TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

March 20, 2026

Organo Judicial 03/20/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "FEBRERO 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 in enfoque prudente en la aceptación del riesgo, dando prioridad a las acciones de mitigación y control frente a eventuales escenarios de exposición.

Confidence

Medium

La confiabilidad de la evaluación continúa siendo baja como consecuencia de la insuficiencia o inconsistencia 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.

Accepted & Actual Risk

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

Organo Judicial 03/20/2026

Riesgo Actual:
Durante el periodo analizado, el nivel de riesgo se mantiene estable respecto al mes anterior, con un valor de 5%, categorizado dentro del rango bajo según los parámetros de referencia establecidos. Este resultado confirma que la exposición a incidentes potenciales permanece bajo control y que los controles de seguridad vigentes mantienen su efectividad operacional. Aun así, se considera crítico sostener un esquema de monitoreo continuo, acompañado de una capacidad de respuesta inmediata, para anticipar desviaciones y prevenir incrementos no planificados en el nivel de riesgo.

Riesgo Aceptado:
El riesgo aceptado se mantiene en 1%, reflejando una estrategia de gestión conservadora y consistente frente al riesgo residual. Este indicador evidencia la correcta implementación de controles preventivos y la priorización de acciones de mitigación, garantizando que la exposición permanezca dentro de los umbrales definidos como aceptables por la organización. La estabilidad de este valor respalda la solidez del marco de gestión de riesgos y la alineación con las políticas corporativas de seguridad.

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

Organo Judicial 03/20/2026

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

	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	1	0

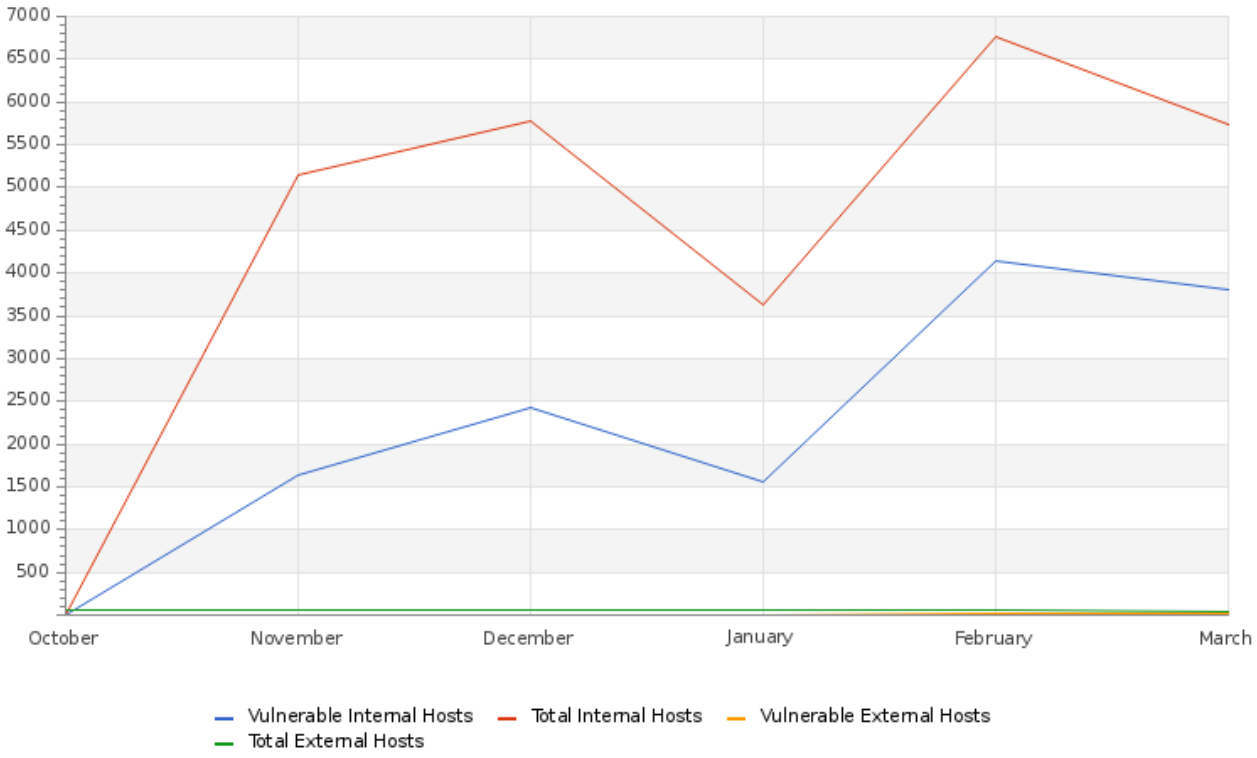
Nivel Actual de Riesgo (5%):
Durante el mes analizado, el nivel de riesgo actual se mantuvo en 5%, sin variaciones respecto al mes anterior. Este comportamiento refleja una estabilidad en la exposición a amenazas, indicando que las condiciones de riesgo no han presentado incrementos. No obstante, es importante continuar con el monitoreo constante y la validación de controles de seguridad para prevenir posibles fluctuaciones que puedan impactar la postura de seguridad.

Accepted Risk (1%):
En cuanto al riesgo aceptado, se observa un incremento de 0% a 1% en comparación con el periodo anterior. Este cambio sugiere un ligero ajuste en el umbral de tolerancia al riesgo, posiblemente asociado a decisiones estratégicas o a la evaluación de riesgos que han sido considerados controlados o mitigables. A pesar de este aumento, el nivel se mantiene bajo, por lo que es recomendable continuar con el seguimiento y la revisión periódica para asegurar que no se incrementen los niveles de exposición.

VULNERABILITY

Organo Judicial 03/20/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de febrero, el total de 6,750 hosts activos se mantuvo estable respecto al período anterior, sin variaciones en la infraestructura registrada. No obstante, se identificaron cambios en el número de hosts vulnerables, vinculados principalmente a la cantidad de equipos incorporados en el período. Este comportamiento confirma que las medidas de seguridad implementadas mantienen su efectividad en la gestión de riesgos, incluso en escenarios de estabilidad en el volumen de activos administrados.

La estabilidad en la infraestructura no debe interpretarse como ausencia de riesgo. Es esencial sostener una supervisión continua y una gestión proactiva de la seguridad, con el objetivo de evitar que la invariabilidad en los activos genere una percepción errónea de control. Se recomienda reforzar los procesos de monitoreo, evaluación periódica de vulnerabilidades y respuesta temprana, asegurando que posibles riesgos latentes sean identificados y mitigados oportunamente.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	190.34.182.227	2
Current	2	

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

Organo Judicial 03/20/2026

Vulnerability Metric

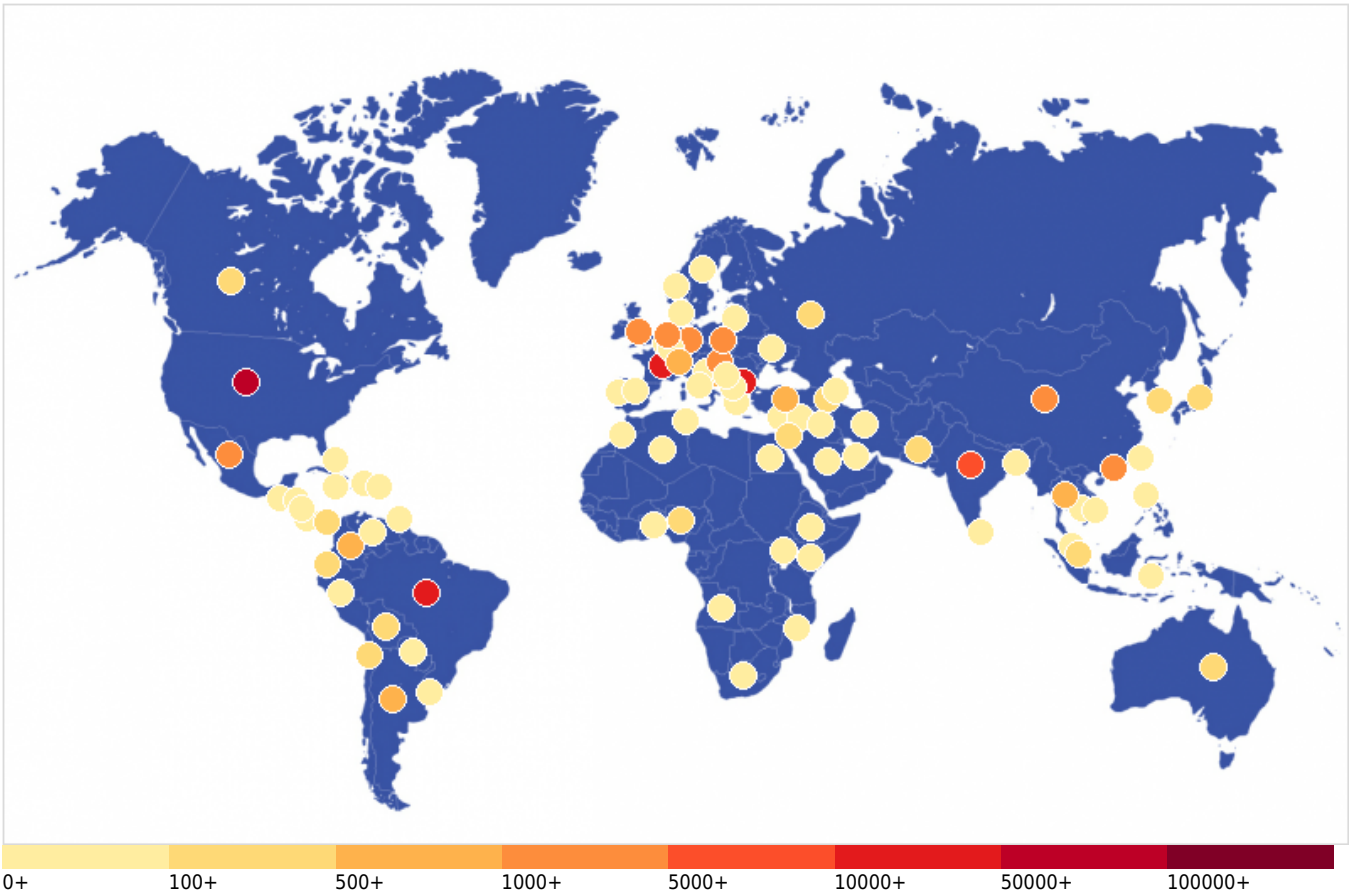
13

Durante el mes de diciembre, se detectaron 876 host de estado crítico, 6309 host de vulnerabilidad alta, 3285 de vulnerabilidad media y 5372 de vulnerabilidad baja, lo que nos indica que la métrica de vulnerabilidad de la organización es 13%.

La distribución evidencia que, aunque la mayoría de los activos se concentran en niveles de riesgo bajo y medio, existe un volumen relevante de hosts críticos y de alta vulnerabilidad que requieren atención prioritaria. La métrica global del 13% refleja un nivel de exposición que, si bien está dentro de parámetros manejables, demanda una gestión proactiva de remediación para evitar que las vulnerabilidades críticas se traduzcan en incidentes de seguridad.

THREATS

Critical Attacks Per Country In Past Week



Algeria - 23
Angola - 6
Argentina - 531
Armenia - 135
Australia - 363
Azerbaijan - 30
Bahamas - 3
Bangladesh - 30
Belgium - 29
Bolivia - 114
Bosnia and Herzegovina - 607
Botswana - 24
Brazil - 20280
Bulgaria - 11053
Cambodia - 30
Canada - 253

Organo Judicial 03/20/2026

Chile - 183
China - 2315
Colombia - 500
Costa Rica - 45
Croatia - 3
Cyprus - 8
Denmark - 12
Dominican Republic - 3
Ecuador - 402
Egypt - 6
Ethiopia - 3
France - 26922
Georgia - 3
Germany - 1423
Greece - 3
Guatemala - 24
Honduras - 12
Hong Kong - 2418
Hungary - 2057
India - 9810
Indonesia - 15
Iraq - 30
Israel - 189
Italy - 3
Jamaica - 16
Japan - 437
Jordan - 9
Kenya - 12
Lithuania - 11
Luxembourg - 69
Malaysia - 21
Mauritius - 15
Mexico - 1403
Morocco - 3
Mozambique - 11
Netherlands - 1366
New Zealand - 3
Nicaragua - 21
Nigeria - 262
North Macedonia - 9
Norway - 68
Pakistan - 126
Panama - 111
Paraguay - 96
Peru - 46
Philippines - 3
Poland - 1301
Portugal - 3
Puerto Rico - 15
Qatar - 3
Russia - 142
Saint Kitts and Nevis - 537
Saudi Arabia - 3
Serbia - 11
Singapore - 444
South Africa - 15
South Korea - 213
Spain - 9
Sri Lanka - 8
Sweden - 15
Switzerland - 656
Taiwan - 58
Thailand - 759
Togo - 6
Trinidad and Tobago - 24
Tunisia - 3
Turkey - 553
Uganda - 32
Ukraine - 69
United Kingdom - 3433
United States - 57012
Uruguay - 9
Venezuela - 60
Vietnam - 26

La gráfica correspondiente al período analizado muestra una distribución global de intentos de ciberataques, con una concentración significativa en América del Norte, Europa y algunas regiones de Asia. En esta ocasión, Estados Unidos se posiciona como la principal fuente con 57,012 intentos registrados, seguido por Reino Unido con 3,433, Francia con 2,692, China con 2,315 y Hong Kong con 2,057.

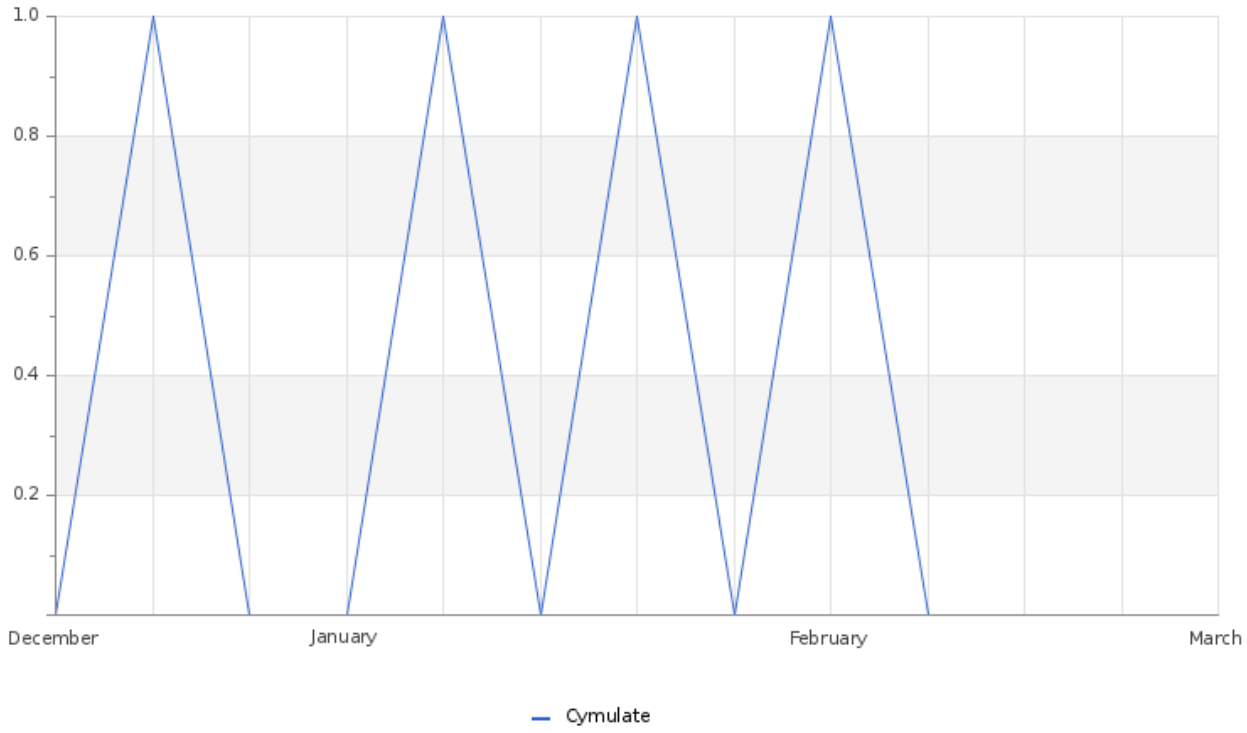
En un segundo nivel se identifican Alemania (1,423), México (1,403), Filipinas (1,301), Países Bajos (1,366) y Bulgaria (1,053), los cuales también representan focos relevantes dentro del volumen total de actividad maliciosa detectada. Asimismo, se observa la participación de otros países como India (981), Brasil (2,280), Turquía (553), Argentina (531) y Singapur (444), lo que refleja una amplia dispersión geográfica en el origen de los ataques.

Esta distribución evidencia que gran parte de la actividad proviene de países con alta infraestructura tecnológica o importantes nodos de conectividad global, lo que puede indicar el uso de servidores comprometidos, servicios en la nube o infraestructuras intermedias para lanzar los ataques. De igual forma, se observa una presencia constante de múltiples regiones, incluyendo Europa del Este, Asia y América Latina, lo que refuerza el carácter global y distribuido del panorama de amenazas.

Este escenario resalta la importancia de mantener estrategias de monitoreo continuo, inteligencia de amenazas y controles de seguridad adaptativos, permitiendo priorizar la detección y mitigación en las regiones con mayor actividad, sin perder una visión integral del entorno de riesgo en constante evolución.

Organo Judicial 03/20/2026

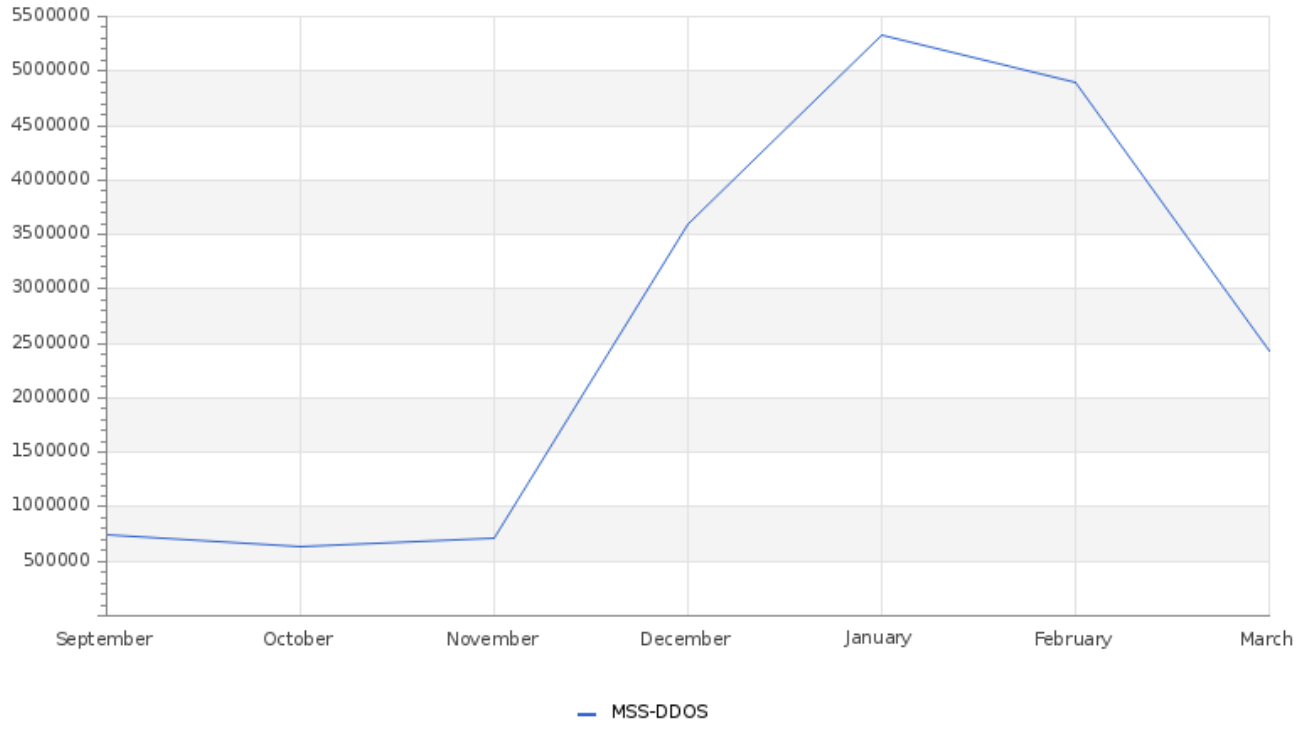
Total Number of Successful MFA authentications per application



Total Attacks Successfully Blocked Per Service

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

Organo Judicial 03/20/2026



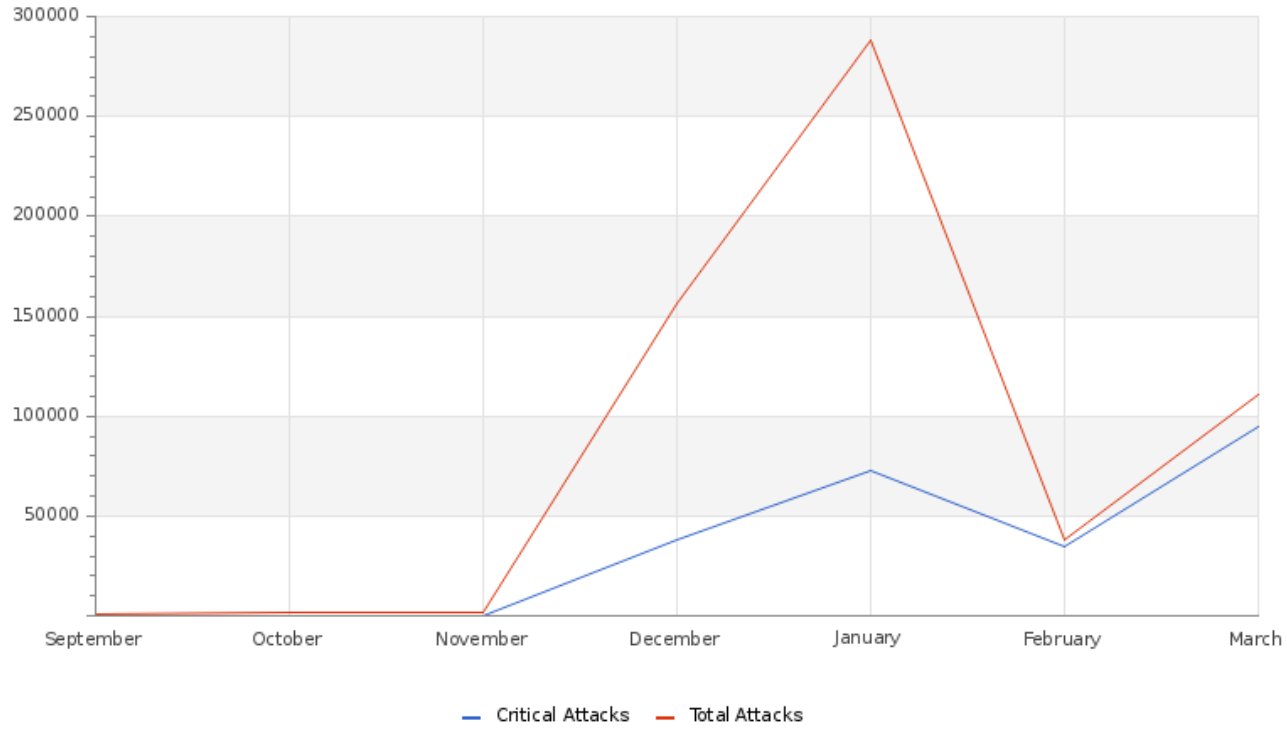
Durante el mes de febrero, el servicio MSS-DDOS registró una reducción significativa en el número de incidentes bloqueados respecto al período anterior, reflejando una disminución notable en la intensidad de las campañas de ataque DDoS. Este comportamiento evidencia un descenso en la actividad maliciosa durante el intervalo analizado.

A pesar de la reducción en el volumen de ataques, el servicio mantuvo una respuesta eficaz y consistente, garantizando la mitigación oportuna de los incidentes y la protección continua de la infraestructura crítica. La capacidad demostrada para adaptarse a escenarios con diferentes niveles de amenaza confirma la resiliencia del sistema y asegura la continuidad operativa frente a ataques DDoS de alta variabilidad.

Attacks Successfully Blocked by Severity

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

Organo Judicial 03/20/2026



Durante el mes de febrero se registró una disminución significativa en el volumen de ataques bloqueados, alcanzando un total aproximado de 40,000 eventos, lo que representa una caída considerable en comparación con el pico observado en enero. Esta reducción sugiere una menor actividad maliciosa o una variación en los patrones de ataque durante el periodo analizado.

En términos de severidad, los Critical Attacks se situaron alrededor de 35,000 eventos, manteniendo una proporción elevada respecto al total de ataques. Esto indica que, aunque el volumen general disminuyó, la criticidad de las amenazas persistió, lo que resalta la importancia de mantener controles de seguridad robustos y capacidades de respuesta activa.

La caída abrupta respecto al mes anterior podría estar asociada a factores como cambios en las campañas de ataque, efectividad de las medidas de mitigación implementadas o variaciones en la superficie de exposición. No obstante, la presencia de un volumen relevante de ataques críticos evidencia que el entorno continúa expuesto a amenazas avanzadas.

Recomendamos mantener el monitoreo continuo, reforzar las capacidades de detección y análisis, y validar la efectividad de los controles implementados para asegurar la contención oportuna de amenazas de alta severidad.

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

Organo Judicial 03/20/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	13	2
Critical Device Outages	0	0

Durante el período actual se registraron 13 interrupciones de dispositivos, lo que representa un incremento significativo frente al mes anterior, en el cual se contabilizaron únicamente 2 interrupciones. A pesar de este aumento en la frecuencia de incidencias, no se reportaron interrupciones críticas, manteniéndose este indicador en niveles nulos. Este resultado confirma que la disponibilidad y el desempeño de los sistemas críticos permanecieron estables, evidenciando la eficacia de los mecanismos de contención y recuperación implementados.

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

Organo Judicial 03/20/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Consejo de Administración de la Carrera de la Defensa Pública	HTTP Advanced	Web Servers	Down		5748	2026-02-10 00:02:45	2026-03-02 00:00:09
www.organojudicial.gob.pa	HTTP	200.46.13.0/26	Down, Warning		415	2026-02-26 17:40:41	2026-03-10 21:14:41
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		152	2026-02-11 17:16:46	2026-03-10 19:34:29
Repositorio digital	HTTP Advanced	Web Servers	Down, Warning		127	2026-02-22 21:29:45	2026-03-10 19:39:30
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		102	2026-02-25 19:18:17	2026-03-10 19:44:30
Gestor Documental	HTTP Advanced	Web Servers	Down, Warning		81	2026-02-10 22:14:04	2026-03-10 19:34:29
Plataforma Moodle Escuela Judicial	HTTP Advanced	Web Servers	Down, Warning		44	2026-02-25 18:58:56	2026-03-10 19:34:29
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		38	2026-02-25 20:12:13	2026-03-10 19:44:30
Probe Device	System Health	Organo Judicial C-GMSA	Down, Warning		24	2026-02-10 04:03:02	2026-03-12 03:03:05
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Down, Warning		23	2026-02-10 01:22:13	2026-02-10 05:23:13
IP.net126-113.psi.net.pa (200.46.126.113)	Ping	200.46.126.112/29	Down, Warning		21	2026-02-16 15:01:29	2026-03-08 05:43:59
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		19	2026-02-26 17:38:42	2026-03-10 19:34:29
Plataforma de correo	HTTP Advanced	Web Servers	Down		11	2026-03-05 00:24:52	2026-03-05 01:14:52
200.46.65.105	Ping	200.46.65.104/29	Down, Warning		9	2026-02-16 16:41:25	2026-03-08 05:43:55
Probe Device	Probe Health	Organo Judicial C-GMSA	Down		3	2026-02-11 04:49:20	2026-02-12 02:00:01

Organo Judicial 03/20/2026

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	1,493,841	0	831	0

El informe del período analizado confirma que la capa MSS-DDOS se mantuvo como la principal línea de defensa frente a intentos de denegación de servicio, bloqueando un total de 1,493,841 ataques, lo que representa un incremento significativo respecto al mes anterior. Este aumento puede estar asociado tanto a la intensificación de campañas maliciosas de gran escala como a la mejora en las capacidades de detección y respuesta del sistema.

De manera consistente con periodos previos, no se registraron incidentes en las demás capas de seguridad (MSS-UTM, MSS-DLP y MSS-EDR), lo que refleja un entorno estable y un control efectivo de amenazas fuera del ámbito DDoS. Este comportamiento sugiere que los mecanismos de protección multicapa continúan funcionando de manera coordinada, garantizando la resiliencia de los sistemas críticos y la eficacia de las políticas de mitigación implementadas.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in High or Critical Vulnerabilities	82
Change in Systems Performance	169
Change in Systems Availability	48
Non Baselined Discovered System	526
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	1

Durante el mes analizado se observó una actividad relevante en eventos operacionales y de seguridad. En particular, se registraron 82 eventos de tipo Change in High or Critical Vulnerabilities, lo que evidencia una exposición significativa a vulnerabilidades críticas y resalta la necesidad de mantener un proceso continuo y efectivo de gestión y remediación.

En el ámbito operativo, se identificaron 169 eventos asociados a Change in Systems Performance, lo que indica variaciones en el rendimiento de los sistemas que podrían impactar la eficiencia de los servicios. Asimismo, se reportaron 48 eventos de Change in Systems Availability, reflejando posibles afectaciones en la continuidad operativa.

Un aspecto relevante corresponde a los 526 eventos de Non Baselined Discovered System, lo que representa un riesgo considerable en términos de control de activos y cumplimiento de configuraciones base, sugiriendo brechas en los procesos de inventario y hardening.

Adicionalmente, se detectó 1 evento de Change in Internal High or Critical Vulnerabilities for IT, IoT and OT, el cual, aunque de baja frecuencia, puede tener un impacto significativo debido a la criticidad de los entornos involucrados.

En conjunto, estos resultados reflejan un entorno con actividad constante tanto en seguridad como en operación, destacando la importancia de fortalecer las capacidades de monitoreo continuo, gestión de vulnerabilidades y control de activos, con el fin de reducir la superficie de ataque y garantizar la estabilidad del entorno tecnológico.

Organo Judicial 03/20/2026

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