TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

March 13, 2026

Organo Judicial 03/13/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "FEBRERO 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 in 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 continúa siendo baja como consecuencia de la insuficiencia o inconsistencia 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.

Accepted & Actual Risk

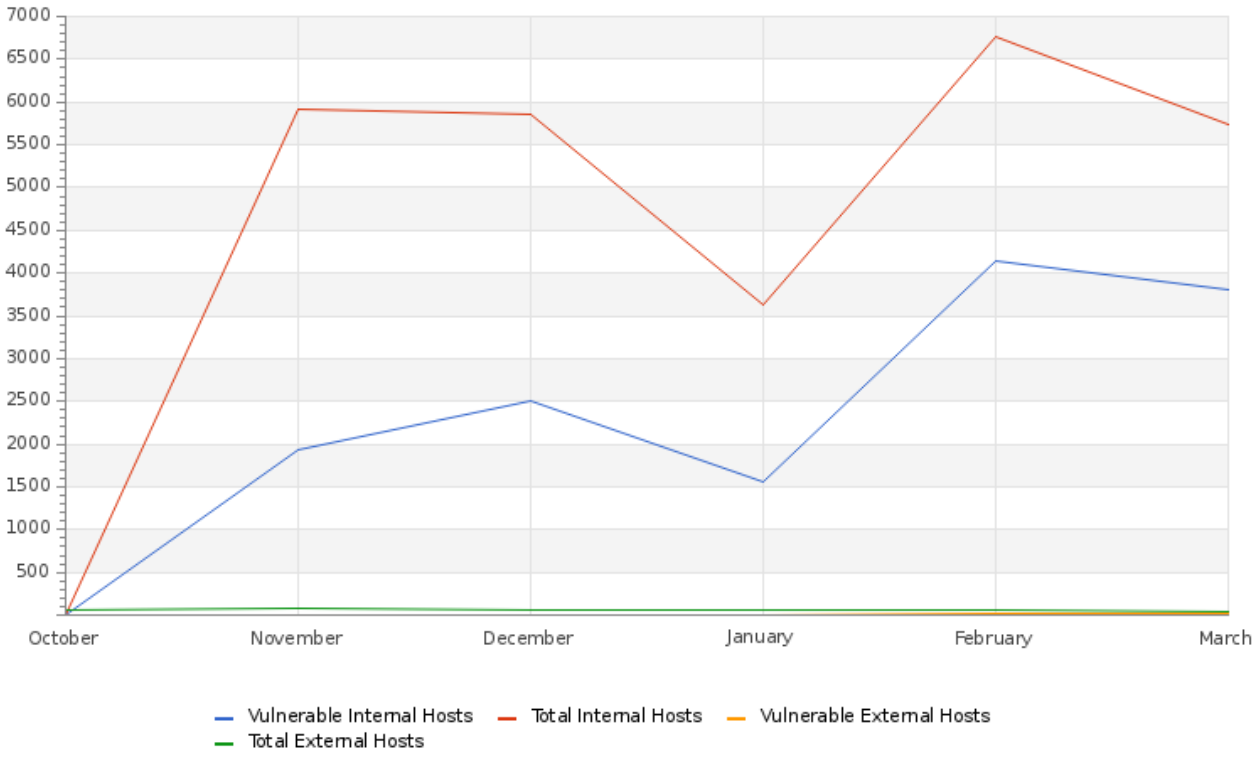
Organo Judicial 03/13/2026

Riesgo Actual:
Durante el periodo analizado, el nivel de riesgo se mantiene estable respecto al mes anterior, con un valor de 5%, categorizado dentro del rango bajo según los parámetros de referencia establecidos. Este resultado confirma que la exposición a incidentes potenciales permanece bajo control y que los controles de seguridad vigentes mantienen su efectividad operacional. Aun así, se considera crítico sostener un esquema de monitoreo continuo, acompañado de una capacidad de respuesta inmediata, para anticipar desviaciones y prevenir incrementos no planificados en el nivel de riesgo.

Riesgo Aceptado:
El riesgo aceptado se mantiene en 1%, reflejando una estrategia de gestión conservadora y consistente frente al riesgo residual. Este indicador evidencia la correcta implementación de controles preventivos y la priorización de acciones de mitigación, garantizando que la exposición permanezca dentro de los umbrales definidos como aceptables por la organización. La estabilidad de este valor respalda la solidez del marco de gestión de riesgos y la alineación con las políticas corporativas de seguridad.

Organo Judicial 03/13/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de febrero, el total de 6,750 hosts activos se mantuvo estable respecto al período anterior, sin variaciones en la infraestructura registrada. No obstante, se identificaron cambios en el número de hosts vulnerables, vinculados principalmente a la cantidad de equipos incorporados en el período. Este comportamiento confirma que las medidas de seguridad implementadas mantienen su efectividad en la gestión de riesgos, incluso en escenarios de estabilidad en el volumen de activos administrados.

La estabilidad en la infraestructura no debe interpretarse como ausencia de riesgo. Es esencial sostener una supervisión continua y una gestión proactiva de la seguridad, con el objetivo de evitar que la invariabilidad en los activos genere una percepción errónea de control. Se recomienda reforzar los procesos de monitoreo, evaluación periódica de vulnerabilidades y respuesta temprana, asegurando que posibles riesgos latentes sean identificados y mitigados oportunamente.

Total Attacks Successfully Blocked

187471

Durante el mes de febrero se registraron 187,471 intentos de ataque bloqueados exitosamente, lo que representa un incremento significativo respecto al mes anterior. Este aumento refleja una mayor actividad maliciosa detectada y contenida en el periodo analizado. A pesar de la intensificación de los intentos, los controles de seguridad implementados mantuvieron una operación eficaz, garantizando un nivel adecuado de protección frente a las amenazas identificadas. La tendencia observada subraya la importancia de mantener un monitoreo continuo, reforzar las capacidades de detección temprana y asegurar la resiliencia de los mecanismos de defensa para sostener la efectividad ante posibles variaciones en el volumen o sofisticación de los ataques.

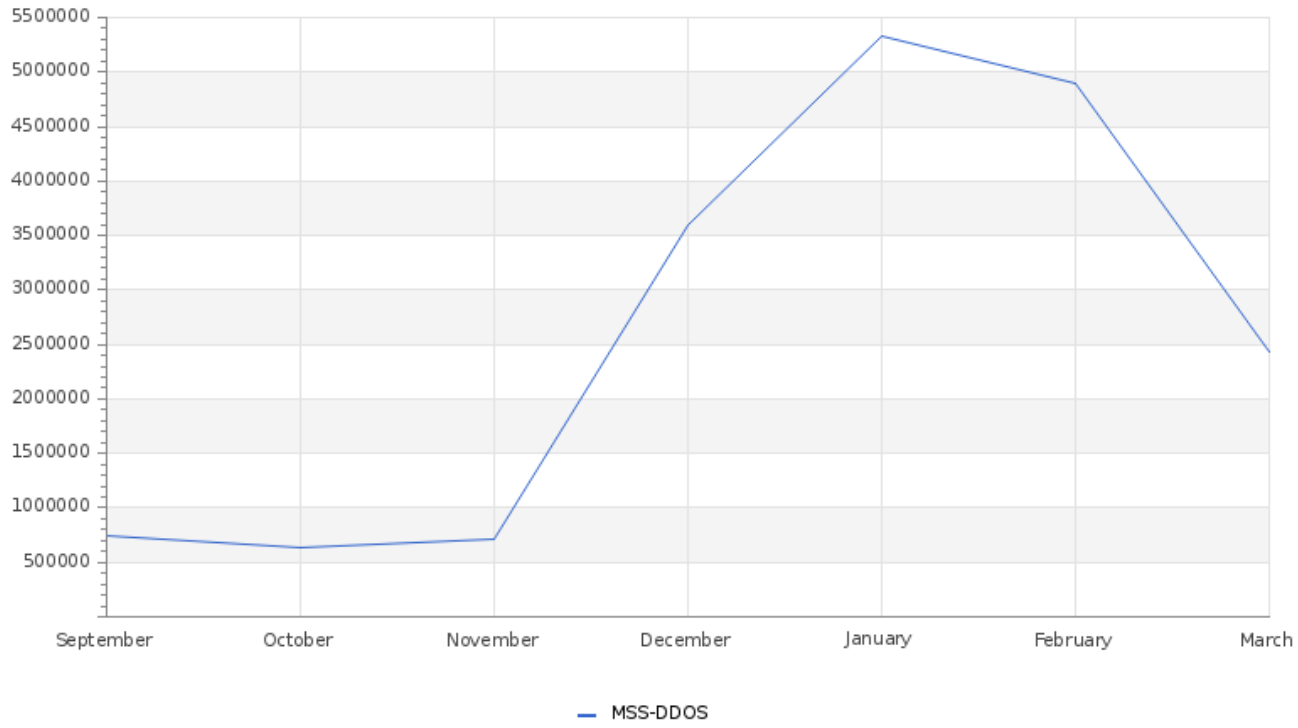
Organo Judicial 03/13/2026

Critical Attacks Successfully Blocked

141256

Durante el presente mes, se identificaron 141,256 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 febrero, el servicio MSS-DDOS registró una reducción significativa en el número de incidentes bloqueados respecto al período anterior, reflejando una disminución notable en la intensidad de las campañas de ataque DDoS. Este comportamiento evidencia un descenso en la actividad maliciosa durante el intervalo analizado.

A pesar de la reducción en el volumen de ataques, el servicio mantuvo una respuesta eficaz y consistente, garantizando la mitigación oportuna de los incidentes y la protección continua de la infraestructura crítica. La capacidad demostrada para adaptarse a escenarios con diferentes niveles de amenaza confirma la resiliencia del sistema y asegura la continuidad operativa frente a ataques DDoS de alta variabilidad.

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

Organo Judicial 03/13/2026

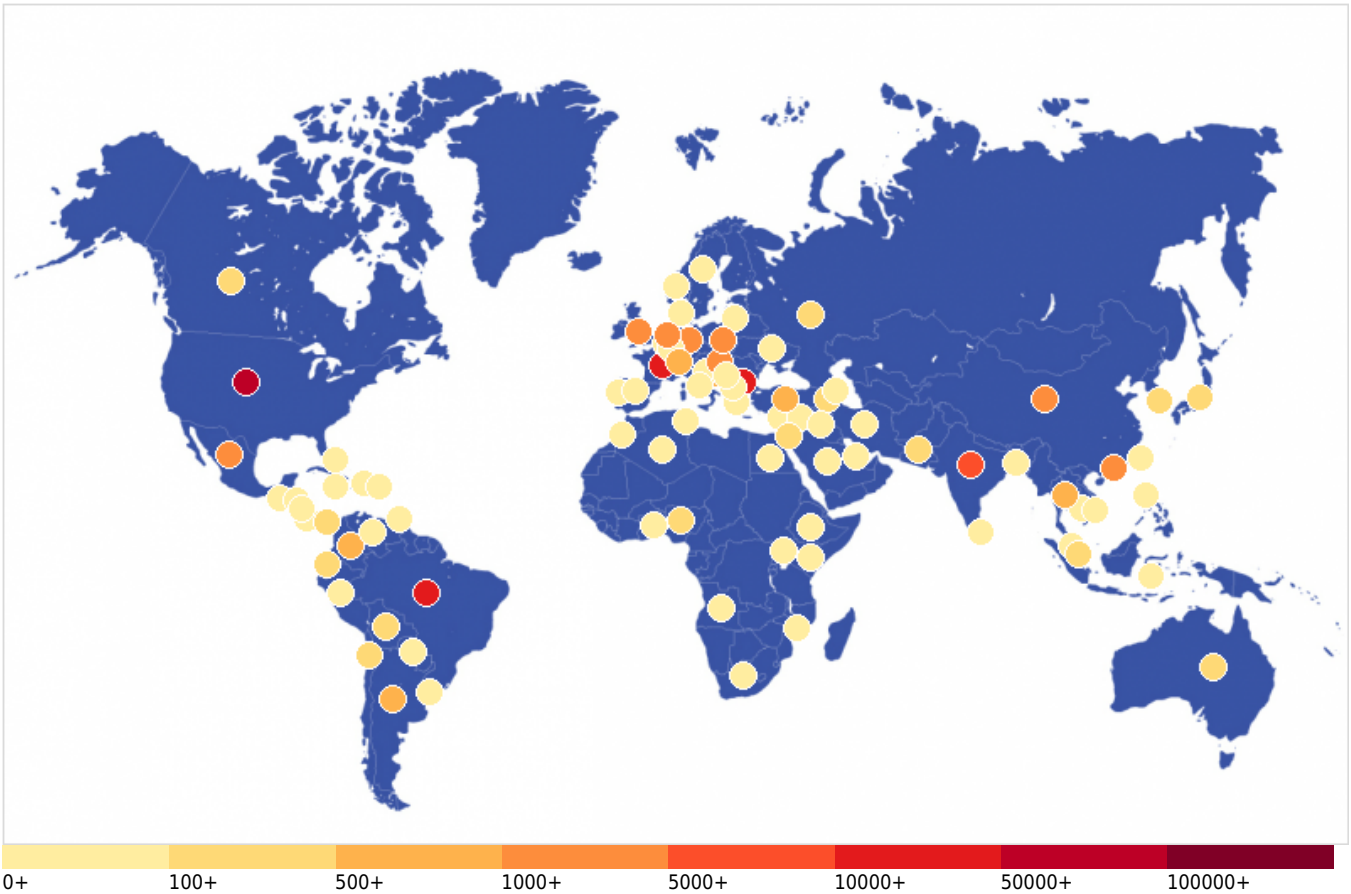
Vulnerability Metric

13

Durante el mes de diciembre, se detectaron 876 host de estado crítico, 6309 host de vulnerabilidad alta, 3285 de vulnerabilidad media y 5372 de vulnerabilidad baja, lo que nos indica que la métrica de vulnerabilidad de la organización es 13%.

La distribución evidencia que, aunque la mayoría de los activos se concentran en niveles de riesgo bajo y medio, existe un volumen relevante de hosts críticos y de alta vulnerabilidad que requieren atención prioritaria. La métrica global del 13% refleja un nivel de exposición que, si bien está dentro de parámetros manejables, demanda una gestión proactiva de remediación para evitar que las vulnerabilidades críticas se traduzcan en incidentes de seguridad.

Critical Attacks Per Country In Past Week



Algeria - 23
Angola - 6
Argentina - 531
Armenia - 135
Australia - 363
Azerbaijan - 30
Bahamas - 3
Bangladesh - 30
Belgium - 29
Bolivia - 114
Bosnia and Herzegovina - 607
Botswana - 24
Brazil - 20280
Bulgaria - 11053
Cambodia - 30
Canada - 253
Chile - 183
China - 2315
Colombia - 500
Costa Rica - 45
Croatia - 3
Cyprus - 8
Denmark - 12
Dominican Republic - 3
Ecuador - 402
Egypt - 6
Ethiopia - 3
France - 26922
Georgia - 3
Germany - 1423
Greece - 3
Guatemala - 24

Honduras - 12
Indonesia - 15
Jamaica - 16
Lithuania - 11
Mexico - 1403
New Zealand - 3
Norway - 68
Peru - 46
Puerto Rico - 15
Saudi Arabia - 3
South Korea - 213
Switzerland - 656
Trinidad and Tobago - 24
Ukraine - 69
Venezuela - 60
Hong Kong - 2418
Iraq - 30
Japan - 437
Luxembourg - 69
Morocco - 3
Nicaragua - 21
Pakistan - 126
Philippines - 3
Qatar - 3
Serbia - 11
Spain - 9
Taiwan - 58
Tunisia - 3
United Kingdom - 3433
Vietnam - 26
Hungary - 2057
Israel - 189
Jordan - 9
Malaysia - 21
Mozambique - 11
Nigeria - 262
Panama - 111
Poland - 1301
Russia - 142
Singapore - 444
Sri Lanka - 8
Thailand - 759
Turkey - 553
United States - 57012
India - 9810
Italy - 3
Kenya - 12
Mauritius - 15
Netherlands - 1366
North Macedonia - 9
Paraguay - 96
Portugal - 3
Saint Kitts and Nevis - 537
South Africa - 15
Sweden - 15
Togo - 6
Uganda - 32
Uruguay - 9

La gráfica correspondiente al período analizado muestra una distribución global de intentos de ciberataques, con una concentración significativa en América del Norte, Europa y algunas regiones de Asia. En esta ocasión, Estados Unidos se posiciona como la principal fuente con 57,012 intentos registrados, seguido por Reino Unido con 3,433, Francia con 2,692, China con 2,315 y Hong Kong con 2,057.

En un segundo nivel se identifican Alemania (1,423), México (1,403), Filipinas (1,301), Países Bajos (1,366) y Bulgaria (1,053), los cuales también representan focos relevantes dentro del volumen total de actividad maliciosa detectada. Asimismo, se observa la participación de otros países como India (981), Brasil (2,280), Turquía (553), Argentina (531) y Singapur (444), lo que refleja una amplia dispersión geográfica en el origen de los ataques.

Esta distribución evidencia que gran parte de la actividad proviene de países con alta infraestructura tecnológica o importantes nodos de conectividad global, lo que puede indicar el uso de servidores comprometidos, servicios en la nube o infraestructuras intermedias para lanzar los ataques. De igual forma, se observa una presencia constante de múltiples regiones, incluyendo Europa del Este, Asia y América Latina, lo que refuerza el carácter global y distribuido del panorama de amenazas.

Este escenario resalta la importancia de mantener estrategias de monitoreo continuo, inteligencia de amenazas y controles de seguridad adaptativos, permitiendo priorizar la detección y mitigación en las regiones con mayor actividad, sin perder una visión integral del entorno de riesgo en constante evolución.

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