TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

September 01, 2026

Organo Judicial 09/01/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "Julio 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 julio no se contó con un nivel cuantificable de riesgo actual en el indicador. No obstante, el análisis del período mantuvo bajo seguimiento vulnerabilidades críticas y altas, actividad asociada al servicio MSS-DDOS y alertas identificadas mediante MSS-EDR

Accepted Risk

n/a

El riesgo aceptado se mantuvo sin un valor cuantificable durante julio. El análisis continúa enfocado en los riesgos identificados y en las condiciones observadas mediante los diferentes servicios de monitoreo, manteniendo el seguimiento sobre los activos y tecnologías con mayor nivel de exposición.

Confidence

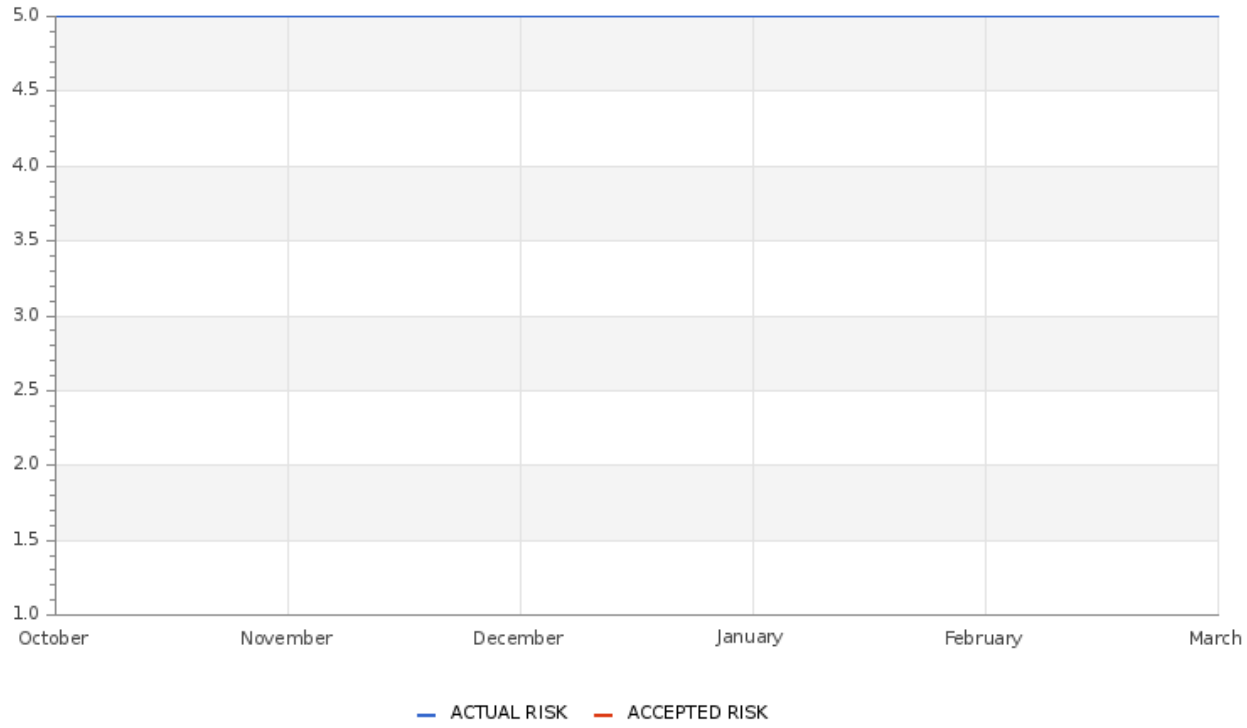
Low

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 julio 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 julio, 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.

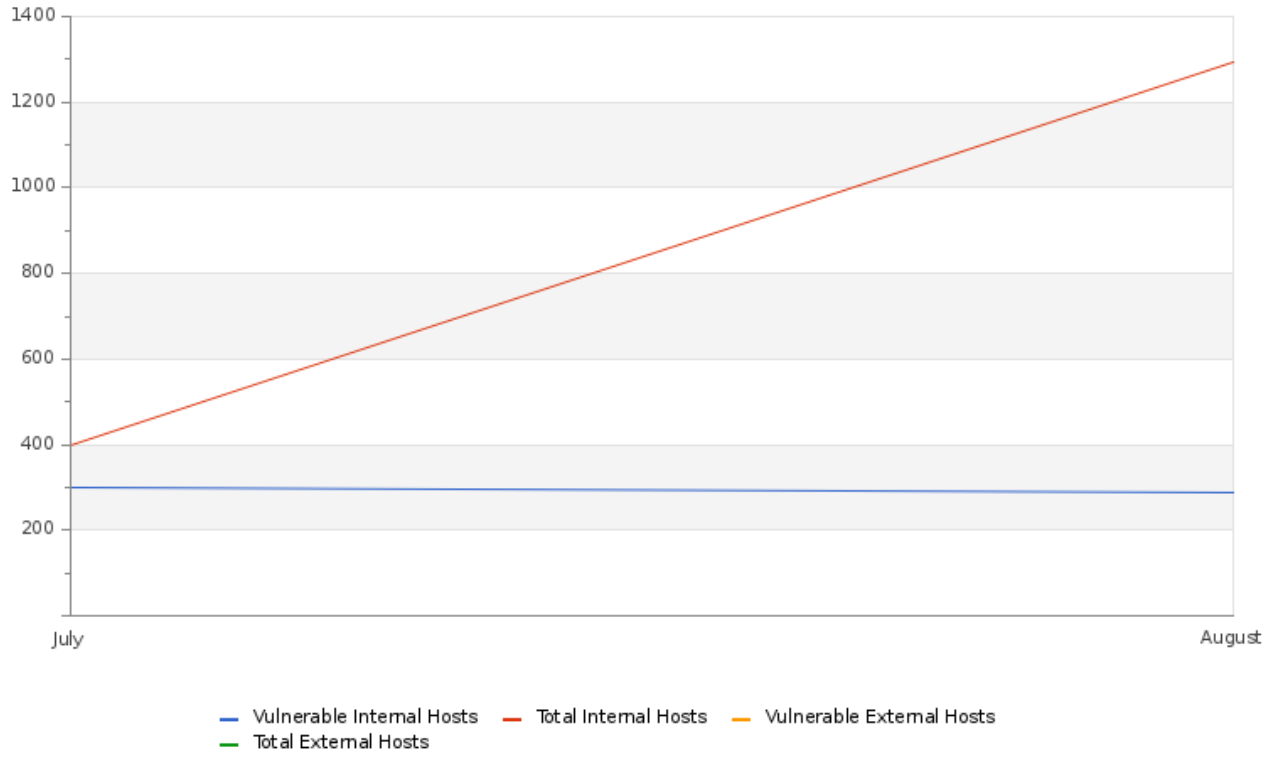
Riesgo Aceptado:
El indicador de riesgo aceptado no presentó variaciones durante el período. Al mantenerse sin un margen de aceptación definido, resulta importante continuar evaluando los riesgos identificados de acuerdo con su criticidad y posible impacto, priorizando aquellos que puedan afectar activos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



Durante julio de 2026, el análisis de vulnerabilidades internas identificó 6,777 hosts evaluados, de los cuales 4,862 presentaron vulnerabilidades activas, reflejando una presencia relevante de sistemas con hallazgos dentro de la infraestructura.

La distribución de vulnerabilidades estuvo compuesta por 580 críticas, 4,295 altas, 2,479 medias y 5,171 bajas. Entre los hallazgos de mayor relevancia se mantuvieron vulnerabilidades asociadas a plataformas Cisco y ArubaOS, así como condiciones relacionadas con IPMI, SNMP y NTP. Adicionalmente, se observó una presencia significativa de ICMP Timestamp, identificada en 4,765 hosts, mientras que la condición SNMP GETBULK Reflection DDoS afectó aproximadamente 500 sistemas.

Este panorama evidencia que una parte importante de la exposición continúa asociada tanto a vulnerabilidades de mayor severidad como a configuraciones y servicios presentes de forma extendida en la infraestructura. Se recomienda mantener la priorización de los hallazgos críticos y altos, junto con el seguimiento de aquellas condiciones que afectan a un mayor número de activos.

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

Organo Judicial 09/01/2026

Vulnerability Metric

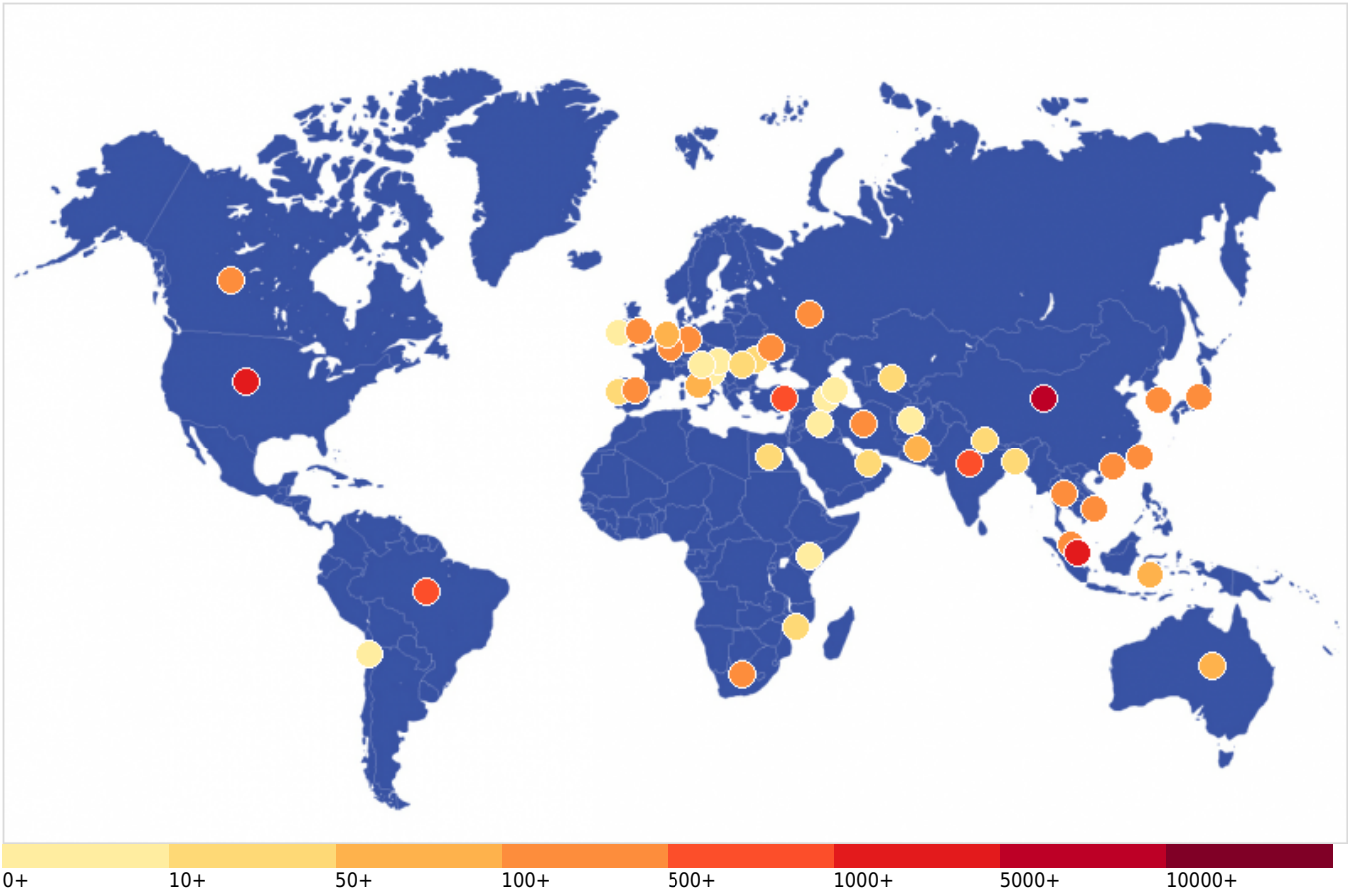
3

Durante julio, el Vulnerability Metric disminuyó de 5 a 3 respecto al período anterior, reflejando una evolución favorable del indicador. No obstante, el análisis del mes identificó 4,862 hosts con vulnerabilidades activas, manteniéndose 580 vulnerabilidades críticas y 4,295 altas, por lo que continúa existiendo una exposición relevante dentro de la infraestructura.

Se recomienda mantener la priorización de los hallazgos críticos y altos, especialmente aquellos asociados a plataformas y activos de mayor relevancia para la operación.

THREATS

Critical Attacks Per Country In Past Week



Afghanistan - 8
Armenia - 6
Australia - 83
Azerbaijan - 8
Bahrain - 5
Bangladesh - 41
Bosnia and Herzegovina - 1
Brazil - 924
Canada - 395
Chile - 7
China - 5536
Egypt - 39
Germany - 421
Hong Kong - 308
Hungary - 9
India - 653
Indonesia - 80
Iran - 186
Iraq - 2
Ireland - 2
Italy - 77
Japan - 143
Kenya - 5
Luxembourg - 114

Organo Judicial 09/01/2026

Malaysia - 130
Nepal - 15
Romania - 46
Slovenia - 3
Taiwan - 133
United Arab Emirates - 16
Vietnam - 129
Mauritius - 13
Netherlands - 59
Russia - 391
South Africa - 130
Thailand - 101
United Kingdom - 228
Moldova - 12
Pakistan - 74
Seychelles - 18
South Korea - 460
Turkey - 826
United States - 3518
Mozambique - 17
Portugal - 46
Singapore - 1093
Spain - 379
Ukraine - 252
Uzbekistan - 35

Durante el período analizado se observa una distribución geográfica amplia de ataques críticos, con actividad proveniente de múltiples regiones. Entre los principales orígenes identificados destacan China, Estados Unidos, Singapur, Turquía e India, concentrando los mayores volúmenes dentro de la gráfica.

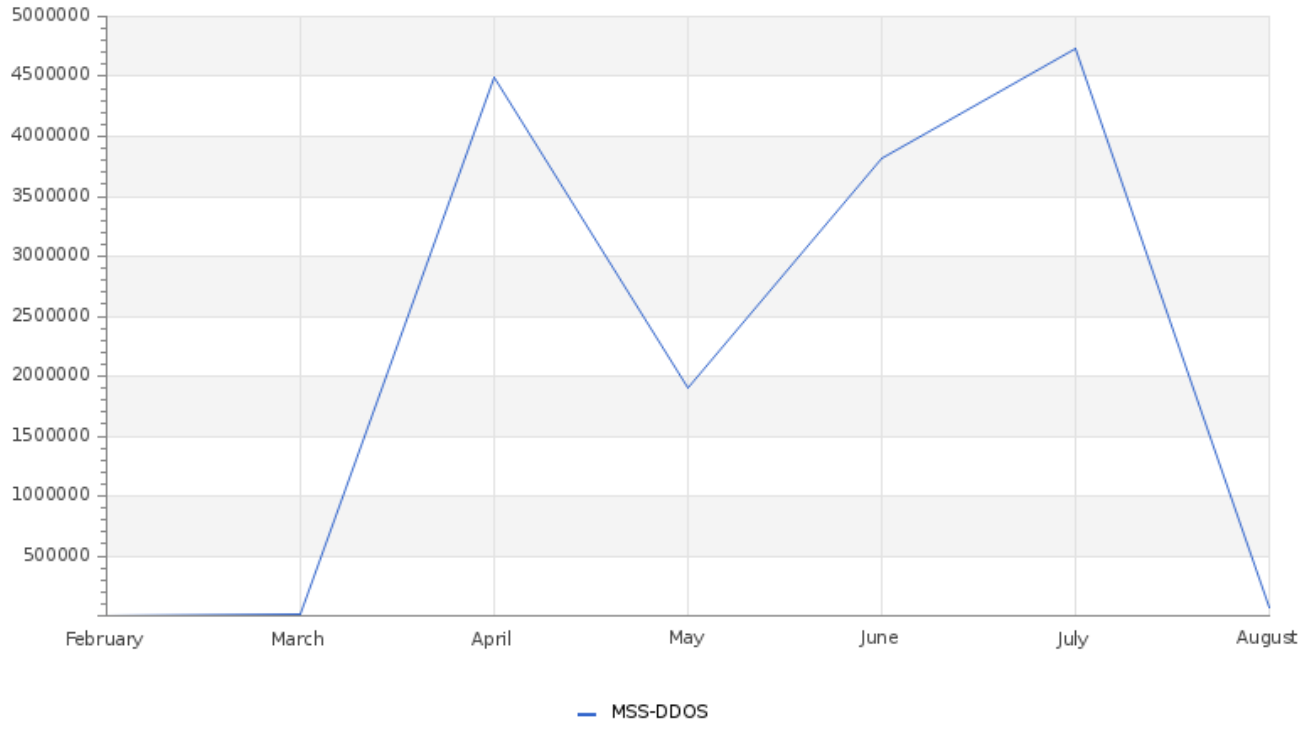
Este comportamiento confirma que la actividad maliciosa dirigida contra los servicios expuestos mantiene un carácter distribuido globalmente y no se encuentra asociada a una única ubicación. La presencia simultánea de eventos desde distintos países es consistente con actividades automatizadas de reconocimiento, escaneo e intentos de explotación, por lo que el origen geográfico debe mantenerse como un indicador complementario dentro del análisis de riesgo.

Durante julio, el servicio MSS-DDOS registró además 4,702,684 eventos asociados a actividad de ataques, manteniéndose una presión significativa sobre la infraestructura expuesta. Se recomienda continuar con el monitoreo de los principales países de origen y prestar especial atención a incrementos relevantes o cambios sostenidos en los patrones de actividad.

Total Number of Successful MFA authentications per application

Total Attacks Successfully Blocked Per Service

Organo Judicial 09/01/2026



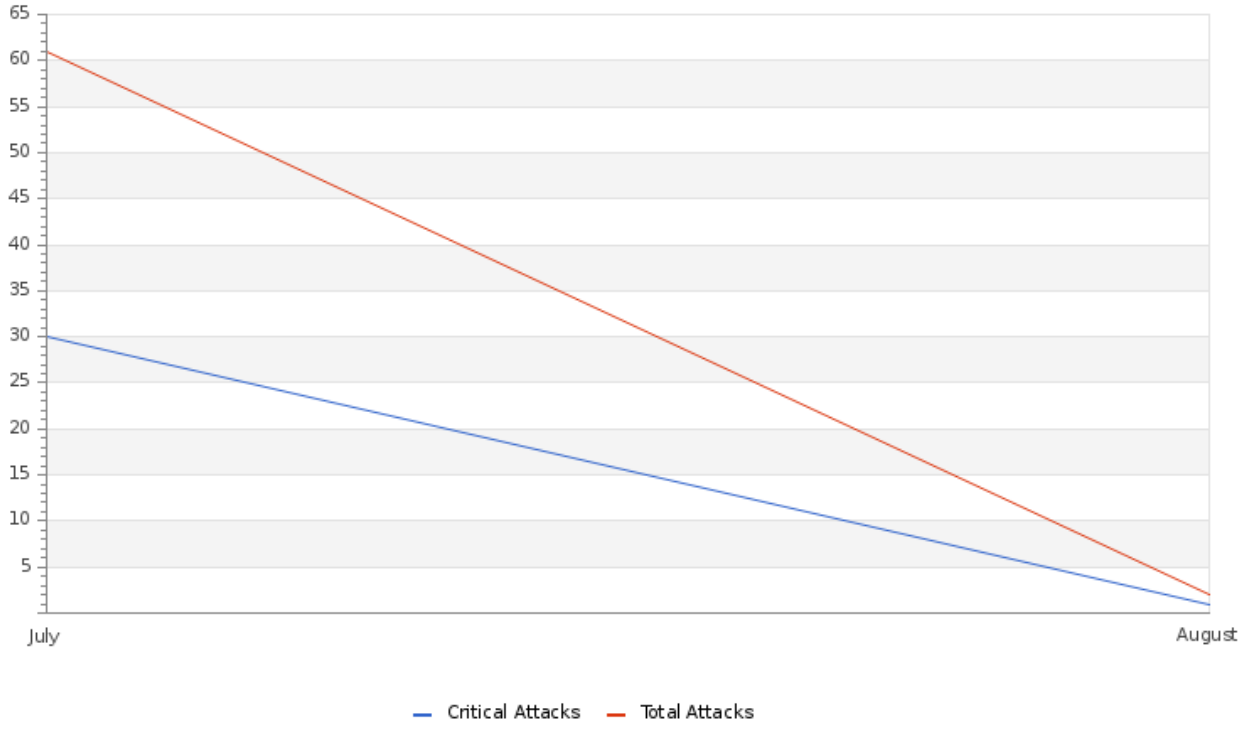
Durante julio se observó un incremento en la actividad asociada al servicio MSS-DDOS respecto a junio, alcanzando un total de 4,702,684 eventos bloqueados durante el período.

La actividad estuvo concentrada principalmente en GeoFeed, con 3,719,354 eventos, seguido de ErtFeed, con 847,279, y Access, con 113,755 eventos. Este comportamiento refleja un aumento en la presión ejercida contra los servicios expuestos, por lo que se recomienda mantener el monitoreo continuo ante variaciones relevantes en los patrones de ataque.

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

Organo Judicial 09/01/2026

Attacks Successfully Blocked by Severity



Durante el cierre de julio, la gráfica refleja 61 ataques bloqueados en las ultimas horas, de los cuales 29 correspondieron a actividad clasificada como crítica.
Sin embargo, al considerar el análisis consolidado del mes de julio, se registraron 4,702,684 ataques, de los cuales 4,567,602 fueron clasificados como críticos, evidenciando que la actividad de mayor severidad representó una parte significativa del volumen observado durante el período. El servicio MSS-DDOS mantuvo una actividad constante, principalmente asociada a GeoFeed, ErtFeed y Access.

Este comportamiento refuerza la importancia de mantener el monitoreo continuo sobre los ataques críticos y las variaciones que puedan presentarse en los servicios expuestos.

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	8	0
Critical Device Outages	0	0

Durante julio se registraron 8 eventos de indisponibilidad asociados a los dispositivos y servicios monitoreados. No se identificaron interrupciones clasificadas como críticas, por lo que no se evidenciaron afectaciones de alta severidad sobre la continuidad de los servicios esenciales.

En términos generales, la actividad observada durante el período evidencia que continúan presentándose eventos de disponibilidad sobre determinados activos, por lo que se recomienda mantener especial seguimiento sobre aquellos que registran recurrencia, con el objetivo de identificar posibles patrones o degradaciones operativas antes de que puedan derivar en afectaciones de mayor impacto.

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

Organo Judicial 09/01/2026

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		8417	2026-07-02 00:03:18	2026-08-01 08:42:52
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		59	2026-07-09 16:36:30	2026-07-23 22:09:27
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		59	2026-07-09 16:51:33	2026-07-23 22:04:32
Repositorio digital	HTTP Advanced	Web Servers	Down		56	2026-07-09 16:41:31	2026-07-09 21:17:14
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		21	2026-07-18 07:58:49	2026-08-01 07:02:49
Probe Device	System Health	Organo Judicial	Warning		19	2026-07-02 13:40:32	2026-07-30 08:05:01
GMSA-OJ HyperV	HTTP	GMSA-OJ	Down, Warning		6	2026-07-13 17:06:47	2026-07-14 21:01:19
Plataforma de correo	HTTP Advanced	Web Servers	Warning		5	2026-07-07 00:36:24	2026-07-27 14:44:17
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Warning		5	2026-07-13 19:02:06	2026-07-21 13:15:15
1.13.46.200.dialup.psinetpa.net (200.46.13.1)	Ping	200.46.13.0/26	Down, Warning		2	2026-07-22 08:33:24	2026-07-29 20:48:24
IP.net126-113.psi.net.pa (200.46.126.113)	Ping	200.46.126.112/29	Down		1	2026-07-29 20:48:03	2026-07-29 20:48:03
200.46.65.105	Ping	200.46.65.104/29	Warning		1	2026-07-29 08:11:16	2026-07-29 08:11:16
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Warning		1	2026-07-23 20:18:56	2026-07-23 20:18:56
GMSA-OJ HyperV	Ping	GMSA-OJ	Warning		1	2026-07-14 21:06:20	2026-07-14 21:06:20

Durante julio, los eventos de disponibilidad se concentraron principalmente en servicios web institucionales, destacándose el Consejo de Administración de la Carrera Judicial, con la mayor recurrencia de eventos durante el período.

También se observaron intermitencias en servicios como Consulta de Fallos, Reporte Biométrico, Repositorio Digital y el Sistema Automatizado de Gestión Judicial, así como eventos de menor frecuencia asociados a GMSA-OJ HyperV, Plataforma de Correo y Plataforma de Gestión de Pleno.

A pesar de la actividad registrada, no se identificaron afectaciones clasificadas como críticas. Se recomienda continuar el seguimiento de los servicios que presentan eventos recurrentes de disponibilidad, con el objetivo de identificar posibles causas comunes y reducir la probabilidad de interrupciones prolongadas.

Organo Judicial 09/01/2026

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	50,535	0	28	0

Durante el cierre de julio, la actividad bloqueada de los ultimos dias se concentró principalmente en los servicios MSS-DDOS, con 50,535 eventos, y MSS-EDR, con 28 eventos.

Sin embargo, al considerar el análisis consolidado del mes, el servicio MSS-DDOS registró 4,702,684 eventos asociados a actividad de ataques, manteniéndose como el servicio con mayor volumen de actividad durante el período.

En cuanto a MSS-EDR, durante julio se documentaron 9 alertas, de las cuales 5 estuvieron asociadas a detecciones de tipo Trojan/TR-Malware y 4 a eventos de tipo Exploit relacionados con EXP/CVE-2017-11882.Gen.

Este comportamiento refleja una mayor concentración de actividad en MSS-DDOS, manteniéndose también eventos relevantes en MSS-EDR que requieren seguimiento continuo.

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

Organo Judicial 09/01/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
High Persistency Detection	39
Change in External High or Critical Vulnerabilities	106
Change in Critical Perimeter Attacks	359
Non Baselined Discovered System	152
Notable Event Alert: Vulnerability exposure from Threat Intelligence	2
Change in Systems Performance	63
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	15
Change in Systems Availability	14
Monitoring for open ports	1

Durante julio, Change in Critical Perimeter Attacks y Non Baselined Discovered System continuaron siendo los principales indicadores de actividad, con 359 y 152 eventos, respectivamente, aunque ambos presentaron una disminución frente al período anterior. La exposición de servicios y el seguimiento de activos descubiertos se mantienen como áreas relevantes de monitoreo.

También se observó una reducción en los eventos relacionados con vulnerabilidades críticas o altas, registrándose 106 eventos de Change in External High or Critical Vulnerabilities y 15 de Change in Internal High or Critical Vulnerabilities for IT, IoT and OT. De igual forma, High Persistency Detection disminuyó a 39 eventos, mientras que los cambios en disponibilidad y rendimiento de los sistemas se redujeron a 14 y 63 eventos, respectivamente.

En términos generales, julio presenta una reducción en la actividad operacional respecto a junio, manteniendo patrones similares de concentración en actividad perimetral, descubrimiento de activos y gestión de vulnerabilidades. Se recomienda continuar el seguimiento de estos indicadores con el objetivo de identificar cambios relevantes o incrementos sostenidos en su comportamiento.

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