TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

July 28, 2026

Organo Judicial 07/28/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "Marzo 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

5%

El nivel de riesgo actual se sigue manteniendo en el mismo rango ya establecido. Esta tendencia refleja una menor actividad de amenazas sobre los activos supervisados, lo que evidencia la efectividad de las medidas de control aplicadas. Sin embargo, es fundamental continuar con un monitoreo constante para garantizar la permanencia de este nivel y anticipar posibles incrementos futuros.

Accepted Risk

1%

El riesgo aceptado permanece en valores bajos que demuestran una gestión adecuada del riesgo residual. Este resultado confirma que la organización mantiene un enfoque prudente en la aceptación del riesgo, dando prioridad a las acciones de mitigación y control frente a eventuales escenarios de exposición.

Confidence

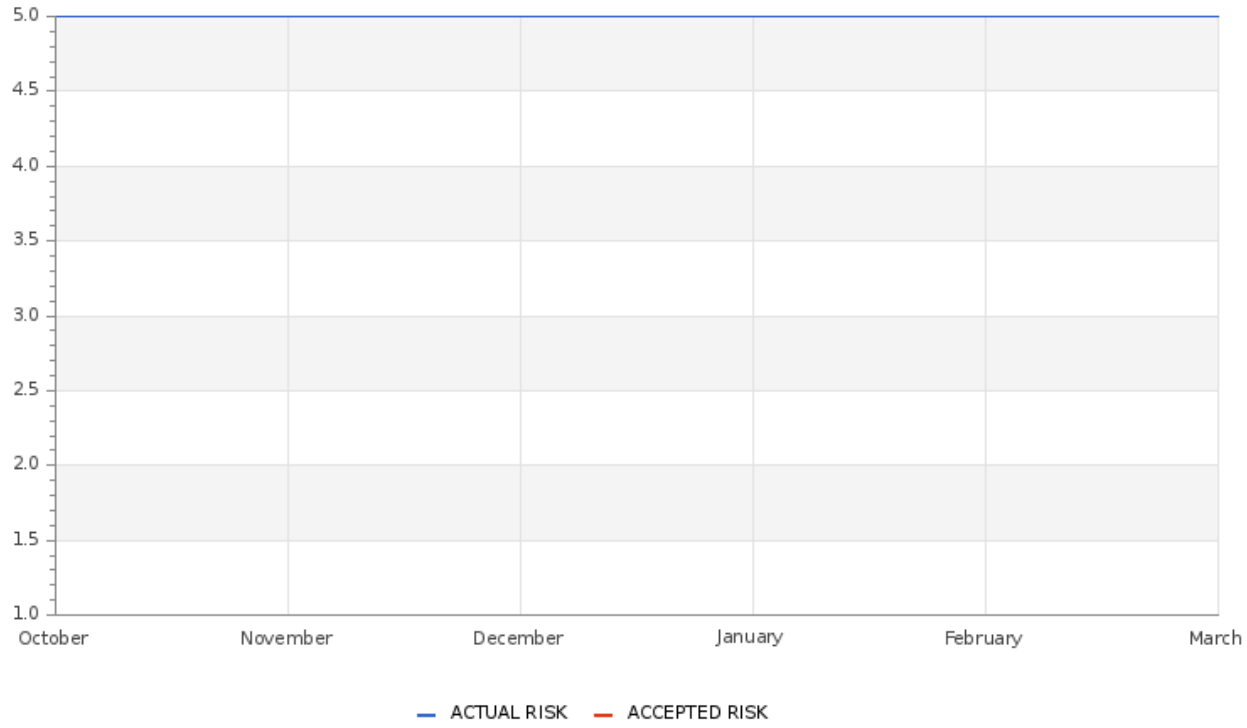
Low

La confiabilidad de la evaluación sigue siendo limitada debido a la insuficiencia y falta de consistencia de los datos disponibles. Se sugiere reforzar los procesos de recopilación y correlación de información para incrementar la precisión del análisis y proporcionar un soporte más sólido a la toma de decisiones en materia de seguridad.

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

Organo Judicial 07/28/2026

Accepted & Actual Risk



Riesgo Actual (5%) Durante el periodo analizado, el nivel de riesgo actual se mantuvo estable en comparación con el mes anterior. El valor del 5% se encuentra dentro de un rango bajo, indicando que la exposición a incidentes potenciales sigue controlada y que las medidas de seguridad implementadas continúan siendo efectivas. No obstante, es esencial mantener una vigilancia constante y una capacidad de respuesta adecuada para prevenir posibles incrementos futuros.

Riesgo Tolerado (1%) El riesgo tolerado se mantuvo en 1%, reflejando una gestión conservadora y consistente del riesgo residual. Este comportamiento demuestra la correcta aplicación de controles preventivos y la priorización de acciones de mitigación frente a posibles exposiciones, manteniendo el nivel de riesgo dentro de parámetros aceptables.

Hosts & Vulnerable Hosts In Last 6 Months

Durante el mes de marzo se evaluaron 4,223 activos internos y 61 activos expuestos a Internet. Del total de activos internos, 2,032 (48.1 %) presentaron al menos una vulnerabilidad, lo que refleja una superficie de exposición significativa dentro de la red corporativa y resalta la importancia de fortalecer las actividades de gestión de vulnerabilidades y aplicación de parches. En el caso de los activos externos, 11 de los 61 evaluados (18.0 %) presentaron vulnerabilidades. Aunque la proporción es considerablemente menor que la observada en el entorno interno, estos activos representan un mayor nivel de riesgo debido a su exposición directa a Internet, por lo que su remediación debe mantenerse como una prioridad.

Organo Judicial 07/28/2026

Total Attacks Successfully Blocked

181349

Durante el mes de marzo se registró un total de 5,765,907 ataques dirigidos a la infraestructura protegida. En los últimos 30 días se han contabilizado 181,349 ataques, principalmente dirigidos a las direcciones IP públicas del rango 200.46.13.x, siendo la IP 200.46.13.17 la que concentró el mayor volumen de eventos. Se observa un predominio de ataques clasificados como críticos, bloqueados principalmente mediante las firmas del ERT Feed , lo que evidencia una actividad constante dirigida contra los servicios publicados y la efectividad de los mecanismos de protección implementados.

Critical Attacks Successfully Blocked

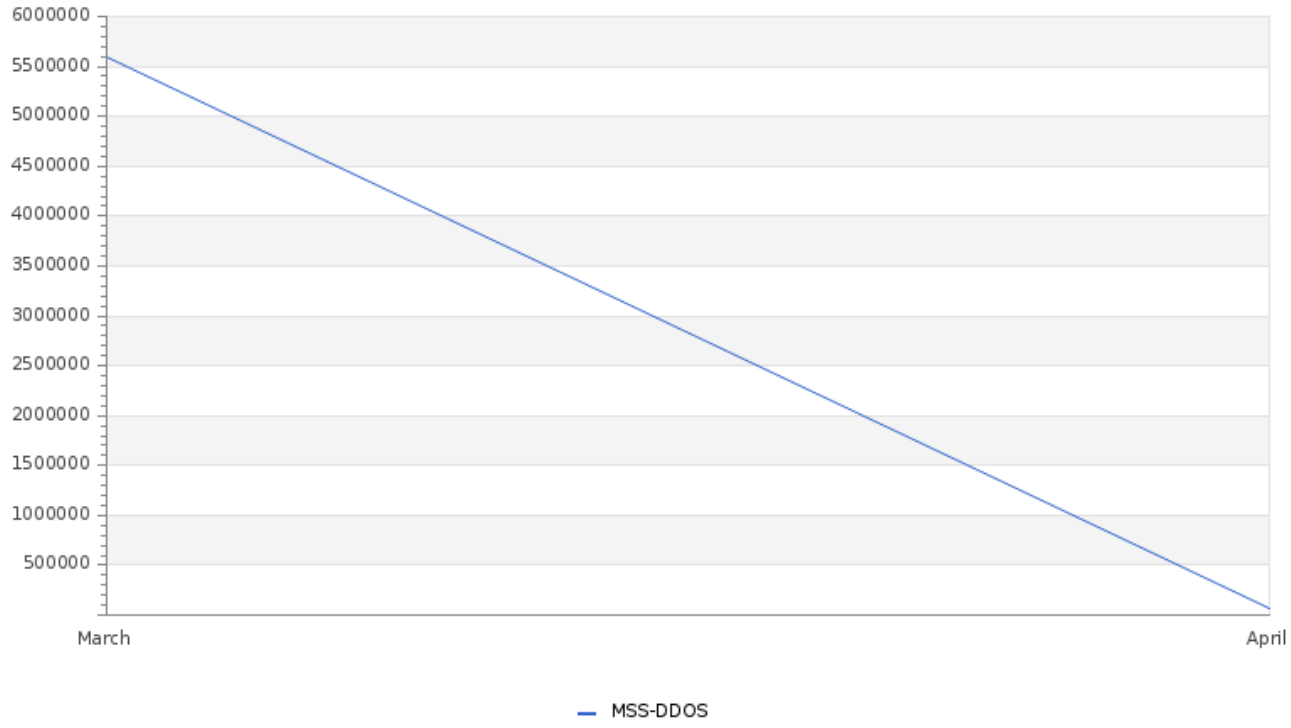
127080

A nivel de ataques críticos, durante el mes de marzo se registró un total de 3,780,043 eventos, mientras que en los últimos 30 días se han contabilizado 127,080. La mayor parte de estos eventos corresponde a firmas del ERT Feed , seguido por ataques relacionados con Access, ERT Active Attacker: WEB e Invalid TCP Flags, lo que evidencia un flujo constante de intentos de explotación dirigidos contra los servicios expuestos y la efectividad de los controles de protección implementados para su bloqueo.

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

Organo Judicial 07/28/2026

Attacks Successfully Blocked



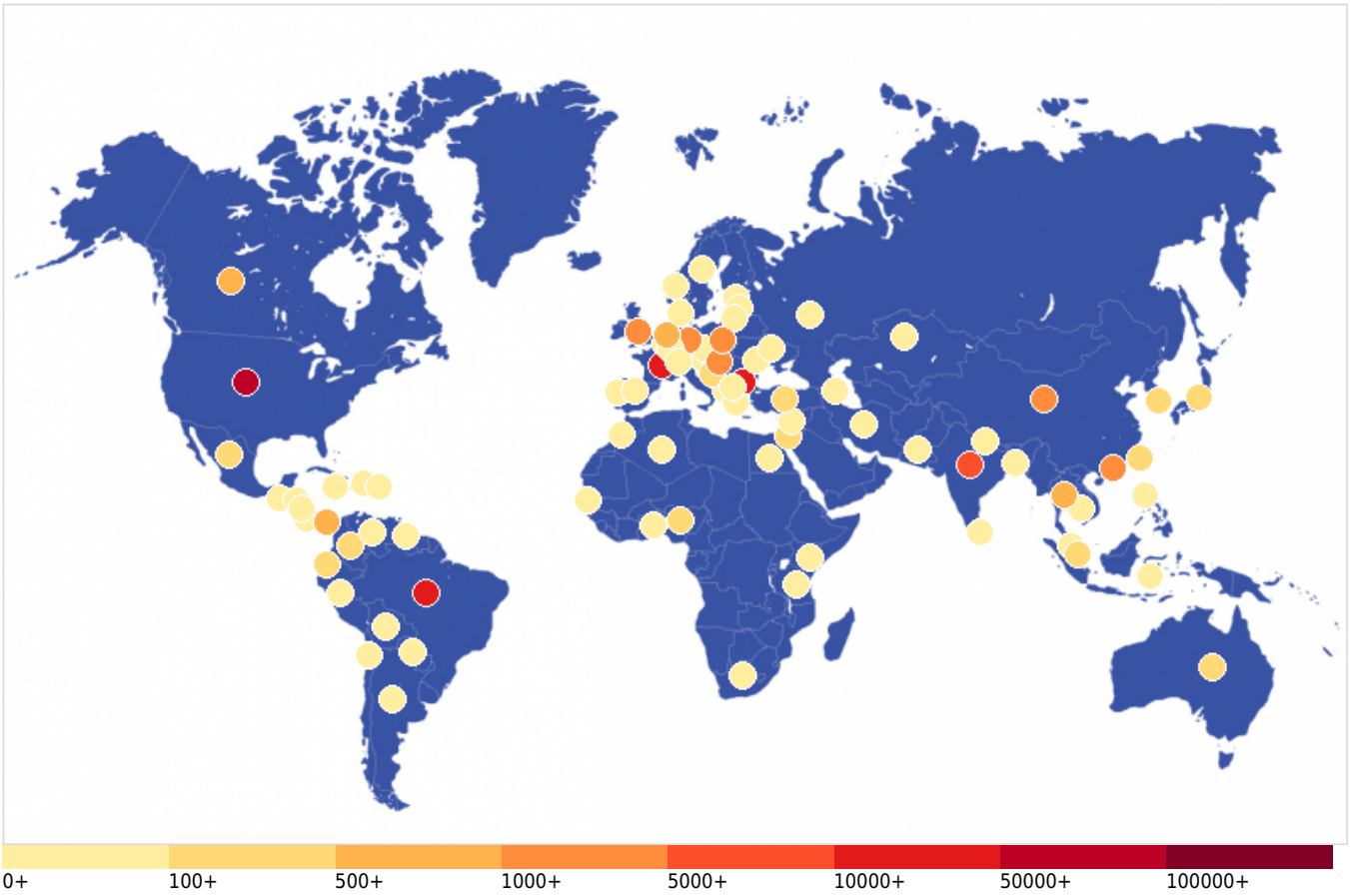
Durante el mes de marzo se registraron 5,765,907 ataques dirigidos a la infraestructura protegida, de los cuales 3,780,043 (65.6 %) fueron clasificados como ataques críticos. Este comportamiento evidencia que una proporción significativa de la actividad maliciosa correspondió a intentos de alto riesgo, los cuales fueron mitigados por los mecanismos de protección implementados, principalmente mediante las firmas del ERT Feed de Radware.

Vulnerability Metric

12

Critical Attacks Per Country In Past Week

Organo Judicial 07/28/2026



Albania - 59
Algeria - 21
Argentina - 99
Australia - 306
Austria - 3
Azerbaijan - 3
Bangladesh - 42
Belgium - 3
Bolivia - 53
Bosnia and Herzegovina - 305
Botswana - 9
Brazil - 23882
Bulgaria - 10441
Cambodia - 6
Canada - 520
Chile - 45
China - 2283
Colombia - 209
Costa Rica - 12
Czechia - 3
Denmark - 3
Dominican Republic - 6
Ecuador - 111
Egypt - 6
Estonia - 3
France - 26089
Germany - 1080
Greece - 3
Guatemala - 12
Guyana - 3
Honduras - 15
Hong Kong - 2100
Hungary - 1113
India - 9769
Indonesia - 69
Israel - 210
Jamaica - 12
Japan - 437
Jordan - 3
Kazakhstan - 34
Kenya - 9
Latvia - 12
Lebanon - 15
Lithuania - 6
Luxembourg - 87
Malaysia - 6
Mauritius - 9
Mexico - 462
Moldova - 3
Morocco - 6
Nepal - 3
Netherlands - 808
New Zealand - 3
Nicaragua - 9
Nigeria - 258
North Macedonia - 3
Norway - 66
Pakistan - 81
Panama - 720
Paraguay - 15
Peru - 12
Philippines - 12
Poland - 1374
Portugal - 3
Puerto Rico - 6
Russia - 61
Saint Kitts and Nevis - 3
Senegal - 9
Seychelles - 3
Singapore - 101
South Africa - 12
South Korea - 196
Spain - 16
Sri Lanka - 25
Sweden - 32
Switzerland - 21
Taiwan - 116
Tanzania - 15
Thailand - 606
Togo - 3
Turkey - 411
Ukraine - 24
United Kingdom - 3383
United States - 66821
Venezuela - 66

El análisis del origen geográfico de los ataques evidencia que la mayor parte de la actividad maliciosa provino de

direcciones IP ubicadas en Estados Unidos (66,821 eventos), seguido por Brasil (23,882), India (9,769), Alemania (6,089) y Reino Unido (3,383). Asimismo, se identificó actividad desde otros países como Hong Kong, China, Panamá y México. Es importante destacar que el país de origen de una dirección IP no necesariamente representa la ubicación real del atacante, ya que es común el uso de infraestructura comprometida, servicios en la nube, VPN y redes de anonimización para ocultar el origen de los ataques.

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