TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

June 13, 2026

Organo Judicial 06/13/2026

TLP AMBER CISO
EXECUTIVE REPORT

Este informe corresponde "Abril 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

El nivel de riesgo actual se mantiene constante con el mes anterior, situándose dentro de un rango bajo. Esto refleja la continuidad en el control de la actividad de amenazas sobre los activos monitoreados y sugiere que las medidas de seguridad implementadas continúan siendo efectivas. Sin embargo, resulta esencial mantener una supervisión constante para preservar este nivel y anticipar posibles cambios en el entorno.

Accepted Risk

n/a

El cliente no ha definido formalmente su nivel de Tolerancia al Riesgo durante la configuración del servicio. Por lo tanto, el análisis se realiza en función del Riesgo Real identificado y las mejores prácticas de ciberseguridad.

Confidence

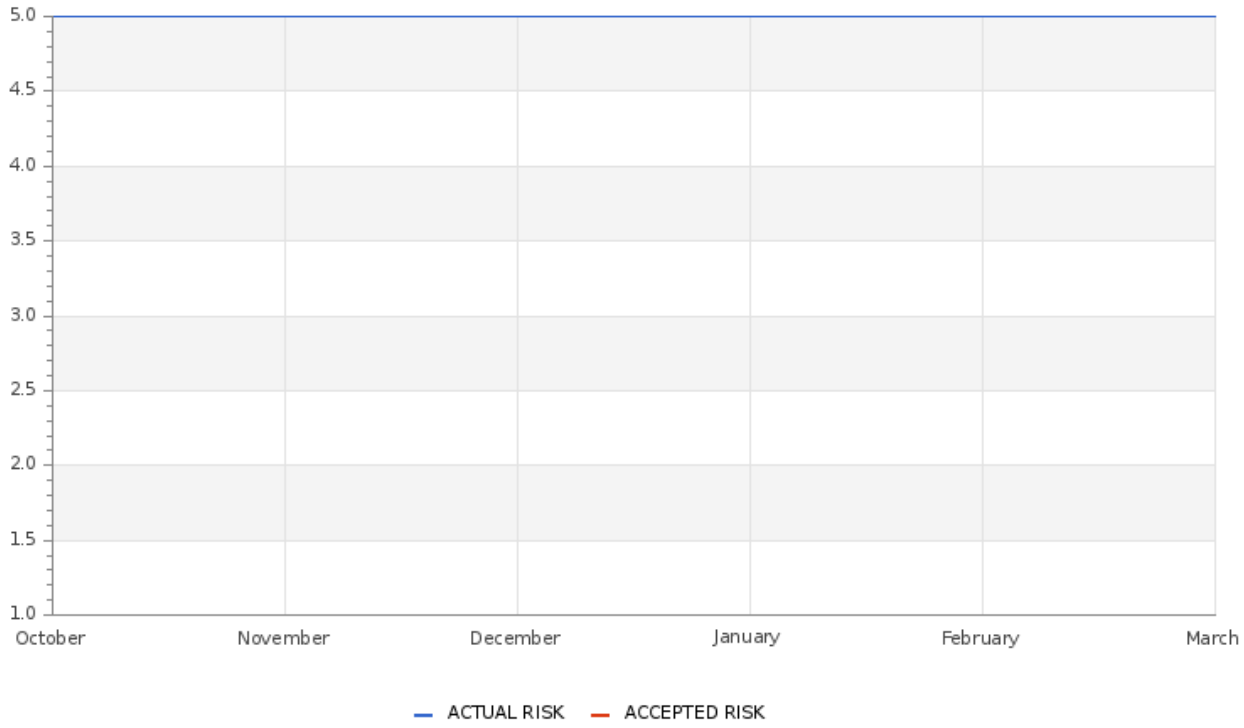
Low

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	0	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	atencionenlinea.organojudicial.gob.pa	0
Current	4	

Durante el período analizado se identificaron vulnerabilidades asociadas al activo atencionenlinea.organojudicial.gob.pa, registrándose un total de 4 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.

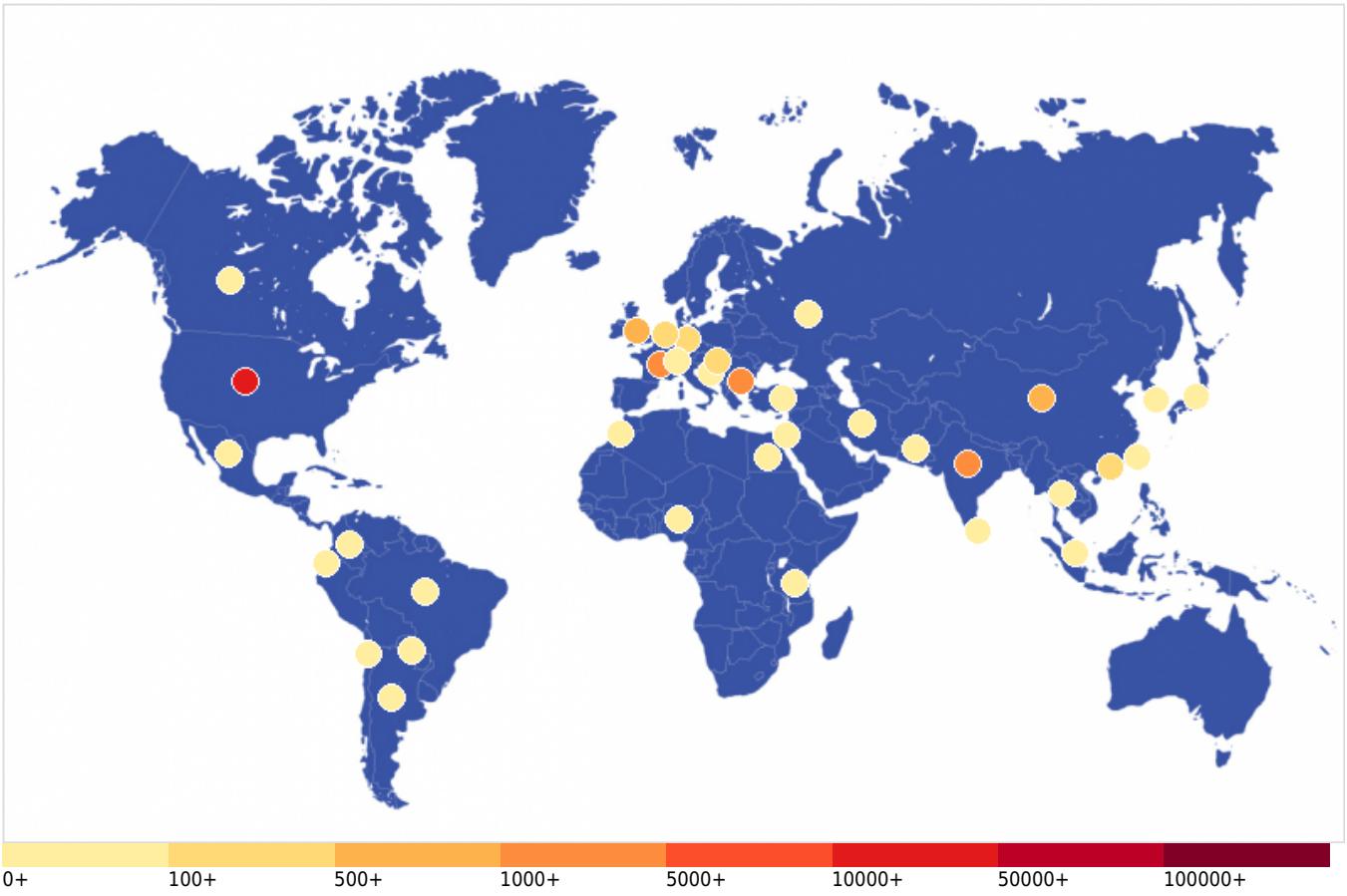
Vulnerability Metric

9

Organo Judicial 06/13/2026

THREATS

Critical Attacks Per Country In Past Week



Argentina - 12
Bosnia and Herzegovina - 19
Brazil - 70
Bulgaria - 1191
Canada - 33
Chile - 2
China - 521
Colombia - 6
Ecuador - 4
Egypt - 2
France - 3155
Germany - 263
Hong Kong - 188
Hungary - 349
India - 1038
Israel - 13
Japan - 45
Jordan - 4
Mexico - 10
Morocco - 1
Netherlands - 202
Nigeria - 12
Pakistan - 4
Paraguay - 1
Russia - 22
Singapore - 5
South Korea - 5
Sri Lanka - 3
Switzerland - 2
Taiwan - 8
Tanzania - 2
Thailand - 2
Turkey - 44
United Kingdom - 510
United States - 10646

La gráfica correspondiente al período analizado muestra una distribución global de ataques críticos, con una mayor concentración de eventos provenientes de América del Norte, Europa y Asia. Estados Unidos se mantiene como la principal fuente de actividad, con 10,646 eventos registrados, seguido por Francia (3,155), Bulgaria (1,191), India (1,038) y China (521).

En un segundo nivel se ubican Reino Unido (510), Hungría (349), Alemania (263), Países Bajos (202) y Hong Kong (188), los cuales también representan una proporción relevante de la actividad observada. Adicionalmente, se identificaron eventos provenientes de otras regiones, incluyendo Turquía, Japón, Canadá, Rusia y Bosnia y Herzegovina, evidenciando una amplia

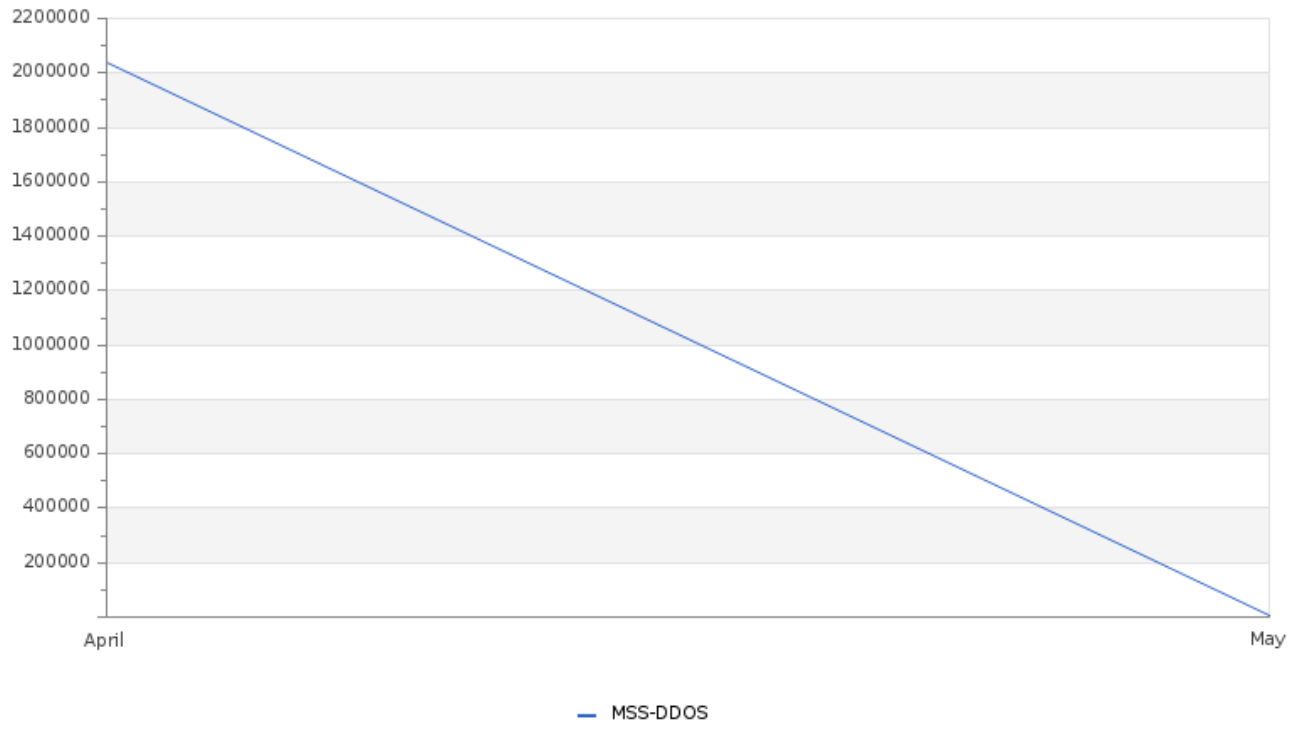
distribución geográfica en el origen de los ataques.

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.

Total Number of Successful MFA authentications per application

Organo Judicial 06/13/2026

Total Attacks Successfully Blocked Per Service



Durante el mes de abril, se registró actividad asociada a intentos de ataques de denegación de servicio distribuido (DDoS) dirigidos a la organización. Este comportamiento evidencia que las amenazas orientadas a afectar la disponibilidad de los servicios expuestos continúan representando un riesgo relevante para la operación institucional.

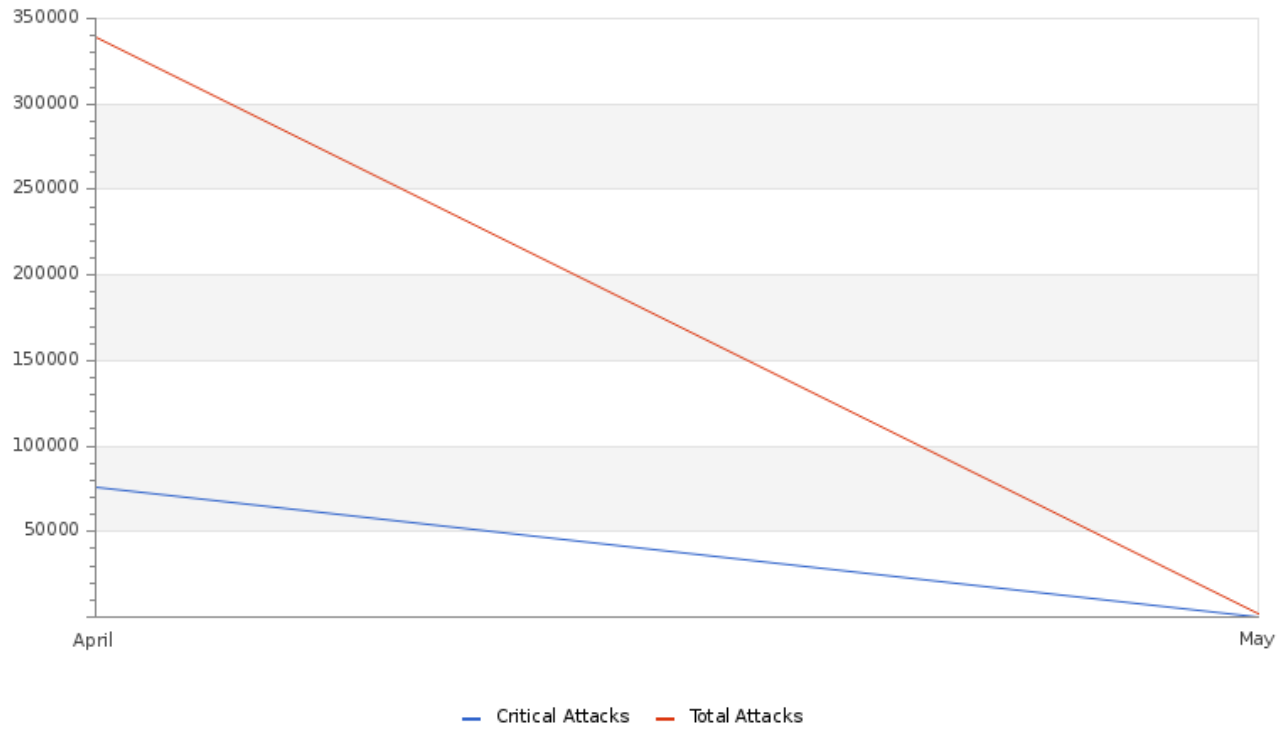
Las capacidades de protección implementadas permitieron detectar y mitigar oportunamente los eventos identificados, contribuyendo a mantener la disponibilidad de los servicios y reduciendo el riesgo de interrupciones operativas. Los resultados observados reflejan la efectividad de los mecanismos de mitigación implementados para enfrentar este tipo de amenazas.

La actividad registrada durante el período resalta la importancia de mantener controles especializados para la protección de los servicios expuestos a Internet, así como capacidades de monitoreo y respuesta que permitan gestionar oportunamente eventos que puedan afectar la disponibilidad de los recursos tecnológicos. Estas capacidades contribuyen a fortalecer la resiliencia operativa y la continuidad de los servicios institucionales.

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 período analizado evidencia un volumen significativo de actividad maliciosa dirigida a la organización, destacando una proporción relevante de ataques clasificados como críticos dentro del total de eventos bloqueados. Durante abril, los controles de seguridad implementados lograron contener eficazmente los intentos de ataque identificados, contribuyendo a reducir el riesgo de afectación sobre los activos y servicios institucionales.

La distribución por severidad refleja la presencia continua de amenazas con potencial impacto sobre la operación de la organización, lo que confirma la necesidad de mantener una postura de seguridad robusta y capacidades de monitoreo permanentes. La capacidad de detección y bloqueo demostrada durante el período permitió gestionar eficazmente tanto eventos críticos como actividades maliciosas de menor severidad, fortaleciendo el nivel general de protección.

Este comportamiento evidencia la efectividad de los controles de seguridad actualmente implementados y resalta la importancia de mantener una estrategia integral de gestión del riesgo cibernético. La visibilidad proporcionada por estos indicadores permite identificar tendencias relevantes, evaluar la evolución del panorama de amenazas y respaldar la toma de decisiones estratégicas orientadas a 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 06/13/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	11	0
Critical Device Outages	0	0

La disponibilidad de los servicios tecnológicos de la organización se mantuvo en niveles adecuados durante el período analizado. Si bien se registró un incremento en los eventos de indisponibilidad respecto al período anterior, no se reportaron interrupciones clasificadas como críticas.

La ausencia de eventos de alta criticidad evidencia la capacidad de la organización para preservar la continuidad de los servicios esenciales y mantener una postura de resiliencia operativa frente a incidentes que pudieran afectar la disponibilidad de la infraestructura tecnológica.

Este comportamiento resalta la importancia de continuar fortaleciendo las capacidades de supervisión y gestión de la disponibilidad, permitiendo identificar tendencias operativas, mitigar riesgos potenciales y respaldar la continuidad de las funciones críticas de la organización.

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Comision de Curadores y Auxiliares Judiciales	HTTP Advanced	Web Servers	Down		8436	2026-04-02 00:04:10	2026-05-01 08:40:11
Plataforma Moodle Escuela Judicial	HTTP Advanced	Web Servers	Down, Warning		1809	2026-04-03 22:39:20	2026-04-16 19:21:22
www.organojudicial.gob.pa	HTTP	200.46.13.0/26	Down, Warning		1744	2026-04-03 19:04:03	2026-04-29 23:15:36
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		1734	2026-04-03 18:48:48	2026-04-16 19:20:50
Plataforma de correo	HTTP Advanced	Web Servers	Down, Warning		1731	2026-04-03 18:49:17	2026-04-16 19:21:19
Sistema Integral de Gestión de Recursos Humanos	HTTP Advanced	Web Servers	Down		133	2026-04-30 21:38:40	2026-05-01 08:40:11
Repositorio digital	HTTP Advanced	Web Servers	Down, Warning		36	2026-04-21 14:46:49	2026-04-25 07:45:29
Probe Device	System Health	Organo Judicial	Warning		31	2026-04-05 03:02:40	2026-04-30 08:46:53
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		25	2026-04-25 06:15:17	2026-04-29 11:13:57
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		25	2026-04-22 03:13:06	2026-04-29 10:13:49
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		12	2026-04-25 06:30:19	2026-04-28 00:59:17
Gestor Documental	HTTP Advanced	Web Servers	Warning		4	2026-04-25 06:20:18	2026-04-25 08:05:32

LATAM HQ +507 836-5355

US HQ +1 (321) 430-0500

Organo Judicial 06/13/2026

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
www.organojudicial.gob.pa	Port	200.46.13.0/26	Down		3	2026-04-15 18:18:12	2026-04-15 18:28:17
Probe Device	Probe Health	Organo Judicial	Down		2	2026-04-17 02:16:43	2026-04-21 08:25:01
www.organojudicial.gob.pa	HTTP Advanced	200.46.13.0/26	Down		1	2026-04-15 18:03:10	2026-04-15 18:03:10

La disponibilidad de los servicios tecnológicos de la organización se mantuvo en niveles adecuados durante el período analizado. Aunque se registraron eventos de indisponibilidad en algunos servicios institucionales, no se identificaron interrupciones de criticidad alta que comprometieran la continuidad de las operaciones o la disponibilidad de los servicios esenciales.

Los eventos observados estuvieron asociados principalmente a plataformas y servicios de soporte institucional. Sin embargo, la ausencia de incidentes críticos evidencia una adecuada capacidad para gestionar eventos de disponibilidad y mantener la estabilidad operativa de la infraestructura tecnológica.

Este comportamiento resalta la importancia de continuar fortaleciendo las capacidades de monitoreo y gestión de la disponibilidad, permitiendo identificar oportunamente posibles afectaciones y reducir su impacto sobre la operación. El seguimiento continuo de estos indicadores contribuye a la gestión del riesgo tecnológico y al mantenimiento de la continuidad de 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	40,856	0	257	0

La gráfica correspondiente al período analizado evidencia la efectividad de los controles de seguridad implementados para la protección de la organización. Durante el período, se registró actividad maliciosa que fue detectada y bloqueada oportunamente, evitando posibles afectaciones a la disponibilidad de los servicios y a los activos tecnológicos institucionales.

La actividad observada estuvo compuesta principalmente por intentos dirigidos a afectar la disponibilidad de los servicios expuestos, así como por eventos asociados a amenazas detectadas en estaciones de trabajo y otros activos tecnológicos. La capacidad de los controles de seguridad para identificar y contener estas actividades permitió reducir el riesgo de impacto sobre la operación de la organización.

Este comportamiento resalta la importancia de mantener una estrategia de seguridad basada en múltiples capas de protección, fortaleciendo las capacidades de prevención, detección y respuesta ante amenazas. La efectividad demostrada durante el período contribuye a la gestión del riesgo cibernético y al mantenimiento de la continuidad de los servicios críticos de la organización.

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

Organo Judicial 06/13/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Notable Event Alert: Endpoint Configuration Management High Priority Event	5
Change in External High or Critical Vulnerabilities	71
Monitoring for open ports	26
Change in Critical Perimeter Attacks	364
Change in Systems Performance	186
Non Baselined Discovered System	356
Change in Systems Availability	26
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	23
High Persistency Detection	71
Threat Intelligence Validation	5
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

Durante el período analizado se identificaron diversos eventos relacionados con cambios en la postura de seguridad de la organización, destacando principalmente Change in Critical Perimeter Attacks (364 eventos), Non Baselined Discovered System (356 eventos) y Change in Systems Performance (186 eventos). Estos indicadores concentraron la mayor parte de la actividad observada y reflejan la importancia de mantener una supervisión continua sobre los activos y servicios críticos de la organización.

Asimismo, se registraron eventos asociados a Change in External High or Critical Vulnerabilities (71 eventos), High Persistency Detection (71 eventos), Monitoring for Open Ports (26 eventos), Change in Systems Availability (26 eventos) y Change in Internal High or Critical Vulnerabilities for IT, IoT and OT (23 eventos). Adicionalmente, se identificaron eventos relacionados con Targeted Campaign Alignment, Threat Intelligence Validation, Endpoint Configuration Management High Priority Event y TEVR BAS Immediate Threats, los cuales requieren seguimiento para una adecuada gestión de la exposición y del riesgo tecnológico.

Los resultados observados reflejan la necesidad de mantener una gestión continua de vulnerabilidades, configuraciones de seguridad y exposición de activos. El seguimiento de estos indicadores permite identificar oportunamente cambios relevantes en la postura de seguridad, priorizar acciones de mitigación y fortalecer las capacidades de protección de la organización, contribuyendo a la continuidad de los servicios institucionales y a la reducción del riesgo cibernético.

Organo Judicial 06/13/2026

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