



GLE
SEC

COMPLETELY
PERCEPTIVE

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 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 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:

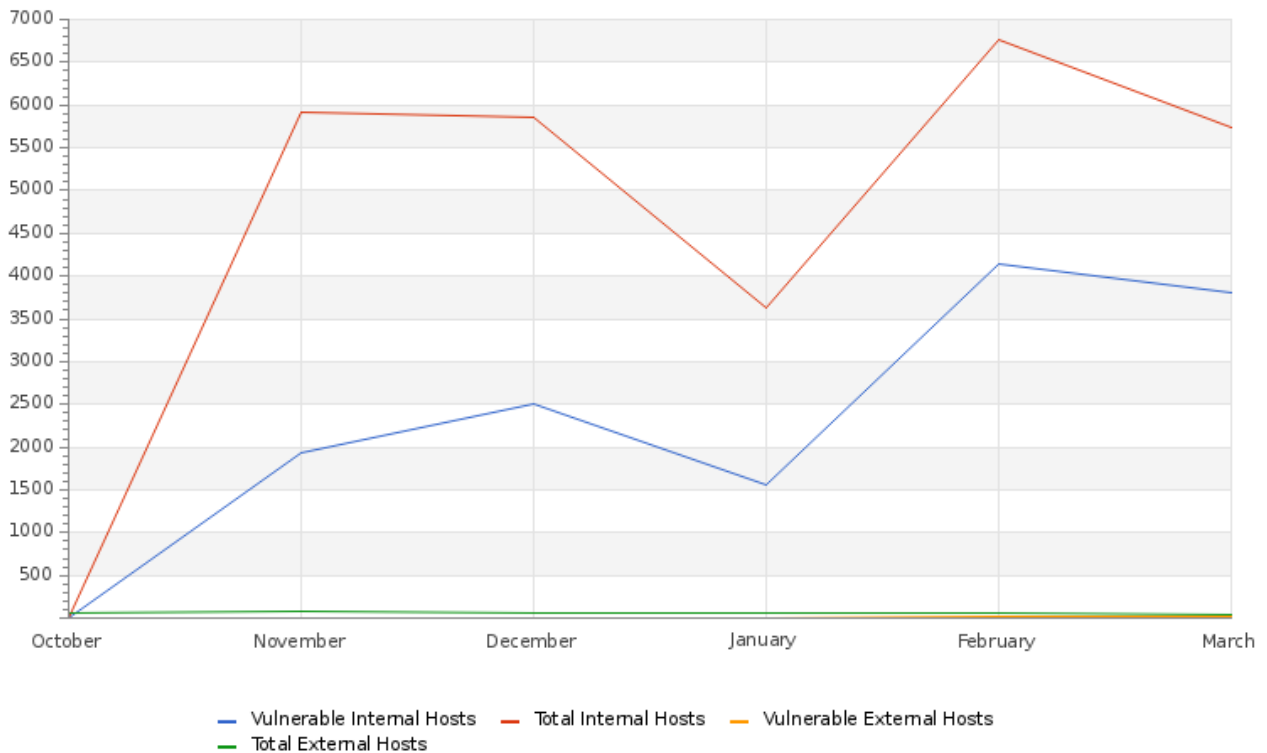
Durante el periodo analizado, el nivel de riesgo se mantiene estable respecto al mes anterior, con un valor de 5%, categorizado dentro del rango bajo según los parámetros de referencia establecidos. Este resultado confirma que la exposición a incidentes potenciales permanece bajo control y que los controles 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.

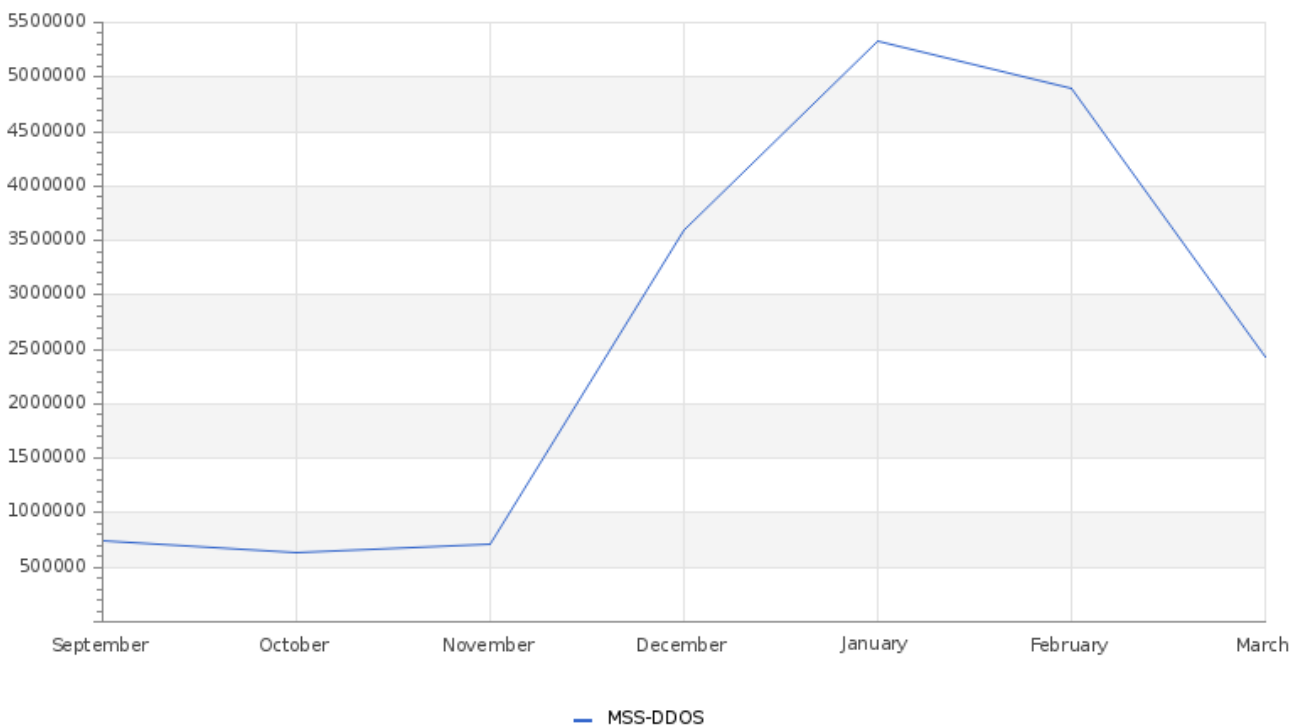
Organo Judicial 03/13/2026

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

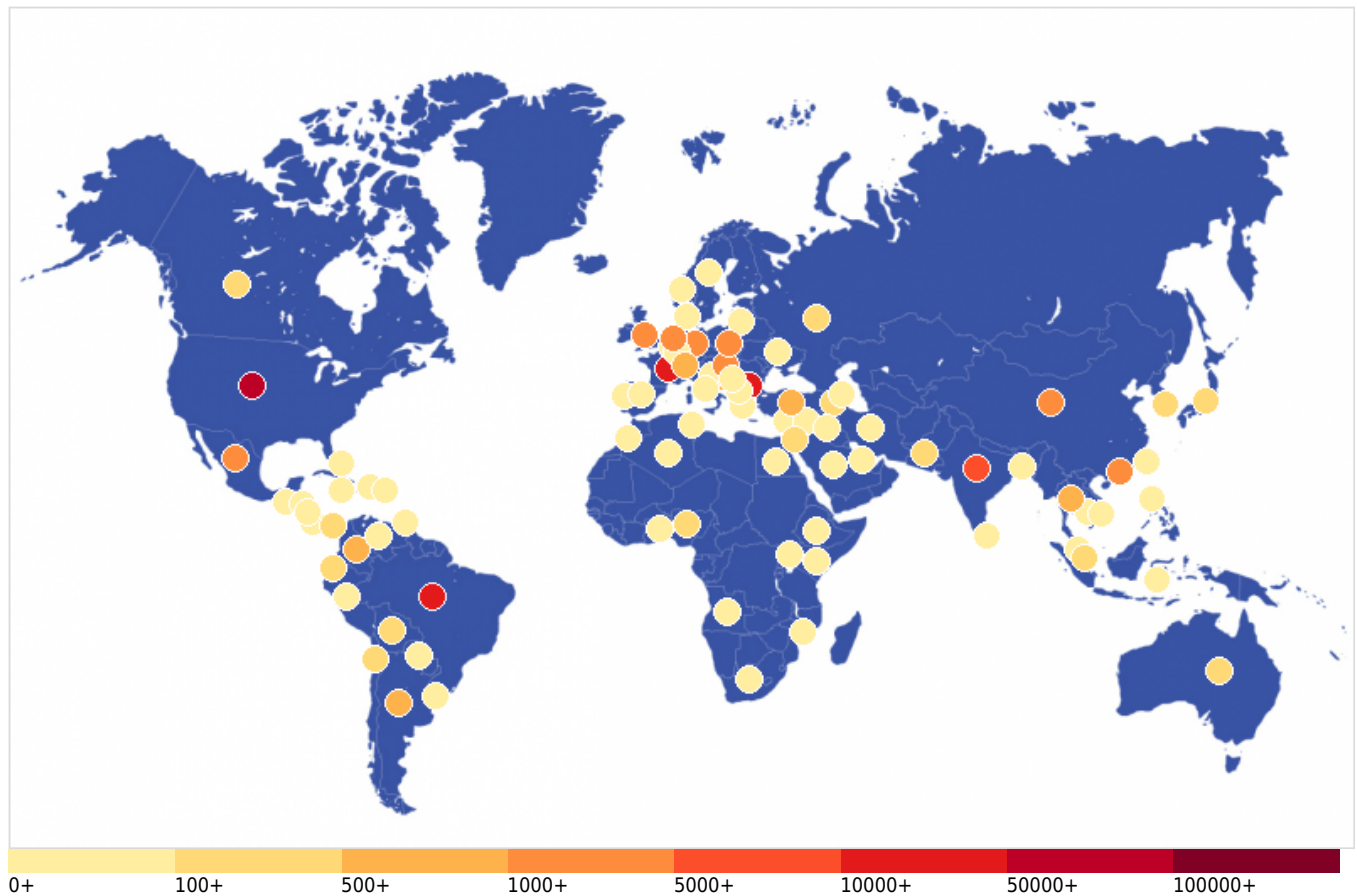


Vulnerability Metric

13

Critical Attacks Per Country In Past Week

Organo Judicial 03/13/2026



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

Organo Judicial 03/13/2026

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.**



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

