



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# CISO EXECUTIVE REPORT

ORGANO JUDICIAL

June 11, 2026



Organo Judicial 06/11/2026

# 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.



Organo Judicial 06/11/2026

**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 06/11/2026

**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	

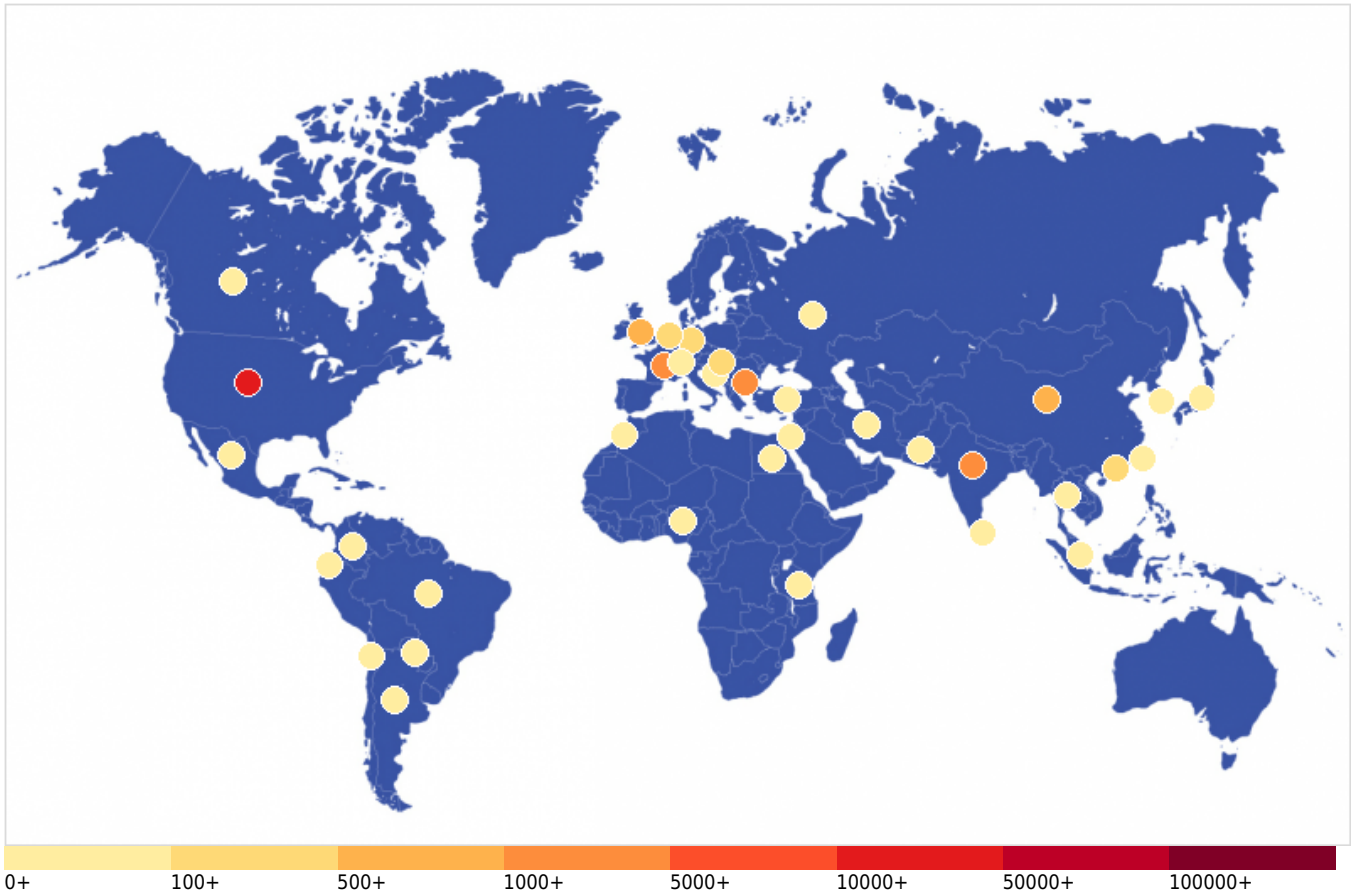
**Vulnerability Metric**

**9**

# THREATS

**Critical Attacks Per Country In Past Week**

Organo Judicial 06/11/2026

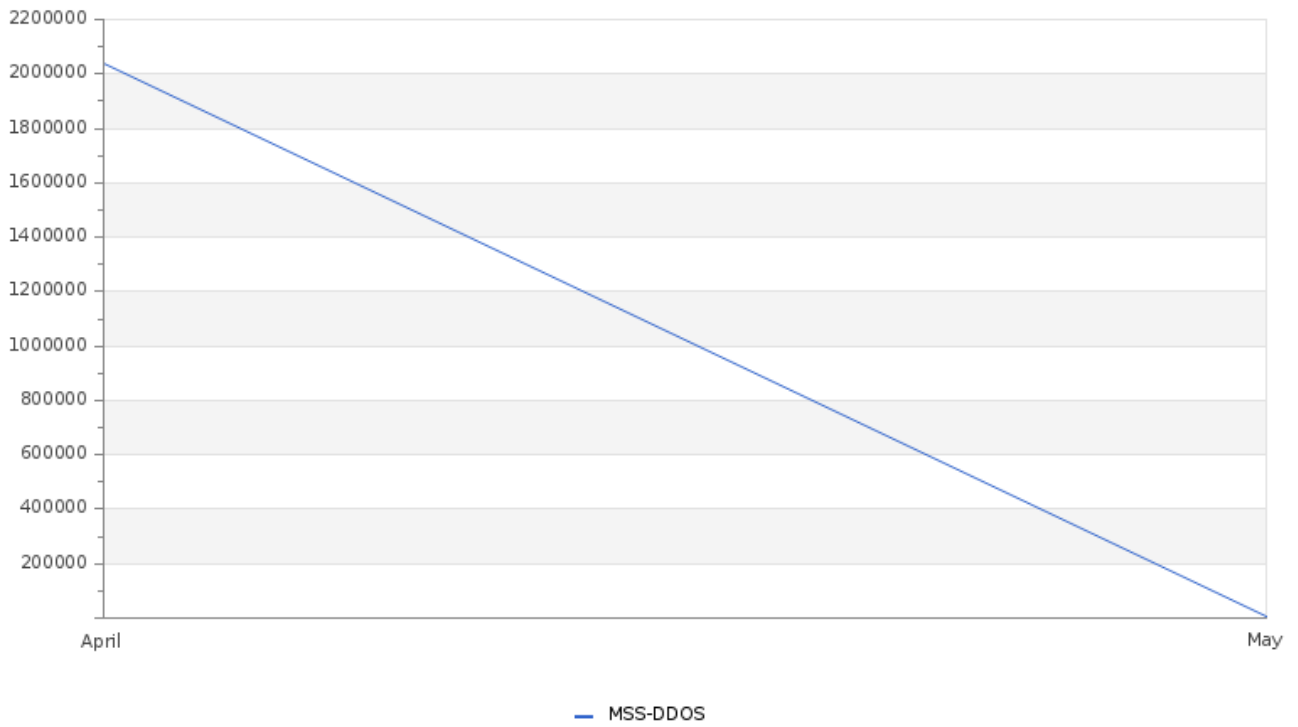


Argentina - 12	Bosnia and Herzegovina - 19	Brazil - 70	Bulgaria - 1191
Canada - 33	Chile - 2	China - 521	Colombia - 6
Ecuador - 4	Egypt - 2	France - 3155	Germany - 263
Hong Kong - 188	Hungary - 349	India - 1038	Israel - 13
Japan - 45	Jordan - 4	Mexico - 10	Morocco - 1
Netherlands - 202	Nigeria - 12	Pakistan - 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	

**Total Number of Successful MFA authentications per application**

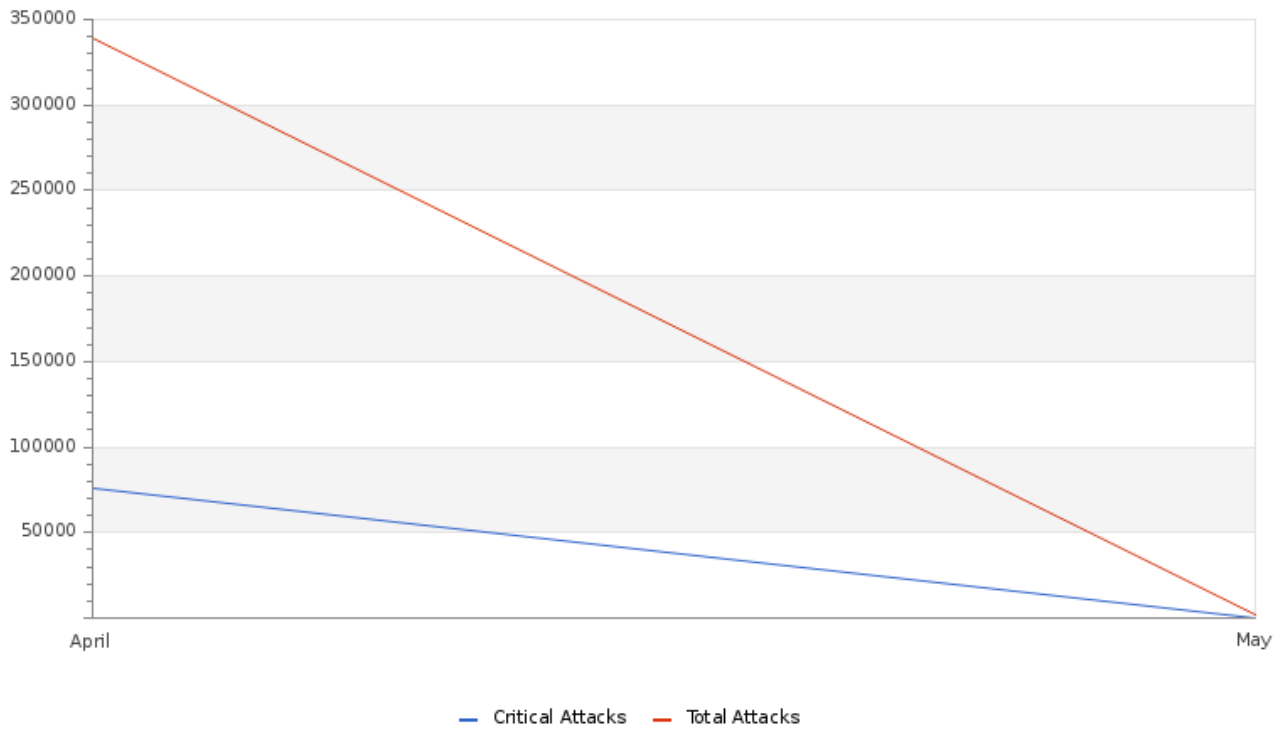
Organo Judicial 06/11/2026

**Total Attacks Successfully Blocked Per Service**



Organo Judicial 06/11/2026

### Attacks Successfully Blocked by Severity



### System Availability and Performance in current & previous month

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

Organo Judicial 06/11/2026

**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
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

**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

Organo Judicial 06/11/2026

# 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	66
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	70
Threat Intelligence Validation	5
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

**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.**



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

## CISO EXECUTIVE REPORT

### HOW CAN WE HELP?

Contact us today for more information on  
our services and security solutions.

