TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

July 28, 2026

Organo Judicial 07/28/2026

TLP AMBER CISO
EXECUTIVE REPORT

Este informe corresponde "Marzo 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

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

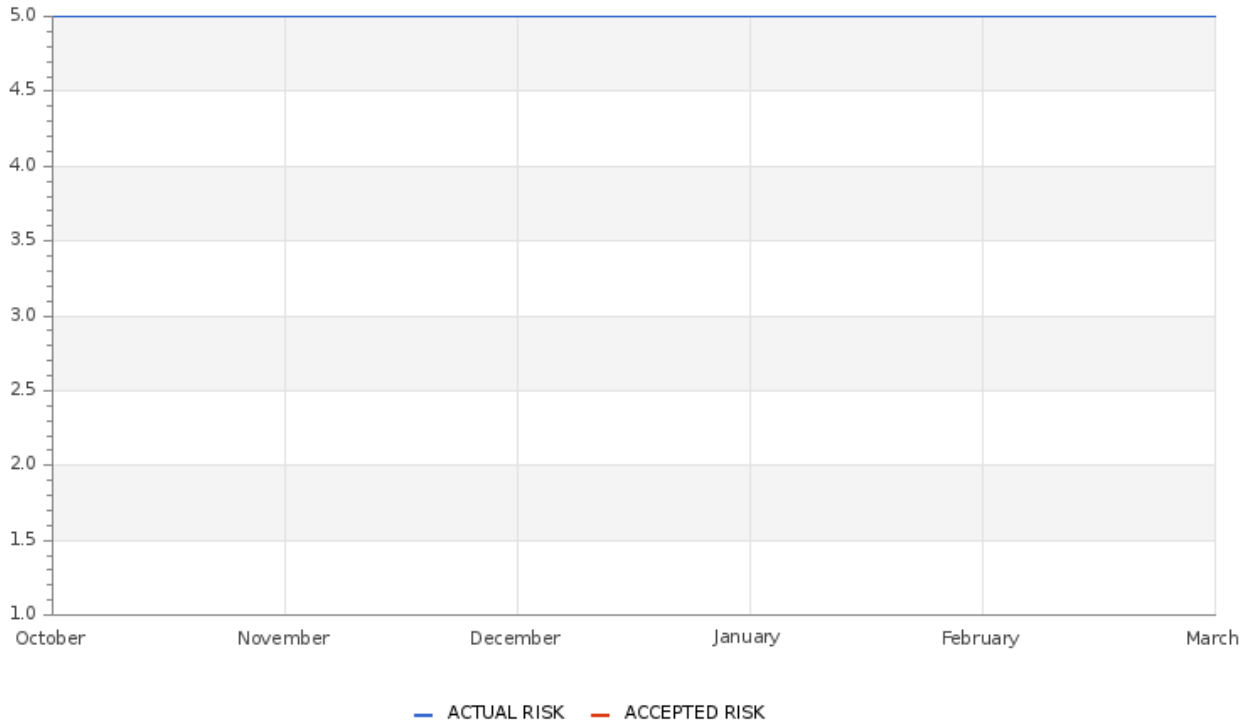
Low

La confiabilidad de la evaluación sigue siendo limitada debido a la insuficiencia y falta de consistencia 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.

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

Organo Judicial 07/28/2026

Accepted & Actual Risk



Riesgo Actual (5%) Durante el periodo analizado, el nivel de riesgo actual se mantuvo estable en comparación con el mes anterior. El valor del 5% se encuentra dentro de un rango bajo, indicando que la exposición a incidentes potenciales sigue controlada y que las medidas de seguridad implementadas continúan siendo efectivas. No obstante, es esencial mantener una vigilancia constante y una capacidad de respuesta adecuada para prevenir posibles incrementos futuros.

Riesgo Tolerado (1%) El riesgo tolerado se mantuvo en 1%, reflejando una gestión conservadora y consistente del riesgo residual. Este comportamiento demuestra la correcta aplicación de controles preventivos y la priorización de acciones de mitigación frente a posibles exposiciones, manteniendo el nivel de riesgo dentro de parámetros aceptables.

Organo Judicial 07/28/2026

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

	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	1	1

Nivel Actual de Riesgo (5%):
Durante este mes, el porcentaje de riesgo detectado en tiempo real se mantuvo en 5%, igual que el mes anterior. Esto indica que la exposición frente a amenazas activas se ha estabilizado, manteniendo la postura de seguridad sin incrementos en el nivel de riesgo. Aun así, es fundamental continuar con el monitoreo constante y la aplicación de controles adecuados para evitar posibles variaciones que puedan afectar la seguridad de la organización.

Riesgo Permitido (1%): La organización mantiene un umbral de riesgo aceptable de 1%, sin cambios respecto al periodo anterior. Este valor refleja un enfoque altamente conservador en la gestión del riesgo, priorizando la mitigación y el control continuo para mantener el nivel de riesgo dentro de los parámetros definidos.

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months

Durante el mes de marzo se evaluaron 4,223 activos internos y 61 activos expuestos a Internet. Del total de activos internos, 2,032 (48.1 %) presentaron al menos una vulnerabilidad, lo que refleja una superficie de exposición significativa dentro de la red corporativa y resalta la importancia de fortalecer las actividades de gestión de vulnerabilidades y aplicación de parches. En el caso de los activos externos, 11 de los 61 evaluados (18.0 %) presentaron vulnerabilidades. Aunque la proporción es considerablemente menor que la observada en el entorno interno, estos activos representan un mayor nivel de riesgo debido a su exposición directa a Internet, por lo que su remediación debe mantenerse como una prioridad.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	5.13.46.200.dialup.psinetpa.net	0
Current	20	

Durante el período analizado se identificaron vulnerabilidades asociadas al activo 5.13.46.200.dialup.psinetpa.net, registrándose un total de 20 hallazgos, en comparación con la ausencia de vulnerabilidades reportadas durante el período anterior.

La variación observada evidencia cambios en la superficie de exposición del activo evaluado y resalta la importancia de mantener procesos continuos de identificación, evaluación y remediación de vulnerabilidades. La detección oportuna de estos hallazgos permite priorizar acciones correctivas orientadas a reducir riesgos potenciales y fortalecer la postura de seguridad de los servicios expuestos.

El monitoreo continuo de vulnerabilidades constituye un componente fundamental de la gestión del riesgo cibernético, proporcionando visibilidad sobre posibles exposiciones y contribuyendo a la protección de los activos institucionales, la resiliencia tecnológica y la continuidad de los servicios críticos de la organización.

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

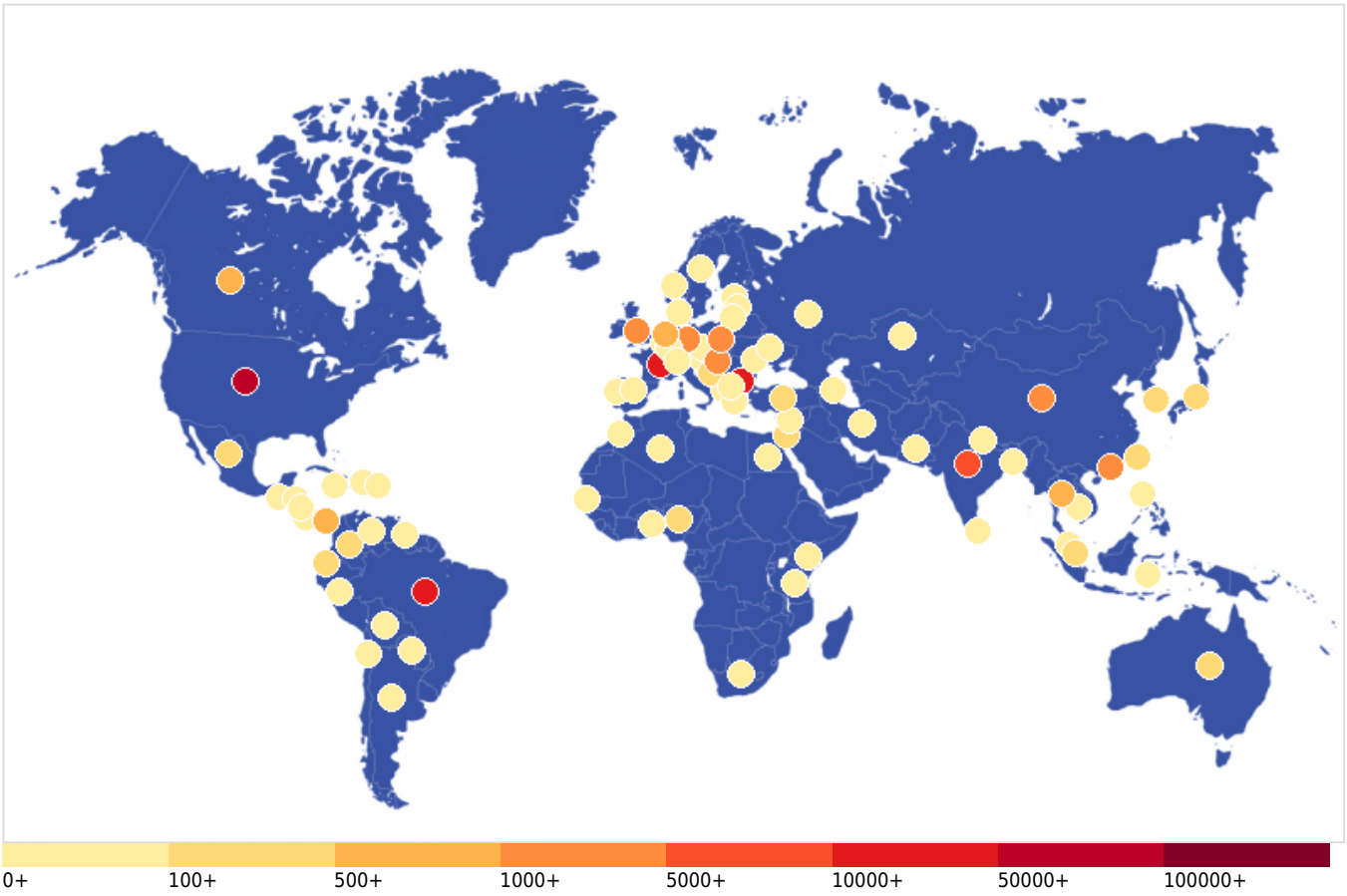
Organo Judicial 07/28/2026

Vulnerability Metric

12

THREATS

Critical Attacks Per Country In Past Week



Albania - 59
Algeria - 21
Argentina - 99
Australia - 306
Austria - 3
Azerbaijan - 3
Bangladesh - 42
Belgium - 3
Bolivia - 53
Bosnia and Herzegovina - 305
Botswana - 9
Brazil - 23882
Bulgaria - 10441
Cambodia - 6
Canada - 520
Chile - 45
China - 2283
Colombia - 209
Costa Rica - 12
Czechia - 3
Denmark - 3
Dominican Republic - 6
Ecuador - 111
Egypt - 6
Estonia - 3
France - 26089
Germany - 1080
Greece - 3
Guatemala - 12
Guyana - 3
Honduras - 15
Hong Kong - 2100
Hungary - 1113
India - 9769
Indonesia - 69
Israel - 210

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

Organo Judicial 07/28/2026

Jamaica - 12
Kenya - 9
Luxembourg - 87
Moldova - 3
New Zealand - 3
Norway - 66
Peru - 12
Puerto Rico - 6
Seychelles - 3
Spain - 16
Taiwan - 116
Turkey - 411
Venezuela - 66
Japan - 437
Latvia - 12
Malaysia - 6
Morocco - 6
Nicaragua - 9
Pakistan - 81
Philippines - 12
Russia - 61
Singapore - 101
Sri Lanka - 25
Tanzania - 15
Ukraine - 24
Jordan - 3
Lebanon - 15
Mauritius - 9
Nepal - 3
Nigeria - 258
Panama - 720
Poland - 1374
Saint Kitts and Nevis - 3
South Africa - 12
Sweden - 32
Thailand - 606
United Kingdom - 3383
Kazakhstan - 34
Lithuania - 6
Mexico - 462
Netherlands - 808
North Macedonia - 3
Paraguay - 15
Portugal - 3
Senegal - 9
South Korea - 196
Switzerland - 21
Togo - 3
United States - 66821

La gráfica correspondiente al período analizado muestra una distribución global de ataques críticos, con una marcada concentración de eventos provenientes de múltiples regiones, destacándose América del Norte, Europa, Asia y Sudamérica como las zonas más activas.

Estados Unidos se mantiene como la principal fuente de actividad, con 66,821 eventos registrados, seguido por Francia (26,089), Brasil (23,882), Bulgaria (10,441) e India (9,769), los cuales representan los volúmenes más significativos dentro del conjunto analizado.

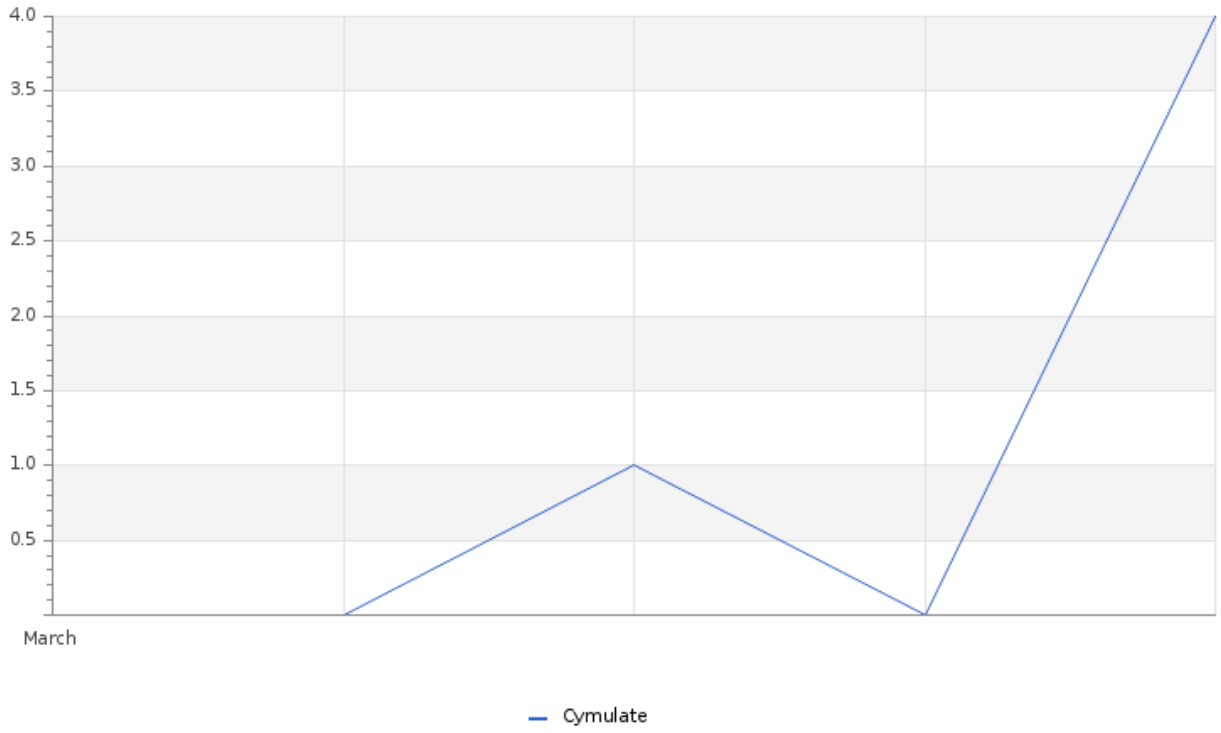
En un segundo nivel se identifican países con una actividad relevante como Reino Unido (3,383), Alemania (1,080), Polonia (1,374), Hong Kong (2,100), Países Bajos (808), Panamá (720), Tailandia (606), Canadá (520), México (462), Turquía (411) y Australia (306), evidenciando una distribución intermedia de eventos asociados a la actividad maliciosa observada.

Adicionalmente, se registran múltiples países con volúmenes menores pero constantes, incluyendo China (2,283), India (9,769), Argentina (99), Colombia (209), Japón (437), Rusia (61), Sudáfrica (12), entre otros, lo que refuerza la naturaleza ampliamente distribuida de las fuentes de ataque a nivel global.

La distribución observada refleja el carácter global de las amenazas que afectan a los servicios expuestos a Internet y pone de manifiesto la utilización de infraestructuras tecnológicas distribuidas para la ejecución de actividades maliciosas. Este comportamiento resalta la importancia de mantener capacidades de monitoreo continuo, inteligencia de amenazas y controles de seguridad que permitan identificar oportunamente cambios en los patrones de ataque y fortalecer la protección de los activos institucionales.

Organo Judicial 07/28/2026

Total Number of Successful MFA authentications per application

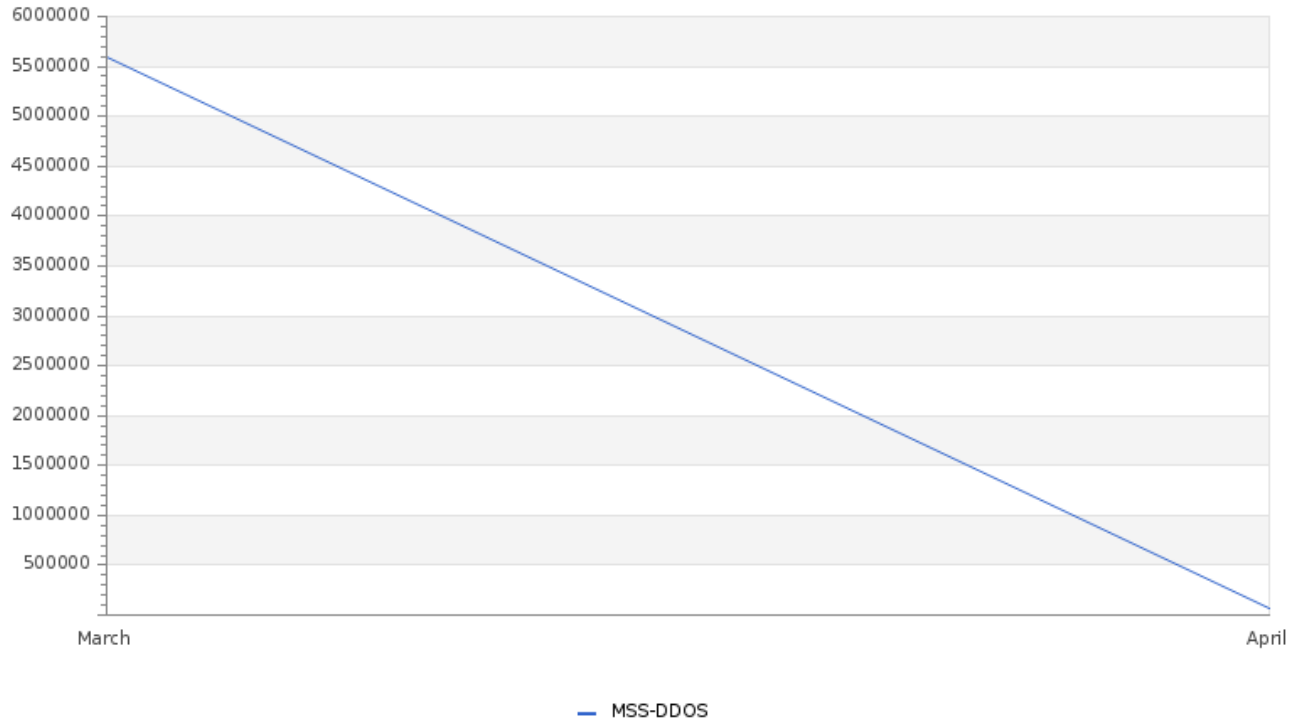


Durante el período analizado se observó un incremento gradual en la cantidad de autenticaciones MFA exitosas realizadas por los usuarios sobre la aplicación protegida. Este comportamiento evidencia un mayor uso del servicio y confirma el correcto funcionamiento del mecanismo de autenticación multifactor, garantizando que los accesos autorizados se realicen mediante un segundo factor de verificación, fortaleciendo así la seguridad del proceso de autenticación.

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

Organo Judicial 07/28/2026

Total Attacks Successfully Blocked Per Service

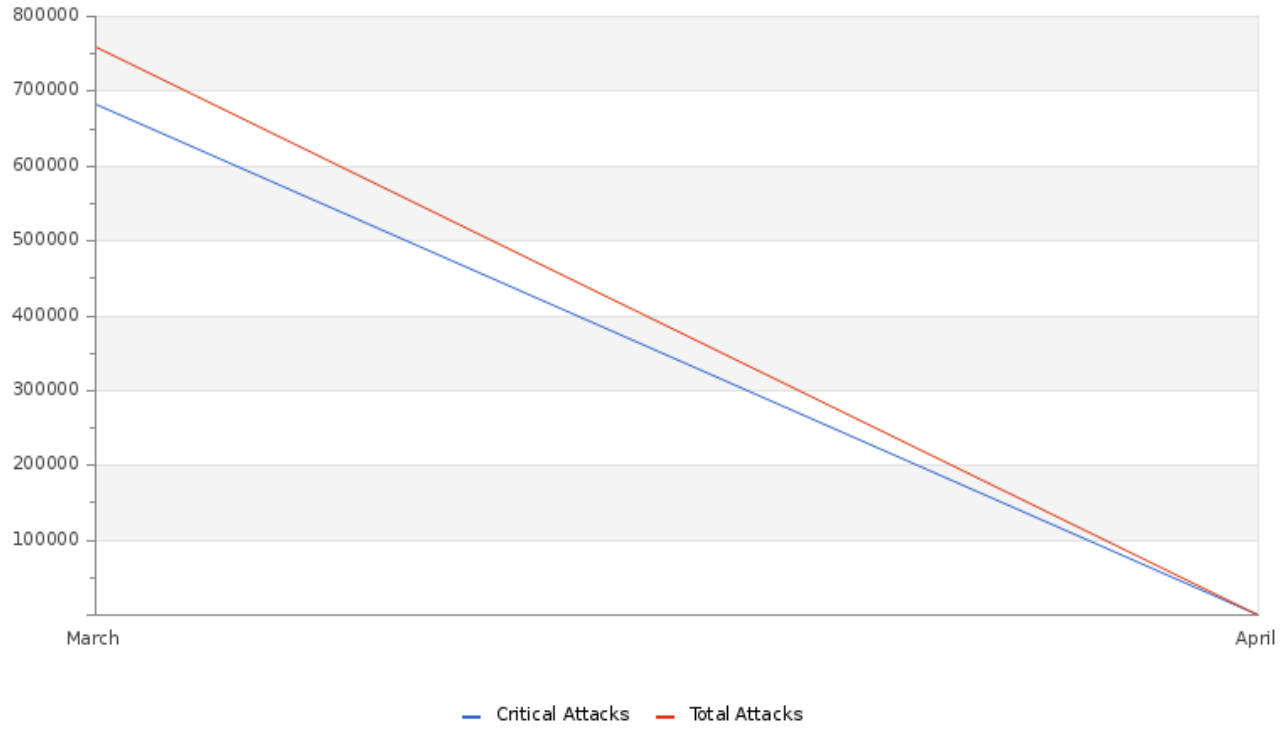


Durante el mes de marzo se registraron un total de 5,765,907 intentos de ataques de denegación de servicio distribuido (DDoS) dirigidos a la infraestructura protegida. De este total, 3,780,043 eventos fueron clasificados como ataques críticos, lo que representa aproximadamente el 65.6 % de la actividad observada. Los mecanismos de protección del servicio MSS-DDoS mitigaron exitosamente estos intentos, evidenciando un volumen elevado y sostenido de actividad maliciosa dirigida a afectar la disponibilidad de los servicios expuestos, así como la efectividad de las capacidades de detección y mitigación implementadas.

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

Organo Judicial 07/28/2026

Attacks Successfully Blocked by Severity



Durante el mes de marzo se registraron 3,780,043 ataques clasificados como críticos, representando aproximadamente el 65.6 % del total de 5,765,907 ataques bloqueados por el servicio MSS-DDoS. Esta proporción evidencia que una parte importante de la actividad maliciosa correspondió a intentos de alto impacto dirigidos a afectar la disponibilidad de los servicios expuestos. La mitigación exitosa de estos eventos confirma la efectividad de los mecanismos de protección implementados para identificar y bloquear amenazas críticas antes de que afectaran la operación de la infraestructura.

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

Organo Judicial 07/28/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	17	3
Critical Device Outages	0	0

La actividad de ataques bloqueados durante el período analizado evidencia la presencia continua de amenazas dirigidas a la organización, observándose una proporción significativa de eventos clasificados como críticos dentro del total de ataques mitigados.

Las capacidades de detección y protección implementadas permitieron contener eficazmente los eventos identificados, evitando que estos generen afectaciones sobre los servicios y activos tecnológicos de la organización. La gestión oportuna de los ataques registrados demuestra la efectividad de los controles de seguridad actualmente desplegados para enfrentar amenazas de distintos niveles de severidad.

Este comportamiento resalta la importancia de continuar fortaleciendo las capacidades de monitoreo, detección y respuesta ante incidentes, permitiendo identificar tendencias en el panorama de amenazas, mitigar riesgos potenciales y respaldar la protección de los activos críticos y la continuidad operativa de la organización

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

Organo Judicial 07/28/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
www.organojudicial.gob.pa	HTTP	200.46.13.0/26	Down, Warning		435	2026-03-09 11:30:46	2026-03-23 22:12:25
Plataforma Moodle Escuela Judicial	HTTP Advanced	Web Servers	Down, Warning		50	2026-03-10 18:09:19	2026-03-29 00:18:59
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		33	2026-03-10 18:29:21	2026-03-31 21:39:27
Repositorio digital	HTTP Advanced	Web Servers	Down, Warning		29	2026-03-10 18:09:19	2026-03-18 06:45:11
Plataforma de correo	HTTP Advanced	Web Servers	Down		27	2026-03-05 00:24:52	2026-03-23 22:12:25
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		25	2026-03-10 18:24:21	2026-03-20 00:35:00
Probe Device	System Health	Organo Judicial	Warning		23	2026-03-14 03:03:39	2026-03-31 03:03:40
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		20	2026-03-10 18:14:20	2026-03-18 06:45:11
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Down, Warning		15	2026-03-22 03:35:53	2026-03-30 13:16:20
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		15	2026-03-10 18:24:21	2026-03-18 06:45:11
Gestor Documental	HTTP Advanced	Web Servers	Down, Warning		14	2026-03-10 18:19:20	2026-03-13 13:32:03
Probe Device	System Health	Organo Judicial C-GMSA	Warning		5	2026-03-10 03:02:35	2026-03-12 03:03:05
GMSA-OJ HyperV	HTTP	GMSA-OJ	Down, Warning		4	2026-03-30 13:16:36	2026-03-30 13:16:36
DevConsejo de Administración de la Carrera Judicial ice	HTTP Advanced	Web Servers	Down, Warning		4	2026-03-30 13:16:31	2026-03-30 13:16:31
Sistema Integral de Gestión de Recursos Humanos	HTTP Advanced	Web Servers	Down, Warning		4	2026-03-17 13:38:13	2026-03-30 13:16:08

Durante el período evaluado, el servicio de monitoreo externo identificó eventos de indisponibilidad y degradación en varios servicios publicados, siendo el sitio www.organojudicial.gob.pa el que registró la mayor cantidad de incidencias (435 eventos). También se observaron eventos recurrentes en plataformas como Moodle, el Sistema Automatizado de Gestión Judicial, el Repositorio Digital y la Plataforma de Correo. Estos resultados evidencian la importancia del monitoreo continuo para detectar oportunamente interrupciones en los servicios expuestos, permitiendo su validación y atención antes de que impacten significativamente la disponibilidad percibida por los usuarios.

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

Organo Judicial 07/28/2026

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	1,166,463	0	977	0

Durante el período analizado, las diferentes capas de seguridad implementadas en la organización contribuyeron a la detección y mitigación de eventos de seguridad dirigidos tanto al perímetro como a los endpoints. La actividad observada confirma la importancia de mantener un enfoque de defensa en profundidad, donde cada servicio cumple un rol específico en la identificación, prevención y contención de amenazas, fortaleciendo la postura de seguridad de la organización.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	320
Change in Systems Availability	137
Change in High or Critical Vulnerabilities	3
Non Baselined Discovered System	1353
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	98
Change in External High or Critical Vulnerabilities	140
Notable Event Alert: Endpoint Configuration Management High Priority Event	6
Monitoring for open ports	26
Change in Critical Perimeter Attacks	674
High Persistency Detection	150
Threat Intelligence Validation	5
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8
Notable Event Alert: Vulnerability exposure from Threat Intelligence	2

Durante el período analizado se registró actividad relevante asociada a cambios en la postura de seguridad, la disponibilidad y el rendimiento de la infraestructura tecnológica. El principal hallazgo correspondió a la detección de 1,076 eventos de “Non Baselined Discovered System”, evidenciando la incorporación o identificación de activos que no forman parte de la línea base de inventario y que requieren validación. Asimismo, se identificaron 364 cambios relacionados con ataques perimetrales críticos y 102 asociados a vulnerabilidades externas críticas. En el entorno interno se registraron 24 vulnerabilidades críticas y 3 de alta severidad, lo que confirma la existencia de una superficie de ataque que requiere seguimiento y remediación continua. Desde el punto de vista operativo, se observaron 220 eventos relacionados con el rendimiento y 97 asociados a la disponibilidad de los servicios, sin evidenciar interrupciones críticas sostenidas durante el período evaluado.

Organo Judicial 07/28/2026

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.**

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