TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

August 18, 2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "MAYO 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

Durante el período evaluado no se identificaron amenazas activas asociadas a los activos vulnerables monitoreados. Aunque permanecen vulnerabilidades en los entornos interno y externo, los controles de seguridad implementados continúan reduciendo la exposición observada, manteniendo el Riesgo Real dentro de un nivel bajo.

Accepted Risk

n/a

El análisis continúa realizándose con base en el Riesgo Real identificado y en las mejores prácticas de ciberseguridad aplicables.

Confidence

Low

El nivel de confianza de la evaluación se mantiene en Low, sin cambios respecto al período anterior, debido a que la visibilidad del entorno continúa siendo parcial y no se dispone de una integración completa de todas las fuentes de información necesarias para realizar una evaluación integral del riesgo.

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

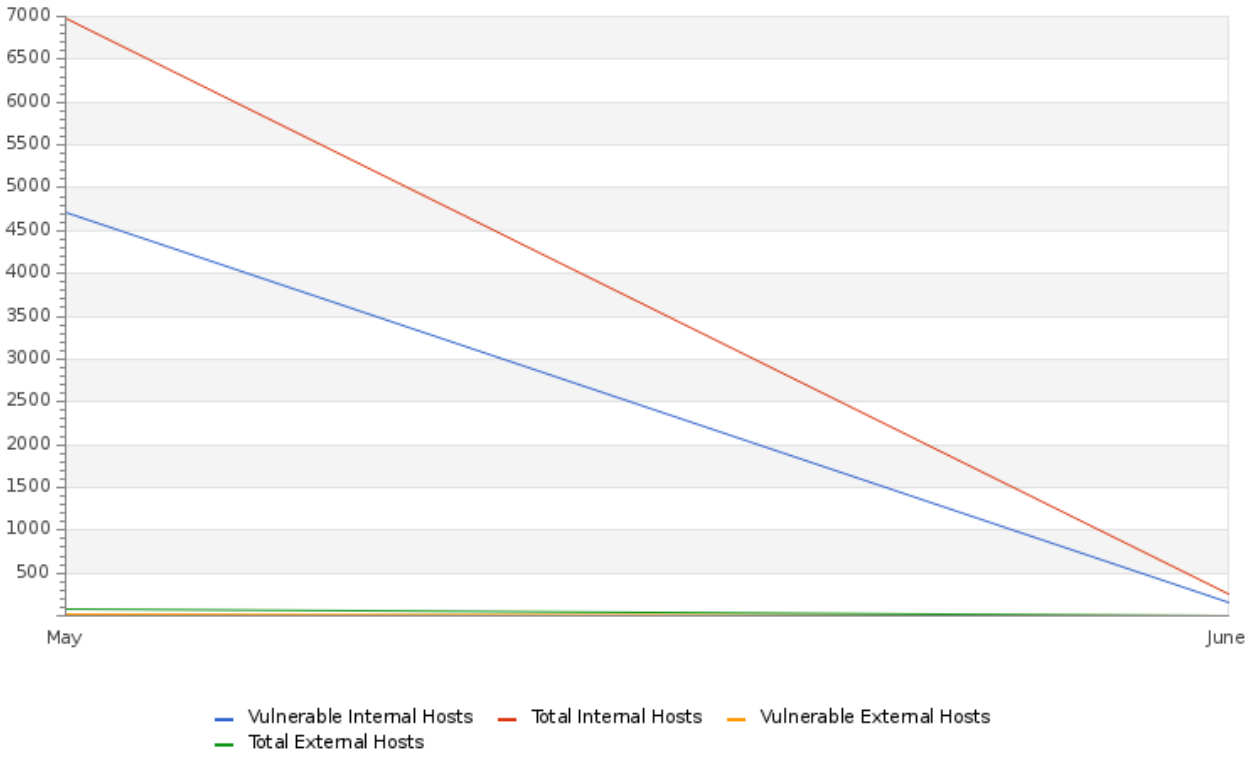
Organo Judicial 08/18/2026

Accepted & Actual Risk

Durante mayo de 2026, los indicadores de Actual Risk y Accepted Risk se mantuvieron sin variaciones respecto al período anterior, por lo que no se identificaron cambios relevantes en el nivel de riesgo representado en el dashboard.
La actividad observada continúa asociada principalmente a intentos de acceso y reconocimiento sobre servicios expuestos, especialmente tráfico dirigido a servicios web y otros activos publicados. Los controles de seguridad implementados continúan mitigando gran parte de esta actividad, manteniendo bajo control la exposición identificada.

Hosts & Vulnerable Hosts In Last 6 Months

Organo Judicial 08/18/2026



Entre marzo y mayo de 2026, la cantidad de hosts evaluados y vulnerables presentó variaciones dentro de la infraestructura interna. En marzo se identificaron 5,061 hosts vulnerables de 7,186 evaluados, representando el mayor volumen del período analizado.
Durante abril se observó una disminución, con 4,484 hosts vulnerables de 6,063 evaluados. Posteriormente, en mayo la cantidad de activos evaluados aumentó a 6,975 hosts, de los cuales 4,715 presentaron vulnerabilidades, lo que representa un incremento de 231 hosts vulnerables respecto a abril.
En términos generales, luego de la reducción observada en abril, durante mayo volvió a incrementarse la cantidad de sistemas vulnerables. Por este motivo, se recomienda mantener el seguimiento continuo de estos activos y priorizar la remediación de aquellos que concentran vulnerabilidades de mayor severidad.

Total Attacks Successfully Blocked

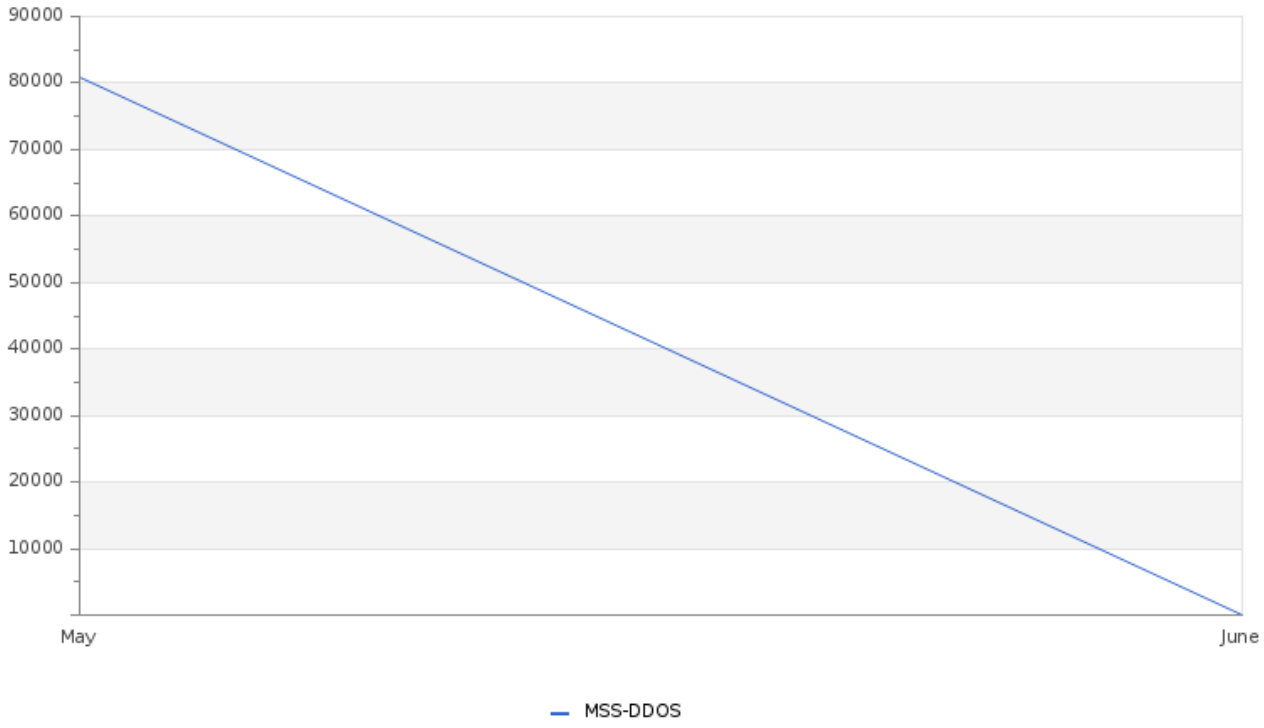
0

Critical Attacks Successfully Blocked

0

Organo Judicial 08/18/2026

Attacks Successfully Blocked



Durante el mes de Mayo se observó actividad asociada a intentos de ataques DDoS dirigidos contra los servicios expuestos de la organización. Este tipo de comportamiento continúa representando un riesgo relevante, principalmente por su capacidad de afectar la disponibilidad de recursos y servicios institucionales.
Los mecanismos de protección implementados permitieron identificar y mitigar de forma oportuna los eventos registrados, reduciendo la posibilidad de interrupciones operativas y contribuyendo a mantener la continuidad de los servicios.
En términos generales, los resultados reflejan una respuesta efectiva de los controles especializados frente a este tipo de amenazas. La actividad observada durante el período confirma la importancia de mantener capacidades continuas de monitoreo, detección y mitigación sobre los servicios expuestos a Internet, fortaleciendo así la resiliencia operativa de la organización.

Vulnerability Metric

8

Durante mayo, el Vulnerability Metric disminuyó de 9 a 8, reflejando una ligera reducción en el nivel de exposición respecto al período anterior. Aunque el indicador presenta una mejora, se mantiene la necesidad de continuar con las actividades de gestión y remediación de vulnerabilidades, especialmente sobre los activos internos donde se concentra la mayor cantidad de hallazgos.
En términos generales, la variación observada indica una mejora moderada en la postura de vulnerabilidades, sin representar todavía una reducción suficiente para disminuir la prioridad de las acciones correctivas.

TLP:AMBER

Organo Judicial 08/18/2026

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