TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

June 13, 2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "Abril 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

El nivel de riesgo actual se mantiene constante con el mes anterior, situándose dentro de un rango bajo. Esto refleja la continuidad en el control de la actividad de amenazas sobre los activos monitoreados y sugiere que las medidas de seguridad implementadas continúan siendo efectivas. Sin embargo, resulta esencial mantener una supervisión constante para preservar este nivel y anticipar posibles cambios en el entorno.

Accepted Risk

n/a

El cliente no ha definido formalmente su nivel de Tolerancia al Riesgo durante la configuración del servicio. Por lo tanto, el análisis se realiza en función del Riesgo Real identificado y las mejores prácticas de ciberseguridad.

Confidence

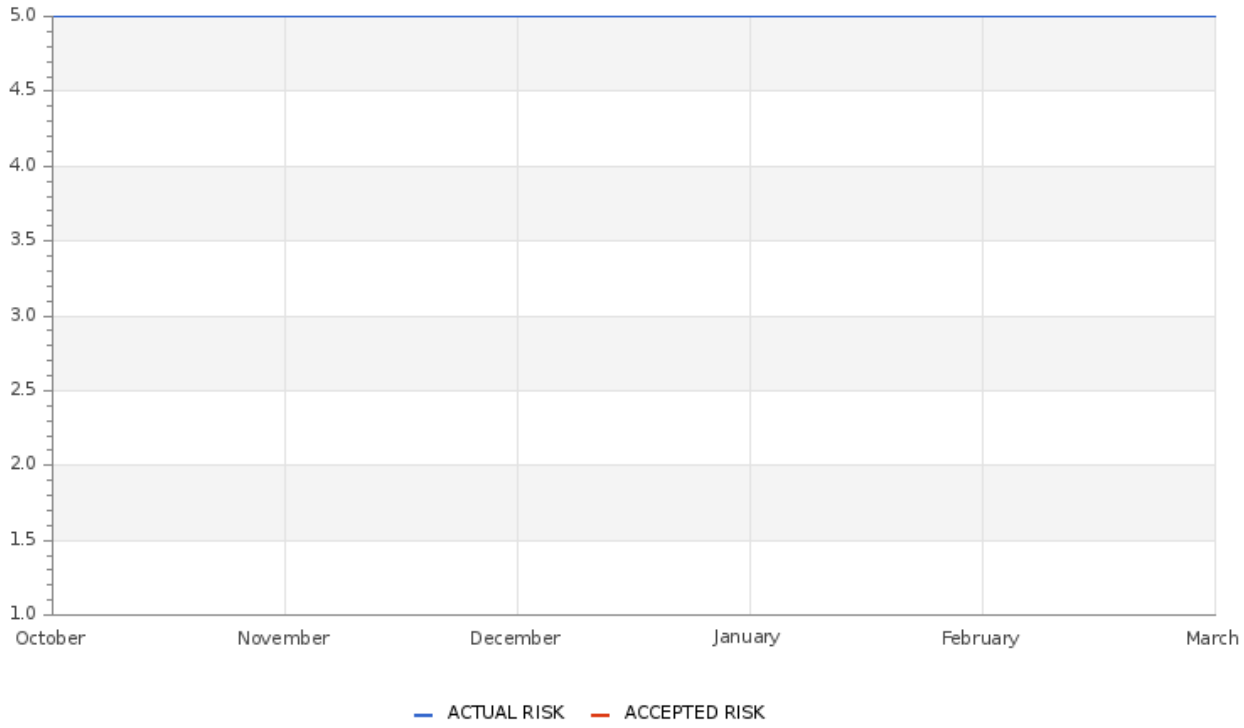
Low

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 06/13/2026

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

Total Attacks Successfully Blocked

6448

Durante el período evaluado se bloquearon exitosamente 6,448 intentos de ataque, lo que representa una disminución significativo respecto al mes anterior. Este aumento evidencia una mayor actividad maliciosa en el período analizado; sin embargo, los controles de seguridad mantuvieron su eficacia, operando de manera consistente y garantizando un nivel adecuado de protección frente a las amenazas detectadas.

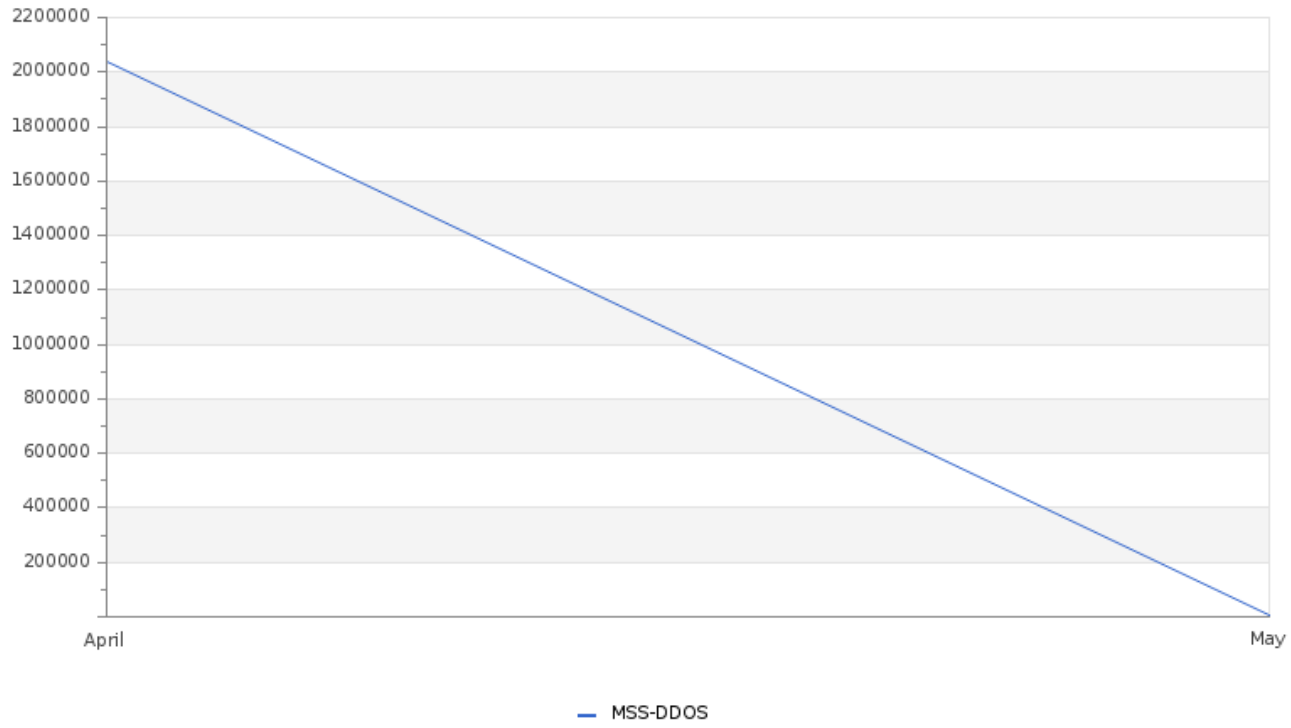
Organo Judicial 06/13/2026

Critical Attacks Successfully Blocked

4906

Durante el período evaluado se identificaron 4,906 eventos clasificados como ataques críticos. A pesar de este volumen, no se registraron afectaciones en la disponibilidad, integridad ni continuidad operativa de la infraestructura ni del servicio. Este resultado demuestra la eficacia de los controles de seguridad implementados, incluyendo mecanismos de detección, prevención y respuesta, así como la capacidad de la arquitectura para absorber y mitigar amenazas de alta criticidad sin generar interrupciones en la operación.

Attacks Successfully Blocked



Durante el mes de abril se registró un total aproximado de 2,000,000 ataques bloqueados, evidenciando una disminución significativa en comparación con el mes anterior.. Esta reducción refleja un comportamiento más estable del entorno y una menor actividad maliciosa durante el período evaluado. En cuanto a la severidad, no se registraron ataques críticos, manteniéndose este indicador en valores nulos. La totalidad de los eventos bloqueados correspondió a ataques de baja severidad, lo que demuestra la eficacia continua de los controles de seguridad para la detección oportuna y la mitigación temprana de amenazas

---

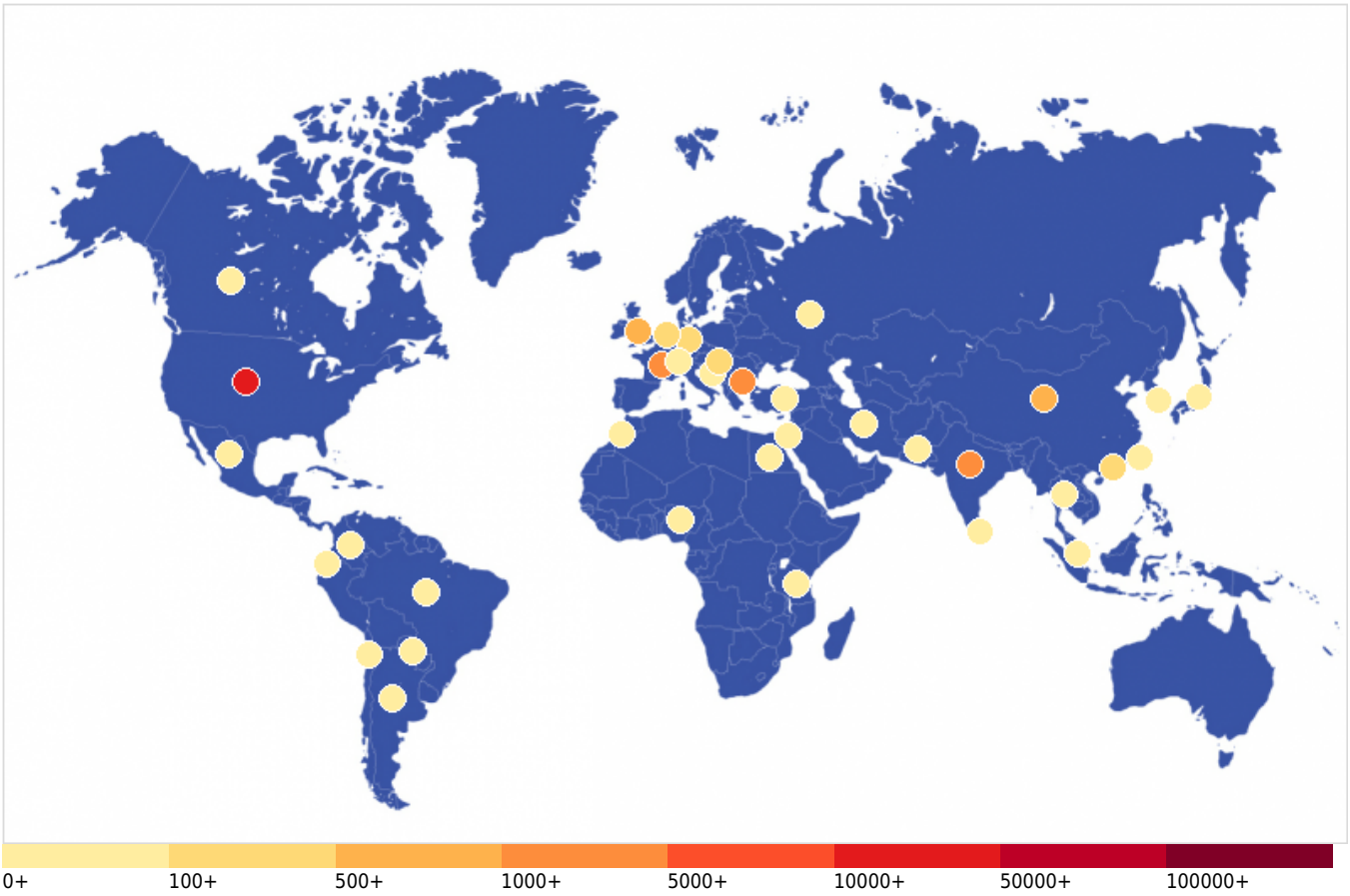
Vulnerability Metric

3

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

Organo Judicial 06/13/2026

Critical Attacks Per Country In Past Week



Argentina - 12
Bosnia and Herzegovina - 19
Brazil - 70
Bulgaria - 1191
Canada - 33
Chile - 2
China - 521
Colombia - 6
Ecuador - 4
Egypt - 2
France - 3155
Germany - 263
Hong Kong - 188
Hungary - 349
India - 1038
Israel - 13
Japan - 45
Jordan - 4
Mexico - 10
Morocco - 1
Netherlands - 202
Nigeria - 12
Pakistan - 4
Paraguay - 1
Russia - 22
Singapore - 5
South Korea - 5
Sri Lanka - 3
Switzerland - 2
Taiwan - 8
Tanzania - 2
Thailand - 2
Turkey - 44
United Kingdom - 510
United States - 10646

La gráfica correspondiente al período analizado muestra una distribución global de ataques críticos, con una mayor concentración de eventos provenientes de América del Norte, Europa y Asia. Estados Unidos se mantiene como la principal fuente de actividad, con 10,646 eventos registrados, seguido por Francia (3,155), Bulgaria (1,191), India (1,038) y China (521). En un segundo nivel se ubican Reino Unido (510), Hungría (349), Alemania (263), Países Bajos (202) y Hong Kong (188), los cuales también representan una proporción relevante de la actividad observada. Adicionalmente, se identificaron eventos provenientes de otras regiones, incluyendo Turquía, Japón, Canadá, Rusia y Bosnia y Herzegovina, evidenciando una amplia distribución geográfica en el origen de los ataques. La distribución observada refleja el carácter global de las amenazas que afectan a los servicios expuestos a Internet y pone de manifiesto la utilización de infraestructuras tecnológicas distribuidas para la ejecución de actividades maliciosas. Este comportamiento resalta la importancia de mantener capacidades de monitoreo continuo, inteligencia de amenazas y controles de seguridad que permitan identificar oportunamente cambios en los patrones de ataque y fortalecer la protección de los activos institucionales

Organo Judicial 06/13/2026

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.**

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