TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

July 29, 2026

Organo Judicial 07/29/2026

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

No se identificaron amenazas activas asociadas a los activos vulnerables durante el período evaluado. Aunque se detectaron vulnerabilidades en los entornos interno y externo, los controles de seguridad implementados continúan mitigando la actividad maliciosa observada, manteniendo el Riesgo Real dentro de un nivel bajo.

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 se mantiene baja debido a que la visibilidad del entorno aún es parcial y no se cuenta con la integración completa de todas las fuentes de información necesarias para obtener una evaluación integral del riesgo.

Accepted & Actual Risk

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

Organo Judicial 07/29/2026

Durante abril de 2026, la infraestructura protegida registró 1,996,818 ataques bloqueados, lo que representa una disminución del 65.4 % respecto a marzo (5,765,907 ataques). Durante los últimos 30 días se contabilizaron 6,448 eventos.

El análisis del tráfico evidencia que los intentos de ataque continuaron concentrándose sobre los servicios web expuestos, principalmente mediante el puerto HTTPS (443). La mayor proporción de los eventos estuvo asociada a mecanismos de inteligencia de amenazas (ERTFeed) y controles de reputación, lo que confirma que los sistemas de protección continúan bloqueando tráfico identificado previamente como malicioso antes de que alcance los activos críticos.

Asimismo, se observó que las direcciones IP públicas con mayor exposición continuaron siendo el principal objetivo de los atacantes, manteniéndose una distribución geográfica similar a meses anteriores, con predominio de eventos provenientes de Estados Unidos.

Es importante destacar que la disminución observada en el volumen de ataques no representa necesariamente una reducción del nivel de amenaza. Durante este período únicamente se recibió telemetría de un equipo DefensePro, limitando la visibilidad del tráfico protegido y reduciendo el número de eventos registrados respecto a meses anteriores.

Organo Judicial 07/29/2026

Hosts & Vulnerable Hosts In Last 6 Months

Entre enero y abril de 2026, el análisis de vulnerabilidades evidenció una variación en la cantidad de activos vulnerables identificados, principalmente dentro del entorno interno de la organización, donde se concentra la mayor superficie de exposición. Durante abril se identificaron 2,840 hosts internos vulnerables de un total de 4,934 activos evaluados, mientras que en el entorno externo se detectaron 16 activos vulnerables de 82 analizados. Esta tendencia confirma la importancia de mantener un proceso continuo de gestión y remediación de vulnerabilidades, priorizando aquellos activos internos que representan la mayor concentración de hallazgos y reduciendo la posibilidad de que puedan ser aprovechados en caso de un compromiso de seguridad.

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.

Critical Attacks Successfully Blocked

4906

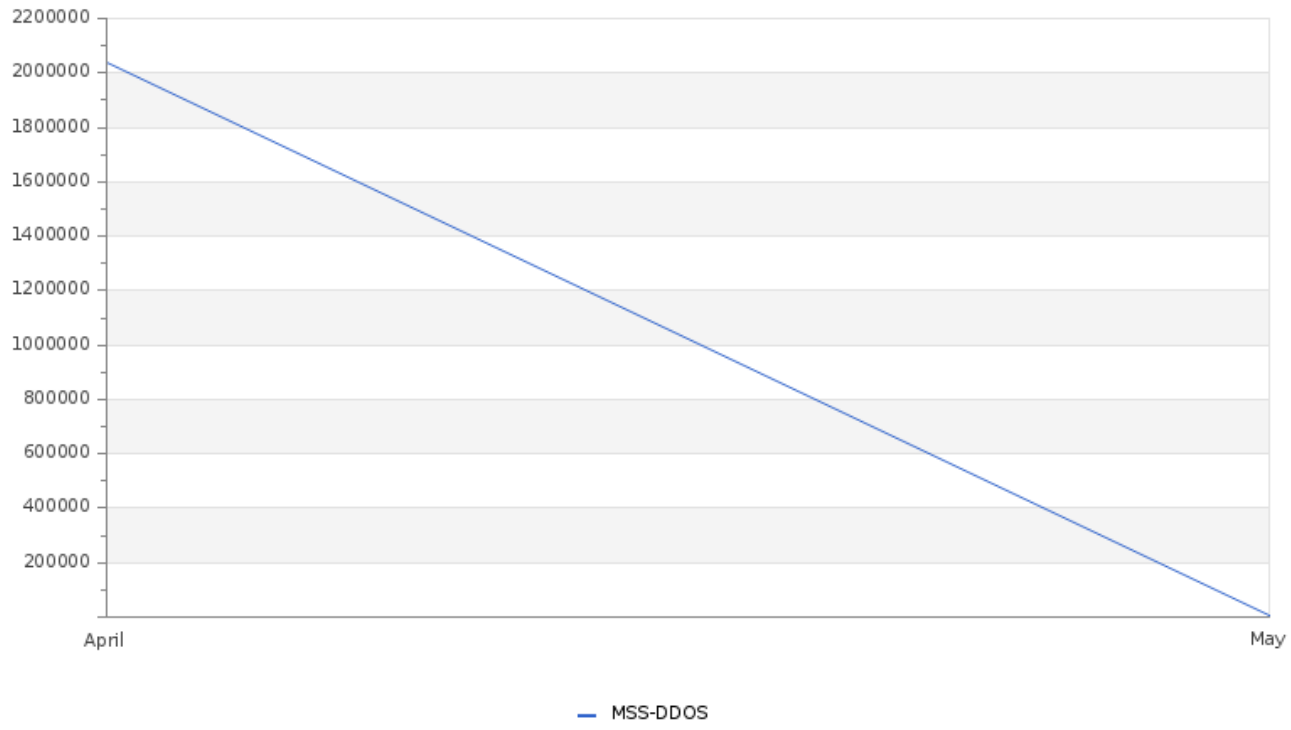
Durante abril de 2026 se bloquearon 1,295,027 ataques de criticidad alta y crítica, lo que representa una disminución del 65.7 % respecto a marzo (3,780,043 ataques críticos). Durante los últimos 30 días se registraron 4,906 eventos críticos.

Los ataques de mayor severidad estuvieron dominados por detecciones asociadas a ERT Active Attacker, lo que evidencia que la inteligencia de amenazas integrada en la plataforma continúa identificando y bloqueando de forma proactiva direcciones IP con actividad maliciosa conocida. En menor proporción se observaron eventos relacionados con listas negras y anomalías de protocolo, manteniéndose como principal objetivo los servicios publicados sobre HTTPS.

Desde una perspectiva ejecutiva, los mecanismos de mitigación continuaron demostrando capacidad para bloquear amenazas de alta criticidad. No obstante, las cifras presentadas deben analizarse considerando la reducción temporal de visibilidad, ya que durante el período únicamente se contó con la telemetría de un DefensePro, por lo que los resultados reflejan únicamente una parte de la actividad real sobre la infraestructura protegida.

Organo Judicial 07/29/2026

Attacks Successfully Blocked



Durante abril de 2026 se bloquearon aproximadamente 2.0 millones de ataques, reflejando una disminución significativa respecto a marzo, cuando se registraron cerca de 5.8 millones de eventos. Aunque esta tendencia muestra un menor volumen de ataques observados durante el período, es importante considerar que la reducción está directamente relacionada con la pérdida de visibilidad del servicio, ya que durante abril únicamente se recibió telemetría de un equipo DefensePro. En consecuencia, las cifras presentadas representan únicamente la actividad registrada por dicho dispositivo y no el comportamiento completo de la infraestructura protegida.

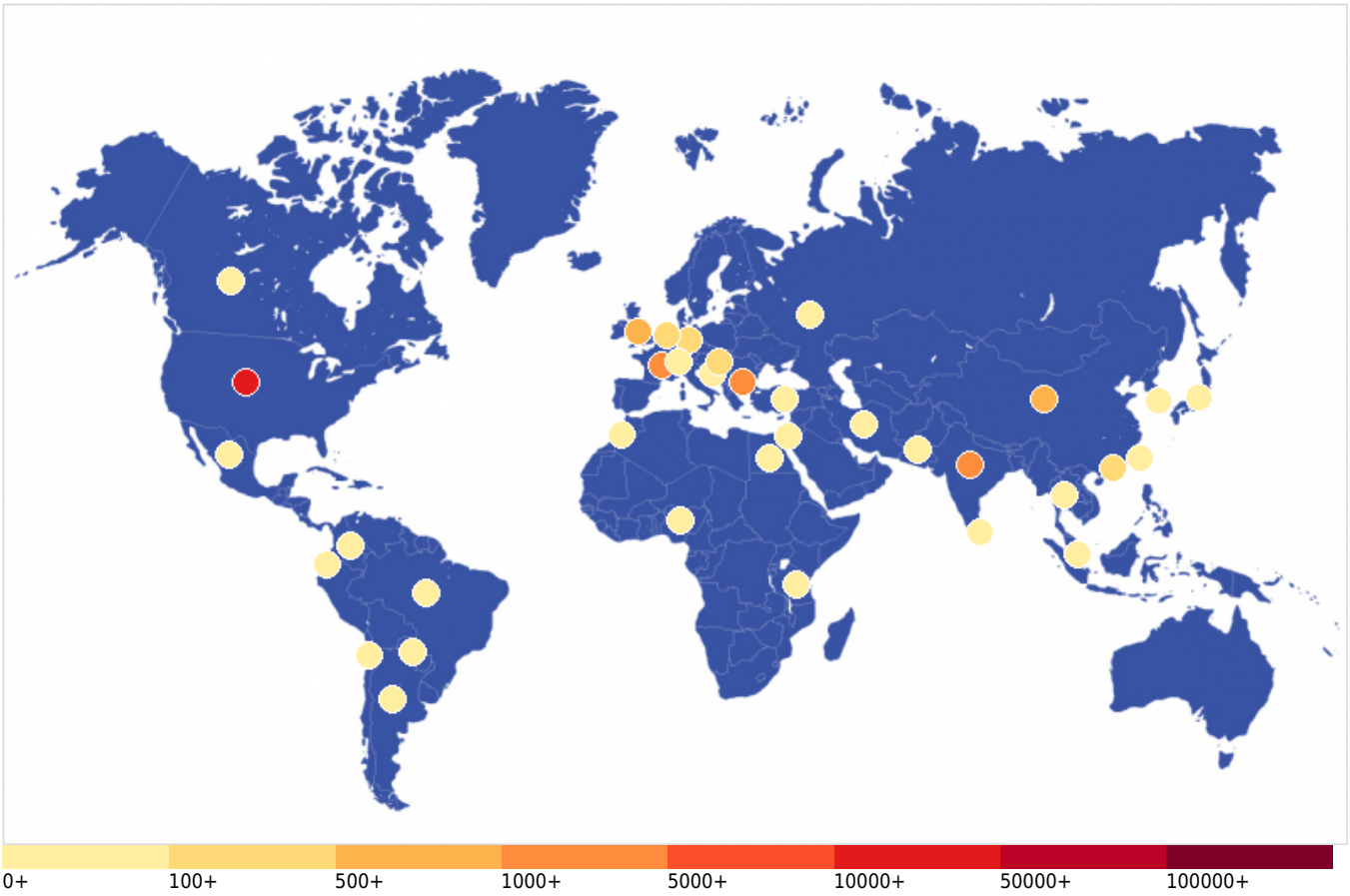
Vulnerability Metric

3

Durante abril, el Vulnerability Metric registró un valor de 3 %, reflejando el nivel de exposición de los activos evaluados. Como complemento a este indicador, el análisis de vulnerabilidades identificó una mayor concentración de hallazgos en el entorno interno respecto a la superficie de ataque externa, reforzando la necesidad de mantener una estrategia continua de gestión y remediación de vulnerabilidades sobre toda la infraestructura tecnológica.

Critical Attacks Per Country In Past Week

Organo Judicial 07/29/2026



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	

Durante el período analizado se observó una distribución global de las fuentes de ataque, evidenciando actividad proveniente de múltiples regiones. Estados Unidos se mantuvo como el principal país de origen con 10,646 eventos registrados, seguido por Francia (3,155), Bulgaria (1,191), India (1,038) y China (521). En un segundo nivel se ubicaron Reino Unido (510), Hungría (349), Alemania (263), Países Bajos (202) y Hong Kong (188). Este comportamiento refleja que la infraestructura expuesta continúa siendo objeto de intentos de ataque desde diferentes ubicaciones geográficas, predominando eventos asociados a infraestructuras internacionales utilizadas para actividades maliciosas y campañas automatizadas de exploración y ataque.

TLP:AMBER

Organo Judicial 07/29/2026

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.**

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