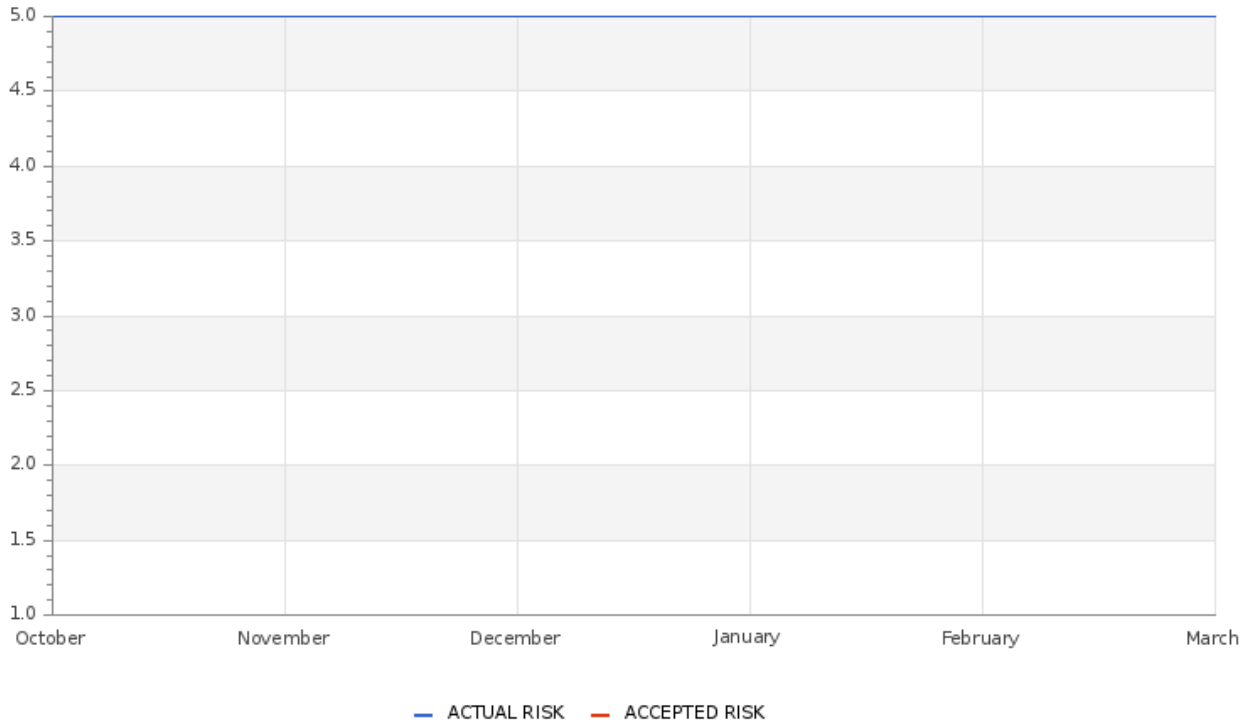
Low

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

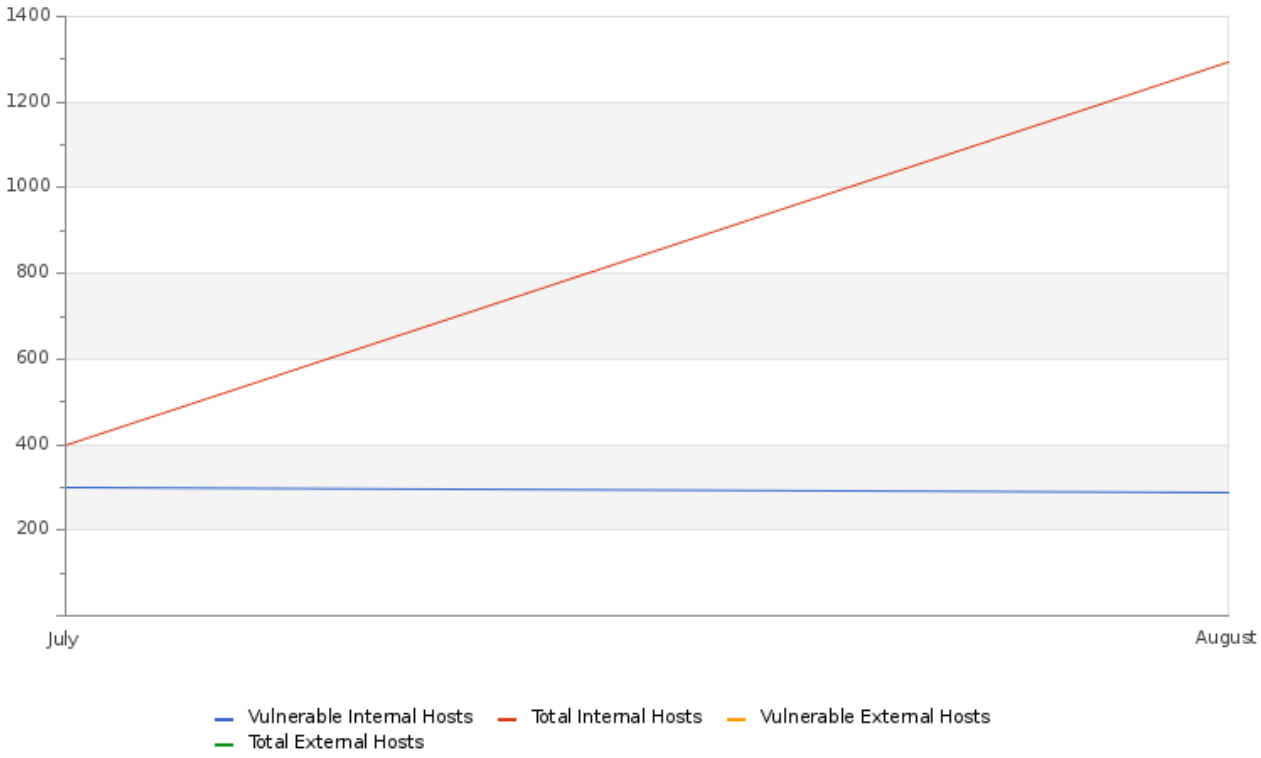


Durante julio no se registraron variaciones en los indicadores de Actual Risk y Accepted Risk. La evaluación continúa sustentándose en la información disponible a través de los servicios de monitoreo y seguridad integrados, por lo que la incorporación de nuevas fuentes de telemetría permitiría aumentar 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 julio de 2026, el análisis de vulnerabilidades internas identificó 6,777 hosts evaluados, de los cuales 4,862 presentaron vulnerabilidades activas, reflejando una presencia relevante de sistemas con hallazgos dentro de la infraestructura.

La distribución de vulnerabilidades estuvo compuesta por 580 críticas, 4,295 altas, 2,479 medias y 5,171 bajas. Entre los hallazgos de mayor relevancia se mantuvieron vulnerabilidades asociadas a plataformas Cisco y ArubaOS, así como condiciones relacionadas con IPMI, SNMP y NTP. Adicionalmente, se observó una presencia significativa de ICMP Timestamp, identificada en 4,765 hosts, mientras que la condición SNMP GETBULK Reflection DDoS afectó aproximadamente 500 sistemas.

Este panorama evidencia que una parte importante de la exposición continúa asociada tanto a vulnerabilidades de mayor severidad como a configuraciones y servicios presentes de forma extendida en la infraestructura. Se recomienda mantener la priorización de los hallazgos críticos y altos, junto con el seguimiento de aquellas condiciones que afectan a un mayor número de activos.

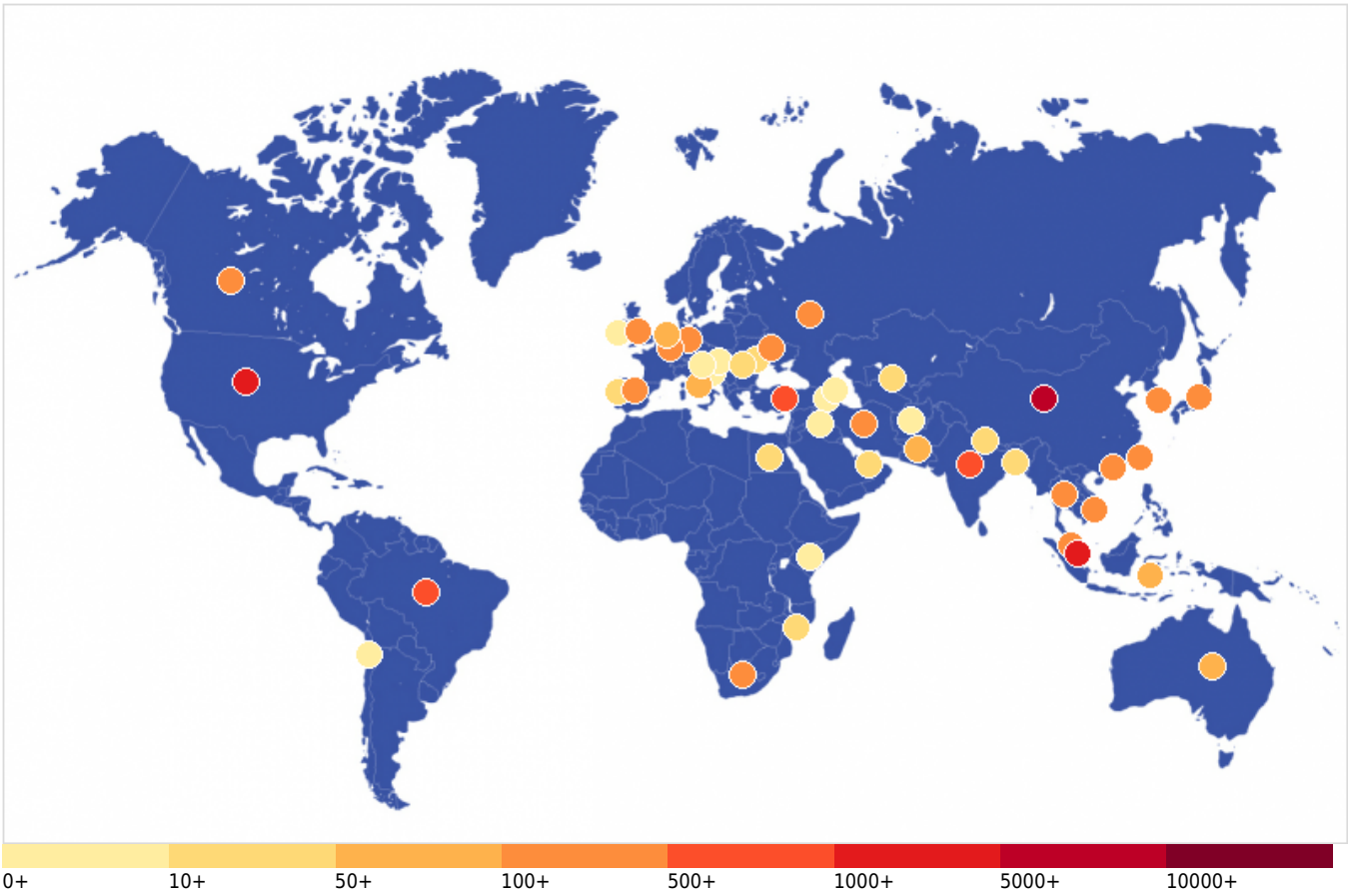
Vulnerability Metric

5

Durante julio, el Vulnerability Metric se mantuvo en un rango entre 3 y 5, reflejando variaciones en el nivel de exposición observado durante el período. El análisis mensual identificó 4,862 hosts con vulnerabilidades activas, incluyendo 580 vulnerabilidades críticas y 4,295 altas, por lo que se mantiene la necesidad de priorizar la remediación de los hallazgos de mayor severidad y aquellos asociados a activos relevantes para la operación.

Organo Judicial 09/01/2026

Critical Attacks Per Country In Past Week



Afghanistan - 8
Armenia - 6
Australia - 83
Azerbaijan - 8
Bahrain - 5
Bangladesh - 41
Bosnia and Herzegovina - 1
Brazil - 924
Canada - 395
Chile - 7
China - 5536
Egypt - 39
Germany - 421
Hong Kong - 308
Hungary - 9
India - 653
Indonesia - 80
Iran - 186
Iraq - 2
Ireland - 2
Italy - 77
Japan - 143
Kenya - 5
Luxembourg - 114
Malaysia - 130
Mauritius - 13
Moldova - 12
Mozambique - 17
Nepal - 15
Netherlands - 59
Pakistan - 74
Portugal - 46
Romania - 46
Russia - 391
Seychelles - 18
Singapore - 1093
Slovenia - 3
South Africa - 130
South Korea - 460
Spain - 379
Taiwan - 133
Thailand - 101
Turkey - 826
Ukraine - 252
United Arab Emirates - 16
United Kingdom - 228
United States - 3518
Uzbekistan - 35
Vietnam - 129

Durante el período analizado se observa una distribución geográfica amplia de ataques críticos, con actividad proveniente de múltiples regiones. Entre los principales orígenes identificados destacan China, Estados Unidos, Singapur, Turquía e India, concentrando los mayores volúmenes dentro de la gráfica.

Este comportamiento confirma que la actividad maliciosa dirigida contra los servicios expuestos mantiene un carácter distribuido globalmente y no se encuentra asociada a una única ubicación. La presencia simultánea de eventos desde distintos países es consistente con actividades automatizadas de reconocimiento, escaneo e intentos de explotación, por lo que el origen geográfico debe mantenerse como un indicador complementario dentro del análisis de riesgo.

Organo Judicial 09/01/2026

Durante julio, el servicio MSS-DDOS registró además 4,702,684 eventos asociados a actividad de ataques, manteniéndose una presión significativa sobre la infraestructura expuesta. Se recomienda continuar con el monitoreo de los principales países de origen y prestar especial atención a incrementos relevantes o cambios sostenidos en los patrones de actividad.

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