TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

June 13, 2026

Organo Judicial 06/13/2026

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

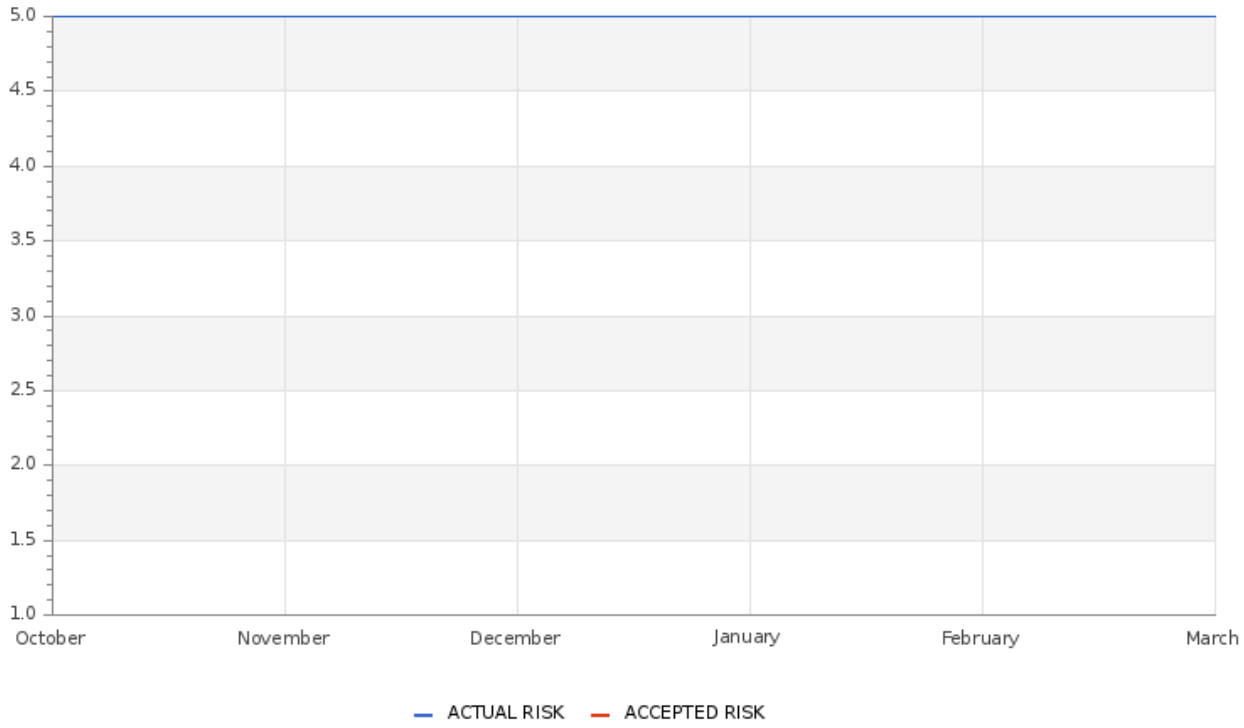
Low

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 06/13/2026

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 06/13/2026

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

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.

Vulnerability Metric

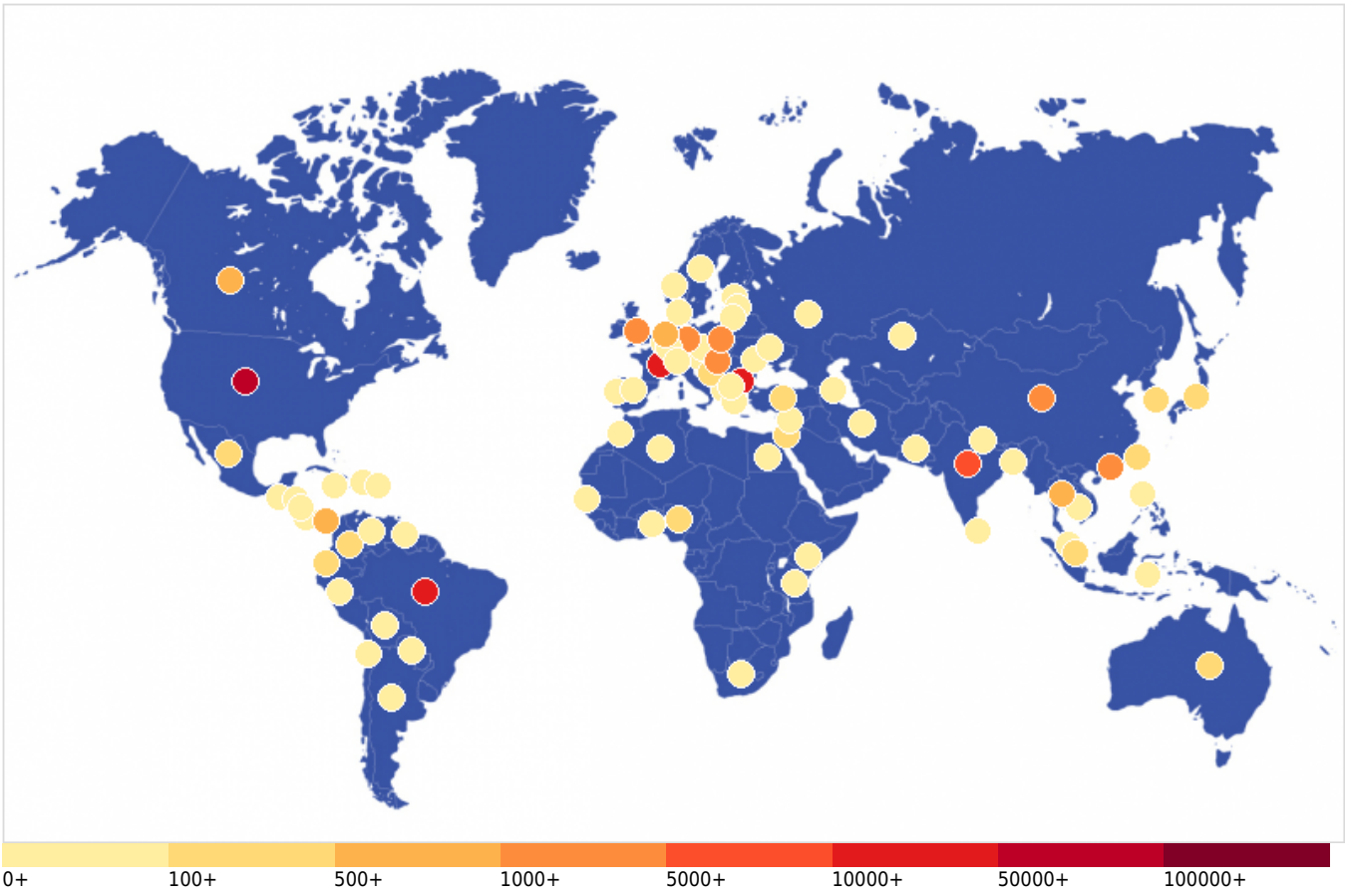
12

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

Organo Judicial 06/13/2026

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
Jamaica - 12
Japan - 437
Jordan - 3
Kazakhstan - 34
Kenya - 9
Latvia - 12
Lebanon - 15
Lithuania - 6
Luxembourg - 87
Malaysia - 6
Mauritius - 9
Mexico - 462
Moldova - 3
Morocco - 6
Nepal - 3
Netherlands - 808
New Zealand - 3
Nicaragua - 9
Nigeria - 258
North Macedonia - 3
Norway - 66
Pakistan - 81
Panama - 720
Paraguay - 15
Peru - 12
Philippines - 12
Poland - 1374
Portugal - 3
Puerto Rico - 6
Russia - 61
Saint Kitts and Nevis - 3
Senegal - 9
Seychelles - 3
Singapore - 101
South Africa - 12
South Korea - 196

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

Organo Judicial 06/13/2026

Spain - 16
Taiwan - 116
Turkey - 411
Venezuela - 66
Sri Lanka - 25
Tanzania - 15
Ukraine - 24
Sweden - 32
Thailand - 606
United Kingdom - 3383
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.

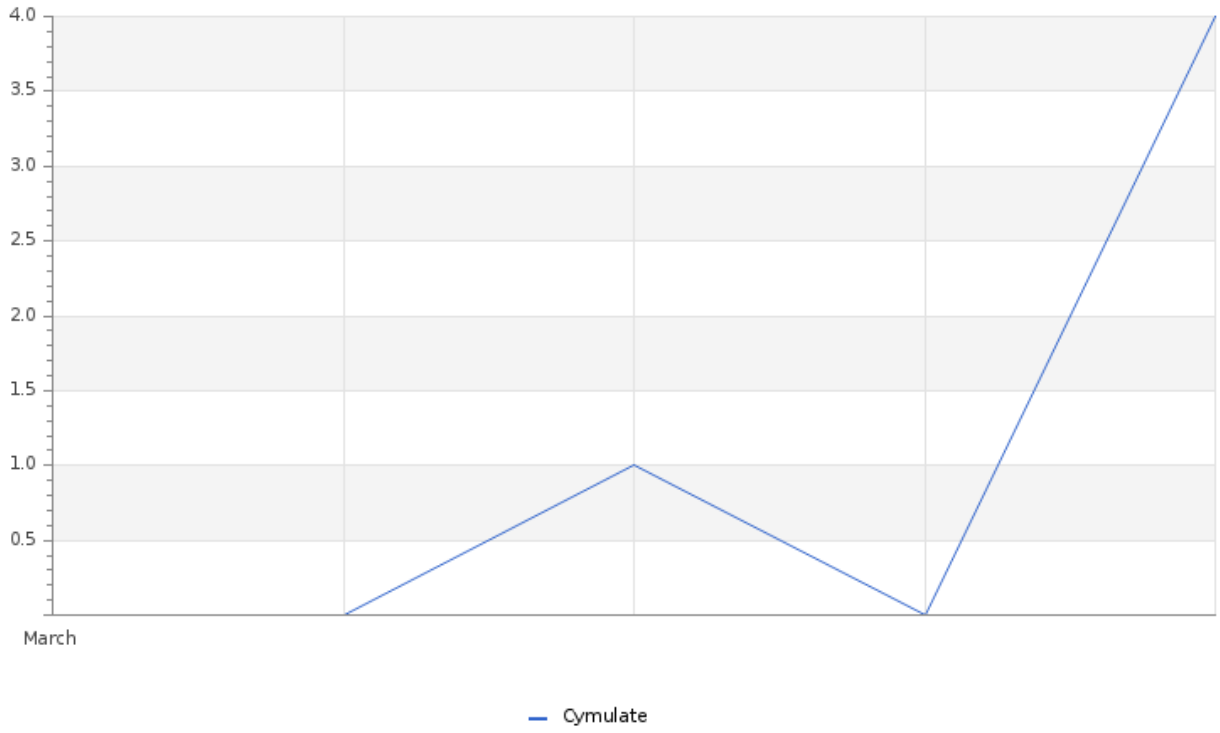
En un segundo nivel se identifican países con una actividad relevante como Reino Unido (3,383), Alemania (1,080), Polonia (1,374), Hong Kong (2,100), Países Bajos (808), Panamá (720), Tailandia (606), Canadá (520), México (462), Turquía (411) y Australia (306), evidenciando una distribución intermedia 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 06/13/2026

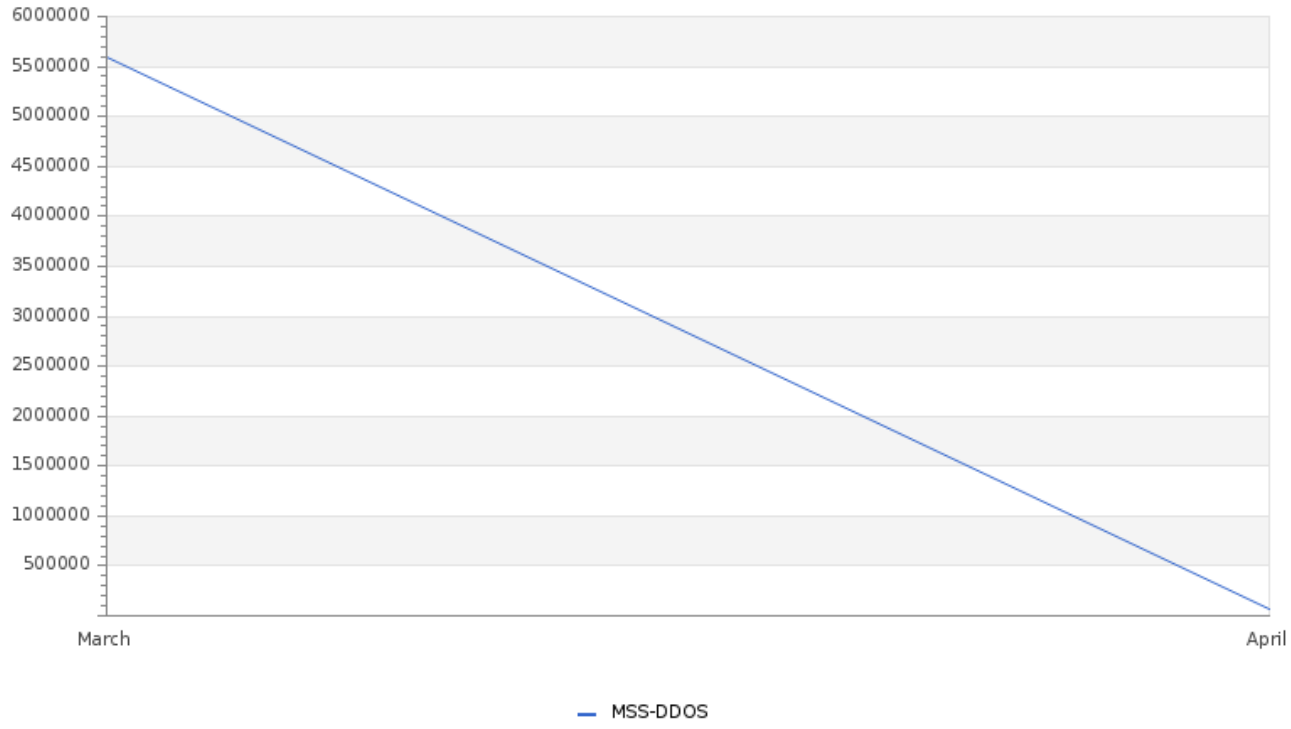
Total Number of Successful MFA authentications per application



Total Attacks Successfully Blocked Per Service

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

Organo Judicial 06/13/2026



Durante el mes de marzo , se registró una actividad significativa asociada a intentos de ataques de denegación de servicio distribuido (DDoS) dirigidos a la organización. De acuerdo con la información observada, los mecanismos de protección lograron bloquear aproximadamente 5.5 millones de ataques , evidenciando un alto volumen de amenazas orientadas a afectar la disponibilidad de los servicios expuestos.

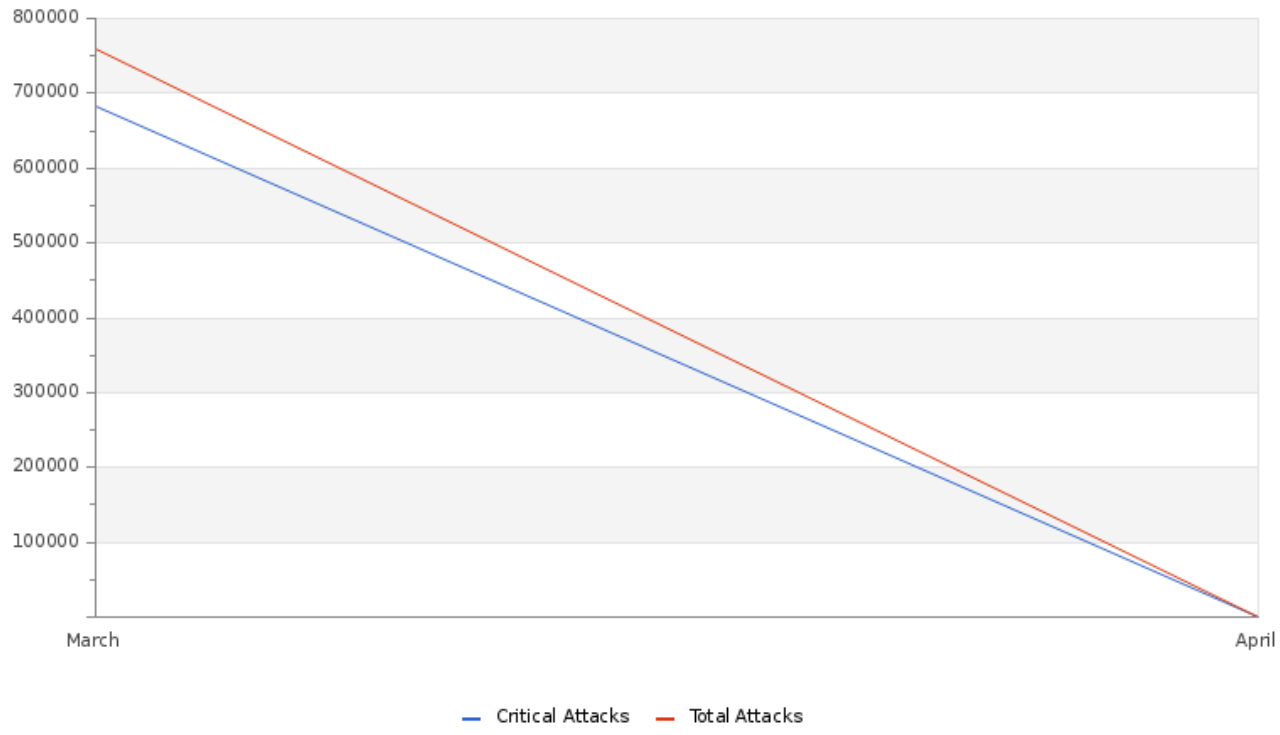
Las capacidades de seguridad implementadas permitieron identificar y mitigar de manera efectiva los eventos detectados, evitando posibles interrupciones en la operación y garantizando la continuidad de los servicios institucionales. Los resultados obtenidos durante el período reflejan la efectividad de las soluciones de protección y de los controles especializados desplegados para enfrentar este tipo de amenazas.

La actividad registrada durante marzo resalta la importancia de mantener herramientas avanzadas de monitoreo, detección y mitigación de ataques DDoS, así como procesos de respuesta oportunas que permitan reducir el impacto de incidentes que puedan comprometer la disponibilidad de los recursos tecnológicos. Estas capacidades fortalecen la resiliencia operativa de la organización y contribuyen a asegurar la continuidad de sus servicios críticos.

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

Organo Judicial 06/13/2026

Attacks Successfully Blocked by Severity



La gráfica correspondiente al mes de marzo evidencia una actividad relevante de amenazas dirigidas a la organización, observándose una proporción significativa de eventos clasificados como críticos dentro del total de ataques bloqueados. Este comportamiento confirma la persistencia de amenazas con potencial impacto sobre la disponibilidad y seguridad de los servicios institucionales.

Los controles de seguridad implementados permitieron detectar y bloquear eficazmente los eventos identificados durante el período, contribuyendo a reducir la exposición al riesgo y fortaleciendo la protección de los activos tecnológicos. La capacidad de respuesta demostrada refleja la efectividad de las medidas de seguridad actualmente desplegadas para la gestión de amenazas de diferentes niveles de severidad.

Los resultados observados resaltan la importancia de mantener capacidades de monitoreo continuo, detección temprana y respuesta oportuna, permitiendo preservar la continuidad operativa y reforzar la postura de ciberseguridad de la organización frente a un entorno de amenazas en constante evolución.

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

Organo Judicial 06/13/2026

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

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

Organo Judicial 06/13/2026

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
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

La disponibilidad de los servicios tecnológicos de la organización se mantuvo en niveles operativos durante el período analizado, a pesar de la ocurrencia de múltiples eventos de indisponibilidad y advertencia en distintos componentes de la infraestructura institucional. No se identificaron afectaciones de criticidad alta que comprometieran de forma sostenida la continuidad de los servicios esenciales.

El activo con mayor número de eventos fue www.organojudicial.gob.pa, con 435 eventos en estado “Down” y “Warning”, concentrando la mayor proporción de las incidencias registradas. Asimismo, se observaron eventos relevantes en plataformas institucionales como la Plataforma Moodle de la Escuela Judicial (50 eventos), el Sistema Automatizado de Gestión Judicial (33 eventos), el Repositorio Digital (29 eventos) y la Plataforma de Correo Institucional (27 eventos).

De igual forma, se identificaron incidencias en otros servicios de soporte y gestión, incluyendo el Reporte Biométrico (25 eventos), la Consulta de Fallos (20 eventos), la Plataforma de Gestión de Pleno (15 eventos) y el Gestor Documental (14 eventos), así como eventos en componentes de infraestructura y monitoreo como Probe Device y entornos GMSA, asociados principalmente a estados de advertencia e indisponibilidad intermitente.

En términos generales, los eventos reflejan afectaciones recurrentes de baja a moderada severidad, principalmente asociadas a indisponibilidades temporales y condiciones de inestabilidad operacional, sin impacto crítico prolongado sobre los servicios institucionales.

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 capas de seguridad de la organización registraron la detección y bloqueo de un volumen significativo de intentos de ataque, lo cual evidencia la exposición continua de los servicios institucionales a actividades maliciosas y la efectividad de los controles implementados a nivel de protección perimetral y endpoints.

La mayor concentración de eventos se presentó en la capa MSS-DDoS, con un total de 1,166,463 intentos bloqueados, reflejando una actividad sostenida de ataques orientados a la interrupción o degradación de la disponibilidad de los servicios. En segundo lugar, la capa MSS-EDR registró 977 eventos bloqueados, asociados a detección de actividad maliciosa a nivel de endpoint.

Las demás capas de seguridad, incluyendo MSS-UTM, MSS-BOT, MSS-DLP y MSS-WAF, no reportaron eventos durante el período analizado, lo que indica ausencia de actividad registrada en dichos vectores o la no detección de intentos en esas superficies específicas.

En términos generales, los resultados evidencian una presión relevante sobre los mecanismos de mitigación DDoS, mientras que el resto de los controles mantuvo un comportamiento estable. Este escenario refuerza la importancia de continuar fortaleciendo las capacidades de monitoreo, correlación de eventos y protección de la disponibilidad de los servicios críticos, a fin de garantizar la resiliencia operativa frente a intentos de ataque y preservar la continuidad de los servicios institucionales.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	220
Change in Systems Availability	97
Change in High or Critical Vulnerabilities	3
Non Baselined Discovered System	1076
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	24
Change in External High or Critical Vulnerabilities	102
Notable Event Alert: Endpoint Configuration Management High Priority Event	6
Monitoring for open ports	26
Change in Critical Perimeter Attacks	364
High Persistency Detection	72
Threat Intelligence Validation	5
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

Durante el período analizado se registró un volumen relevante de eventos operacionales asociados a cambios en la disponibilidad, rendimiento y postura de seguridad del entorno tecnológico.

El principal hallazgo corresponde a “Non Baselined Discovered System”, con 1,076 eventos, evidenciando la detección de activos no inventariados previamente, lo cual requiere fortalecimiento del control de la línea base.

Asimismo, se observaron 364 eventos de cambios en ataques perimetrales críticos y 102 cambios en vulnerabilidades externas críticas, junto con 24 vulnerabilidades internas críticas y 3 de alta criticidad, lo que refleja exposición activa de la superficie de ataque.

En el ámbito operativo, se identificaron 220 eventos de rendimiento y 97 de disponibilidad, sin afectaciones críticas sostenidas en los servicios.

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.**

Organo Judicial 06/13/2026

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