TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

September 01, 2026

Organo Judicial 09/01/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "JUNIO 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.

RISK

Actual Risk

n/a

Durante junio no se identificaron amenazas activas que permitieran establecer un nivel cuantificable de riesgo actual. Aunque permanecen hallazgos de vulnerabilidad y actividad de seguridad bajo monitoreo, los controles implementados continúan limitando la exposición observada durante el período.

Accepted Risk

n/a

El análisis se mantiene enfocado en los riesgos identificados y en las condiciones observadas durante el monitoreo.

Confidence

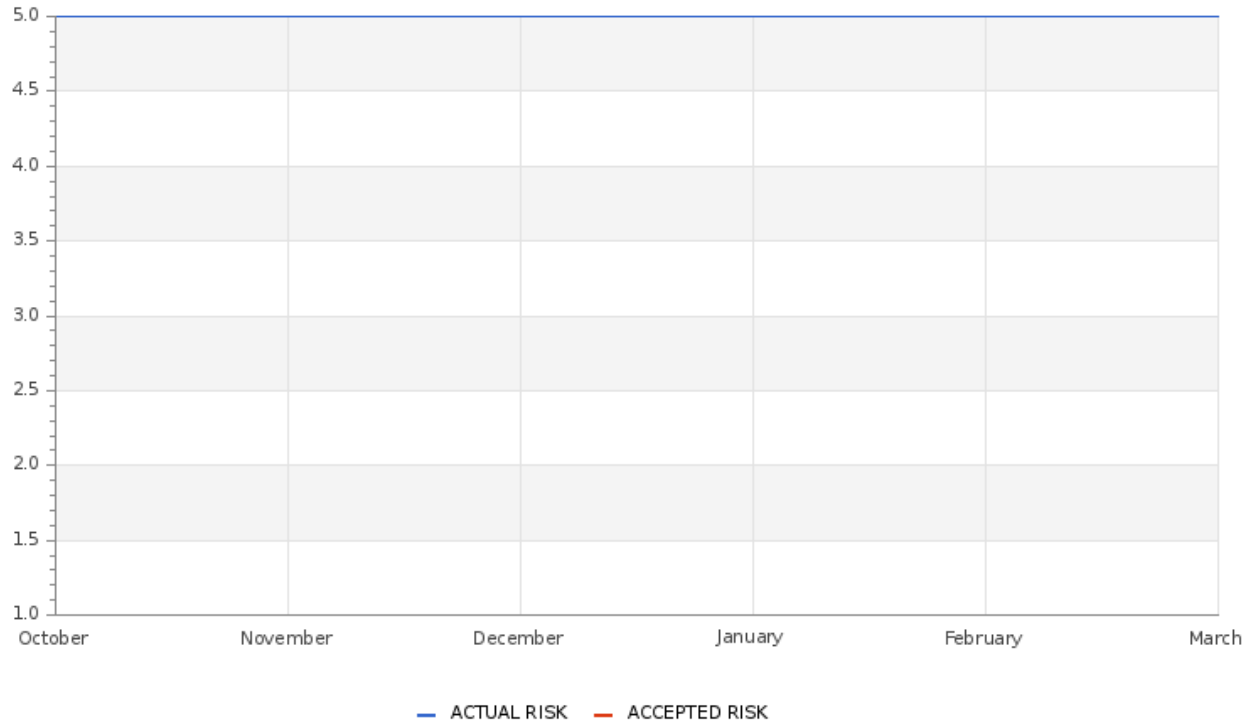
Low

El nivel de confianza se mantiene en Low, debido a que la visibilidad disponible continúa siendo parcial y no se cuenta con la integración completa de todas las fuentes necesarias para realizar una valoración integral del riesgo.

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

Organo Judicial 09/01/2026

Accepted & Actual Risk



Durante junio no se registraron variaciones en los indicadores de Actual Risk y Accepted Risk
La evaluación continúa sustentándose en la información disponible a través de los servicios de monitoreo y seguridad integrados, por lo que la incorporación de nuevas fuentes de telemetría permitiría aumentar la precisión y el nivel de confianza de futuras evaluaciones.

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	0	0

Nivel Actual de Riesgo:
Durante junio, el nivel de riesgo se mantuvo estable respecto al período anterior, sin evidenciar incrementos en la exposición general de la organización. Este comportamiento refleja una continuidad en la postura de seguridad observada, aunque se mantiene la necesidad de supervisar los cambios en vulnerabilidades, actividad perimetral y eventos detectados por los distintos controles de seguridad.

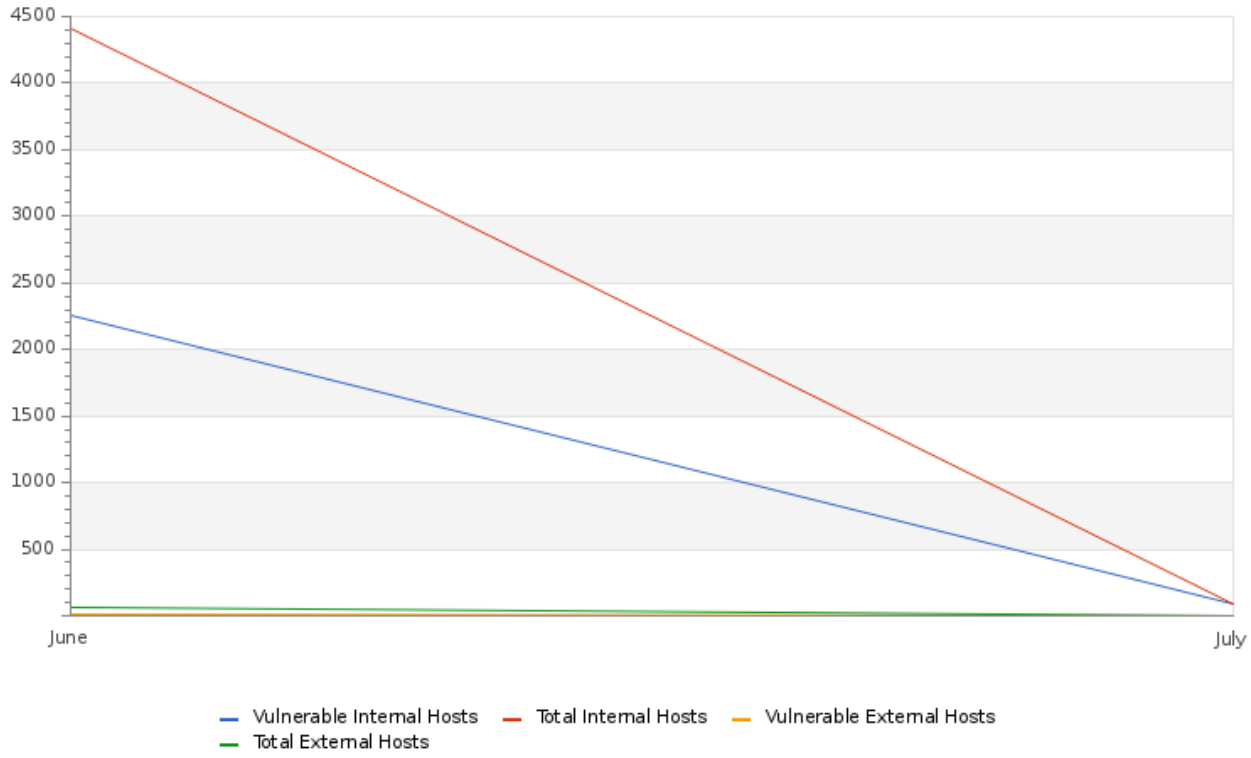
Riesgo Aceptado:
El indicador de riesgo aceptado no presentó variaciones durante el período. Al mantenerse sin un margen de aceptación definido, resulta importante continuar evaluando los riesgos identificados de acuerdo con su criticidad y posible impacto, priorizando aquellos que puedan afectar activos o servicios relevantes para la operación.

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

Organo Judicial 09/01/2026

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



Entre mayo y junio de 2026, la evolución de los activos internos muestra una mejora en el nivel de exposición de la infraestructura. Durante junio se evaluaron 7,072 hosts internos, de los cuales 4,298 presentaron vulnerabilidades activas.

Frente a mayo, cuando se identificaron 4,742 hosts vulnerables de 7,051 evaluados, junio registró una disminución de 444 activos vulnerables, a pesar de que la cantidad total de sistemas evaluados aumentó ligeramente. Como resultado, la proporción de hosts vulnerables disminuyó de aproximadamente 67.3 % a 60.8 %, reflejando una mejora durante el período.

La superficie externa continúa representando una proporción considerablemente menor frente al entorno interno, por lo que la principal concentración de exposición permanece dentro de la infraestructura interna. Se recomienda mantener el seguimiento de esta tendencia y priorizar los activos que concentran vulnerabilidades de mayor severidad.

Organo Judicial 09/01/2026

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	ojbiocontrol.organojudicial.gob.pa	0
Current	3	

Durante junio se observaron variaciones en la cantidad de vulnerabilidades asociadas a distintos activos monitoreados. Entre los hosts que presentaron cambios durante el período destaca ojbiocontrol.organojudicial.gob.pa, donde se identificaron nuevos hallazgos respecto al mes anterior.

Este comportamiento evidencia cambios en la exposición de determinados sistemas y refuerza la importancia de mantener un seguimiento continuo sobre los activos que presentan incrementos o nuevas vulnerabilidades, con el objetivo de validar su criticidad y priorizar las acciones de remediación correspondientes.

Vulnerability Metric

5

Durante junio, el Vulnerability Metric disminuyó de 8 a 5 respecto al período anterior, reflejando una mejora relevante en el nivel de exposición asociado a las vulnerabilidades identificadas.

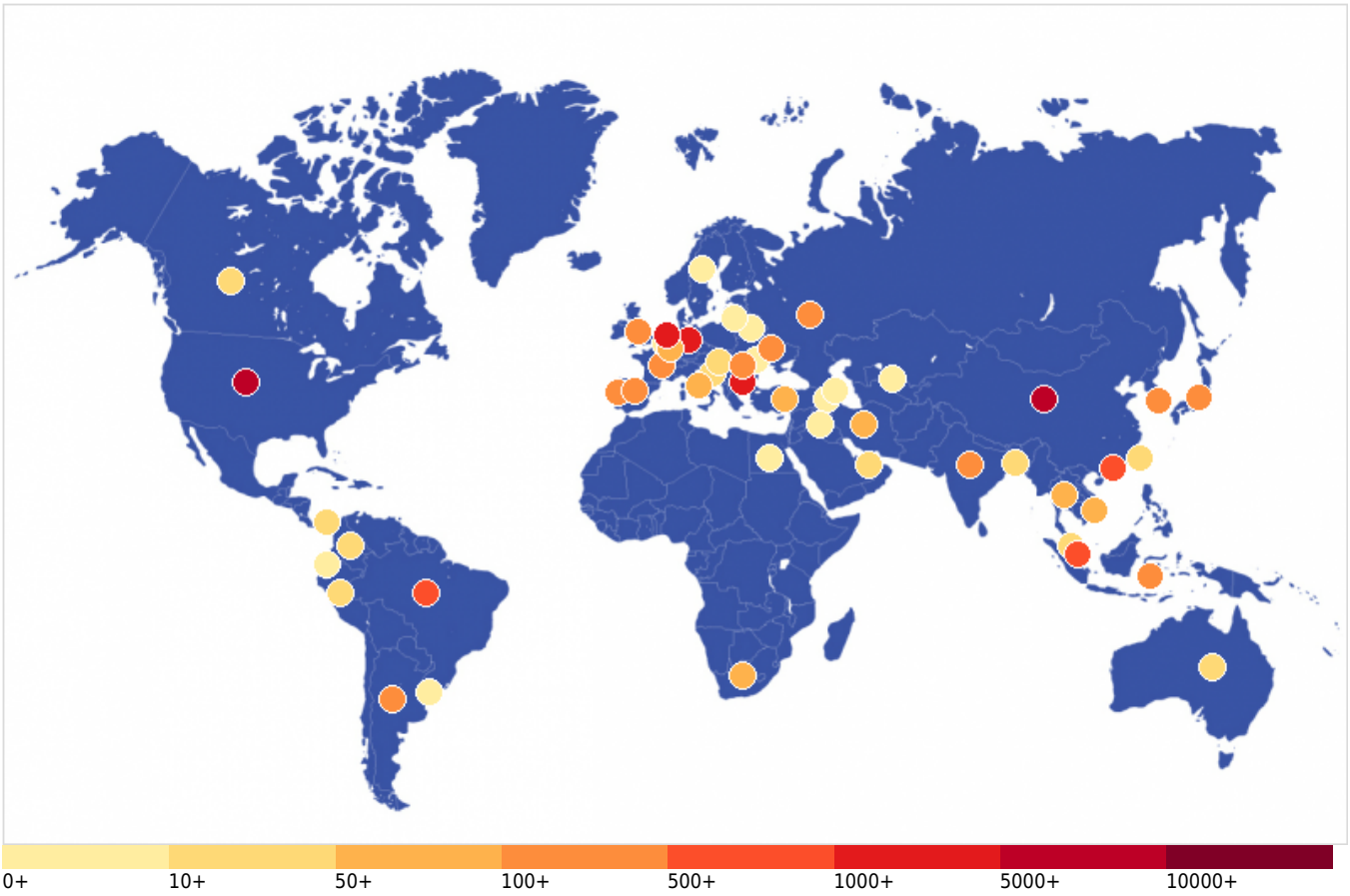
Esta reducción es consistente con la disminución observada en la cantidad de hosts vulnerables durante el período y sugiere una evolución favorable en la postura de vulnerabilidades. No obstante, se recomienda mantener la priorización de los hallazgos críticos y altos, especialmente aquellos asociados a activos de mayor relevancia para la operación.

THREATS

Critical Attacks Per Country In Past Week

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

Organo Judicial 09/01/2026



Andorra - 111
Argentina - 414
Armenia - 4
Australia - 41
Azerbaijan - 3
Bangladesh - 24
Belarus - 4
Belgium - 2
Bosnia and Herzegovina - 19
Brazil - 582
Bulgaria - 3072
Canada - 22
China - 5746
Colombia - 10
Ecuador - 3
Egypt - 3
France - 288
Germany - 1173
Hong Kong - 517
Hungary - 10
India - 481
Indonesia - 159
Iran - 64
Iraq - 2
Italy - 65
Japan - 229
Lithuania - 2
Luxembourg - 97
Malaysia - 39
Mauritius - 2
Moldova - 4
Netherlands - 1342
New Zealand - 34
Panama - 12
Peru - 22
Portugal - 161
Romania - 147
Russia - 225
Saint Kitts and Nevis - 57
Seychelles - 15
Singapore - 669
South Africa - 52
South Korea - 339
Spain - 390
Sweden - 4
Taiwan - 34
Thailand - 55
Turkey - 83
Ukraine - 127
United Arab Emirates - 11
United Kingdom - 243
United States - 6024
Uruguay - 2
Uzbekistan - 9
Vietnam - 95

Durante el período analizado se observa una distribución geográfica amplia de ataques críticos, con actividad proveniente de múltiples regiones, principalmente de Norteamérica, Europa y Asia. Este comportamiento evidencia que la exposición de los servicios publicados no se encuentra asociada a una única ubicación o fuente específica, sino a un entorno de amenazas distribuido globalmente.

La presencia simultánea de actividad desde diferentes países es consistente con comportamientos automatizados de reconocimiento, escaneo y explotación de servicios expuestos, por lo que el origen geográfico debe considerarse como un indicador complementario y no como el único criterio para determinar el nivel de riesgo.

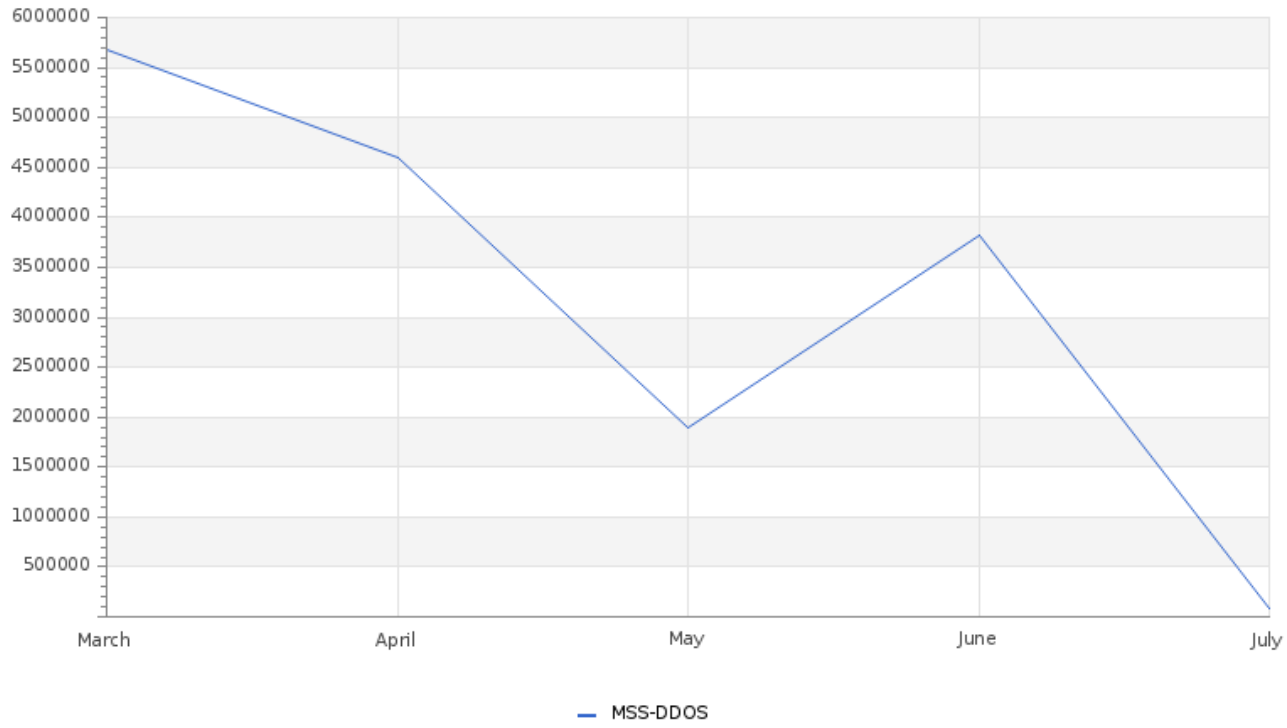
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Organo Judicial 09/01/2026

Este panorama refuerza la importancia de mantener controles perimetrales, mecanismos de reputación y filtrado, así como monitoreo continuo sobre los activos expuestos, prestando especial atención a cambios relevantes en los patrones de origen y a incrementos dirigidos contra servicios críticos.

Total Number of Successful MFA authentications per application

Total Attacks Successfully Blocked Per Service



Durante junio de 2026 se observó un repunte significativo en la actividad asociada al servicio MSS-DDoS, registrándose 3,785,490 eventos, frente a 1,801,502 eventos identificados en mayo, lo que representa un incremento aproximado del 110.13 %.

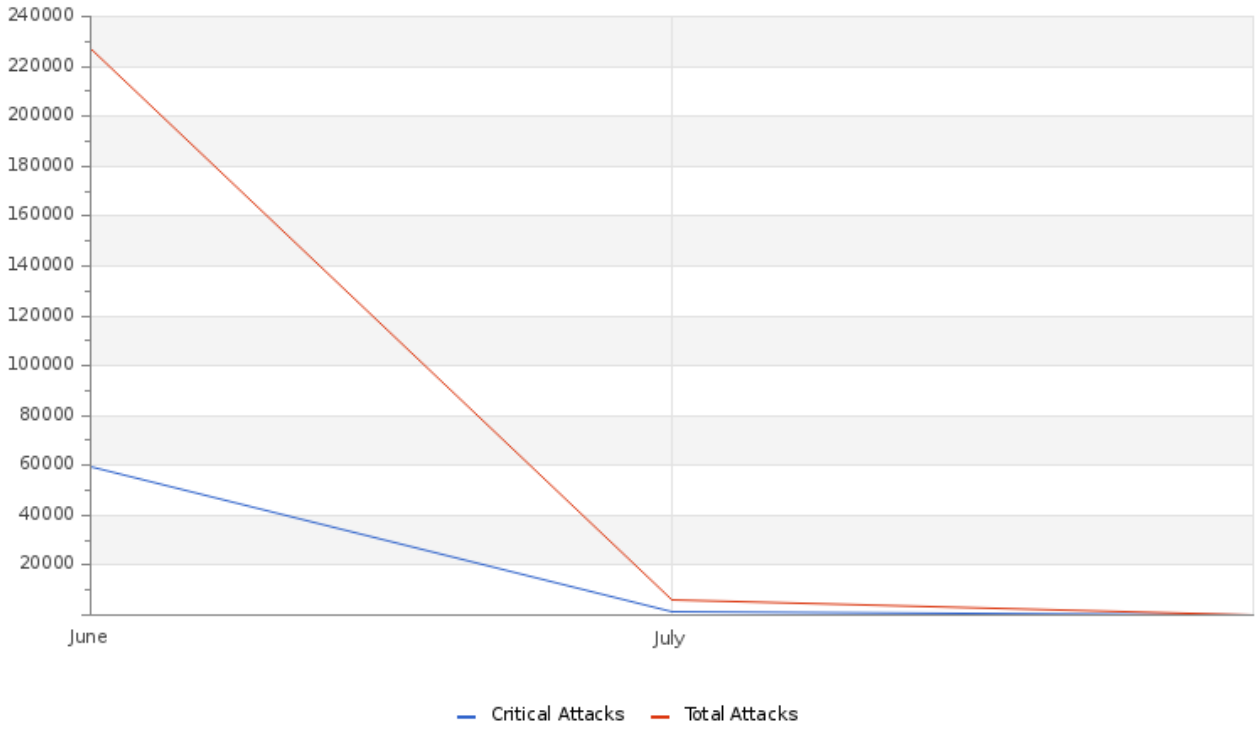
A pesar de este incremento respecto al mes anterior, el volumen registrado en junio se mantuvo por debajo de los niveles observados durante marzo y abril, de acuerdo con la tendencia reflejada en la gráfica. La actividad del mes estuvo concentrada principalmente en las categorías Access, con 1,618,644 eventos, y GeoFeed, con 1,573,500 eventos, representando en conjunto la mayor parte de la actividad detectada.

En términos generales, el comportamiento evidencia variaciones importantes en el volumen mensual de ataques dirigidos contra los servicios expuestos, por lo que se recomienda mantener el monitoreo continuo para identificar incrementos anómalos o cambios sostenidos en los patrones de actividad.

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

Organo Judicial 09/01/2026

Attacks Successfully Blocked by Severity



Durante junio de 2026, el servicio MSS-DDoS registró 3,785,490 ataques bloqueados, de los cuales 2,150,903 fueron clasificados como críticos. La cantidad de eventos críticos representa una presencia significativa dentro de la actividad total observada durante el período, evidenciando una presión relevante sobre los servicios y activos expuestos de la organización.

A pesar del volumen y la severidad de la actividad identificada, los controles de protección implementados permitieron bloquear los ataques detectados, reduciendo el riesgo de afectación sobre la disponibilidad y continuidad de los servicios institucionales. Durante el período también se identificaron variaciones relevantes en la actividad de ataques perimetrales críticos dirigidos hacia determinados activos, los cuales fueron mantenidos bajo seguimiento debido a su nivel de severidad y comportamiento respecto a sus valores habituales.

En este sentido, se recomienda mantener especial seguimiento sobre la evolución de los ataques críticos y los activos que concentran los mayores niveles de actividad, con el objetivo de identificar oportunamente cambios significativos en los patrones de ataque y mantener priorizadas las medidas de protección correspondientes.

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

Organo Judicial 09/01/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	19	4
Critical Device Outages	0	0

Durante junio se observó un incremento significativo en los eventos de indisponibilidad respecto al período anterior, lo que refleja una mayor recurrencia de afectaciones sobre los dispositivos y servicios monitoreados.

A pesar de este aumento, no se registraron interrupciones clasificadas como críticas, por lo que no se evidenciaron afectaciones de alta severidad sobre la continuidad de los servicios esenciales.

Este comportamiento hace recomendable mantener especial seguimiento sobre los activos que presentan eventos recurrentes de disponibilidad, con el objetivo de identificar posibles patrones, causas comunes o degradaciones operativas antes de que puedan derivar en afectaciones de mayor impacto.

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
DevConsejo de Administración de la Carrera Judicial ice	HTTP Advanced	Web Servers	Down		8229	2026-06-01 00:01:25	2026-07-01 09:00:47
Comision de Curadores y Auxiliares Judiciales	HTTP Advanced	Web Servers	Down		4600	2026-06-01 00:01:25	2026-06-18 18:00:05
www.organojudicial.gob.pa	Sitio Web Organo Judicial	200.46.13.0/26	Down, Warning		4493	2026-06-01 00:01:26	2026-06-18 17:54:45
GMSA-OJ HyperV	HTTP	GMSA-OJ	Down, Warning		135	2026-06-08 12:58:57	2026-06-23 15:15:41
GMSA-OJ HyperV	Ping	GMSA-OJ	Down, Warning		130	2026-06-08 12:58:57	2026-06-23 15:05:39
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		52	2026-06-06 18:44:08	2026-06-17 22:02:08
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		49	2026-06-06 18:44:15	2026-06-17 22:02:15
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		49	2026-06-06 18:44:12	2026-06-17 22:02:12
Repositorio digital	HTTP Advanced	Web Servers	Down, Warning		48	2026-06-06 18:43:34	2026-06-20 06:00:43
Plataforma Moodle Escuela Judicial	HTTP Advanced	Web Servers	Down, Warning		48	2026-06-06 18:42:55	2026-06-17 22:01:54
Plataforma de correo	HTTP Advanced	Web Servers	Down, Warning		42	2026-06-06 18:44:12	2026-06-30 23:34:17
Gestor Documental	HTTP Advanced	Web Servers	Down, Warning		42	2026-06-06 18:42:45	2026-06-17 22:01:44

Organo Judicial 09/01/2026

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		39	2026-06-06 18:43:51	2026-06-30 16:53:13
Probe Device	System Health	Organo Judicial	Warning		26	2026-06-01 03:01:51	2026-07-01 03:39:55
200.46.65.105	Ping	200.46.65.104/29	Down, Warning		17	2026-06-17 00:10:43	2026-06-23 11:05:01

Durante junio, los eventos de disponibilidad se concentraron principalmente en servicios web institucionales, observándose una mayor recurrencia de intermitencias e indisponibilidades momentáneas en el Consejo de Administración de la Carrera Judicial, la Comisión de Curadores y Auxiliares Judiciales y el portal www.organojudicial.gob.pa.

También se identificaron eventos de menor frecuencia en componentes de infraestructura como GMSA-OJ HyperV, así como en distintas plataformas institucionales, entre ellas Consulta de Fallos, Reporte Biométrico, Repositorio Digital, Moodle, Plataforma de Correo y el Sistema Automatizado de Gestión Judicial.

A pesar del incremento general de eventos de disponibilidad durante el período, no se identificaron afectaciones clasificadas como críticas. El comportamiento observado sugiere mantener seguimiento sobre los servicios que presentan intermitencias recurrentes, con el objetivo de identificar posibles patrones y reducir la probabilidad de afectaciones prolongadas sobre la operación.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	0	72,743	0	148	0

Durante los últimos días de junio, la actividad bloqueada se concentró principalmente en el servicio MSS-DDOS, con 72,743 eventos, mientras que MSS-EDR registró 148 eventos.

Sin embargo, al considerar el análisis consolidado del mes de junio, el servicio MSS-DDOS registró un total de 3,785,490 eventos asociados a actividad de ataques, confirmando que este servicio concentró la mayor actividad observada durante el período.

Este comportamiento evidencia la importancia de mantener el seguimiento continuo de ambos servicios, especialmente ante variaciones significativas en el volumen o severidad de los eventos detectados.

Organo Judicial 09/01/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	136
Change in Critical Perimeter Attacks	502
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	83
Non Baselined Discovered System	453
High Persistency Detection	89
Change in External High or Critical Vulnerabilities	144
Change in Systems Availability	46
Notable Event Alert: Vulnerability exposure from Threat Intelligence	3
Monitoring for open ports	1

Critical Perimeter Attacks y Non Baselined Discovered System continúan siendo los principales indicadores de actividad, por lo que la exposición de servicios y el control sobre activos descubiertos permanecen como áreas relevantes de seguimiento. También persisten eventos relacionados con vulnerabilidades críticas o altas, tanto internas como externas, aunque con una tendencia descendente frente al período anterior.

Los eventos de High Persistency Detection y cambios en la disponibilidad de los sistemas mantienen presencia durante el mes, lo que evidencia la necesidad de continuar correlacionando la actividad de seguridad con el comportamiento operativo de la infraestructura.

En términos generales, junio presenta una menor presión operacional, pero mantiene patrones similares a los observados previamente, con mayor concentración en exposición perimetral, descubrimiento de activos y gestión de vulnerabilidades.

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

CISO 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