



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# CISO EXECUTIVE REPORT

ORGANO JUDICIAL

August 18, 2026



Organo Judicial 08/18/2026

# TLP AMBER CISO

## EXECUTIVE REPORT

Este informe corresponde "JUNIO 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

Durante junio no se identificaron amenazas activas que permitieran establecer un nivel cuantificable de riesgo actual. Aunque permanecen hallazgos de vulnerabilidad y actividad de seguridad bajo monitoreo, los controles implementados continúan limitando la exposición observada durante el período.

### Accepted Risk

n/a

El análisis se mantiene enfocado en los riesgos identificados y en las condiciones observadas durante el monitoreo.

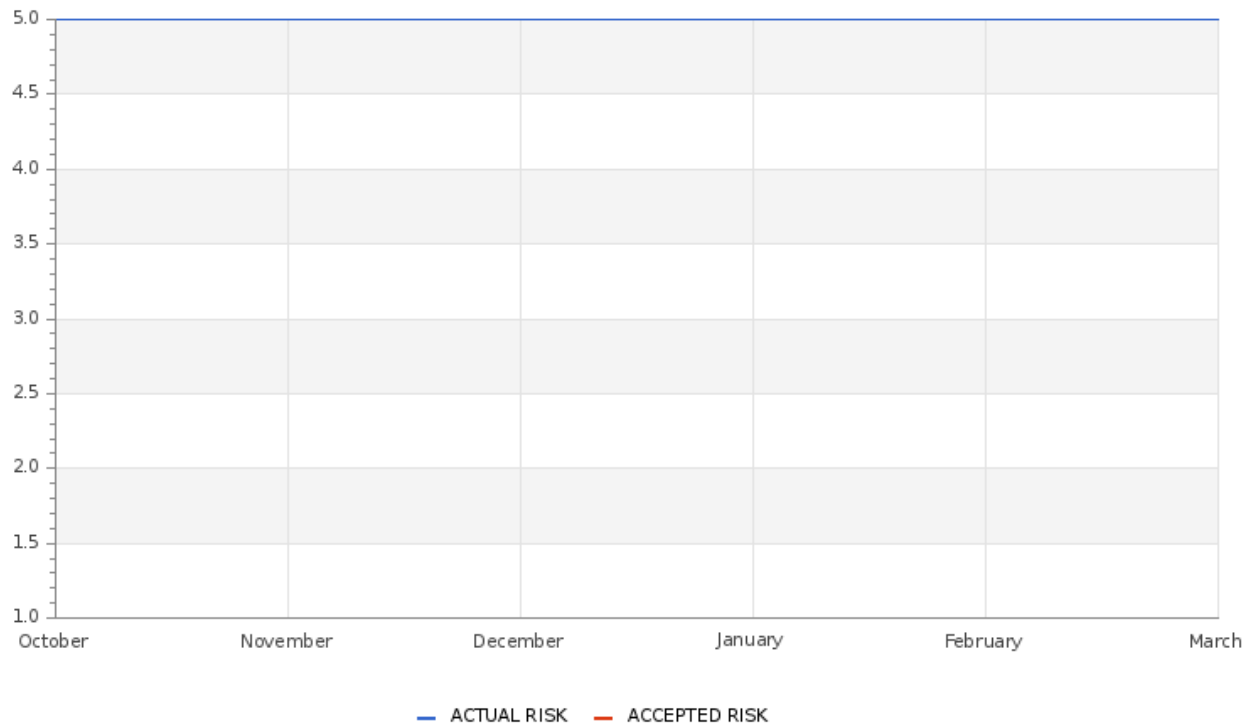
### Confidence

**Low**

El nivel de confianza se mantiene en Low, debido a que la visibilidad disponible continúa siendo parcial y no se cuenta con la integración completa de todas las fuentes necesarias para realizar una valoración integral del riesgo.



Organo Judicial 08/18/2026

**Accepted & Actual Risk**

Durante junio no se registraron variaciones en los indicadores de Actual Risk y Accepted Risk

La evaluación continúa sustentándose en la información disponible a través de los servicios de monitoreo y seguridad integrados, por lo que la incorporación de nuevas fuentes de telemetría permitiría aumentar la precisión y el nivel de confianza de futuras evaluaciones.

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

|               | Current Month | Previous Month |
|---------------|---------------|----------------|
| Actual Risk   | 5             | 5              |
| Accepted Risk | 0             | 0              |

**Nivel Actual de Riesgo:**

Durante junio, el nivel de riesgo se mantuvo estable respecto al período anterior, sin evidenciar incrementos en la exposición general de la organización. Este comportamiento refleja una continuidad en la postura de seguridad observada, aunque se mantiene la necesidad de supervisar los cambios en vulnerabilidades, actividad perimetral y eventos detectados por los distintos controles de seguridad.

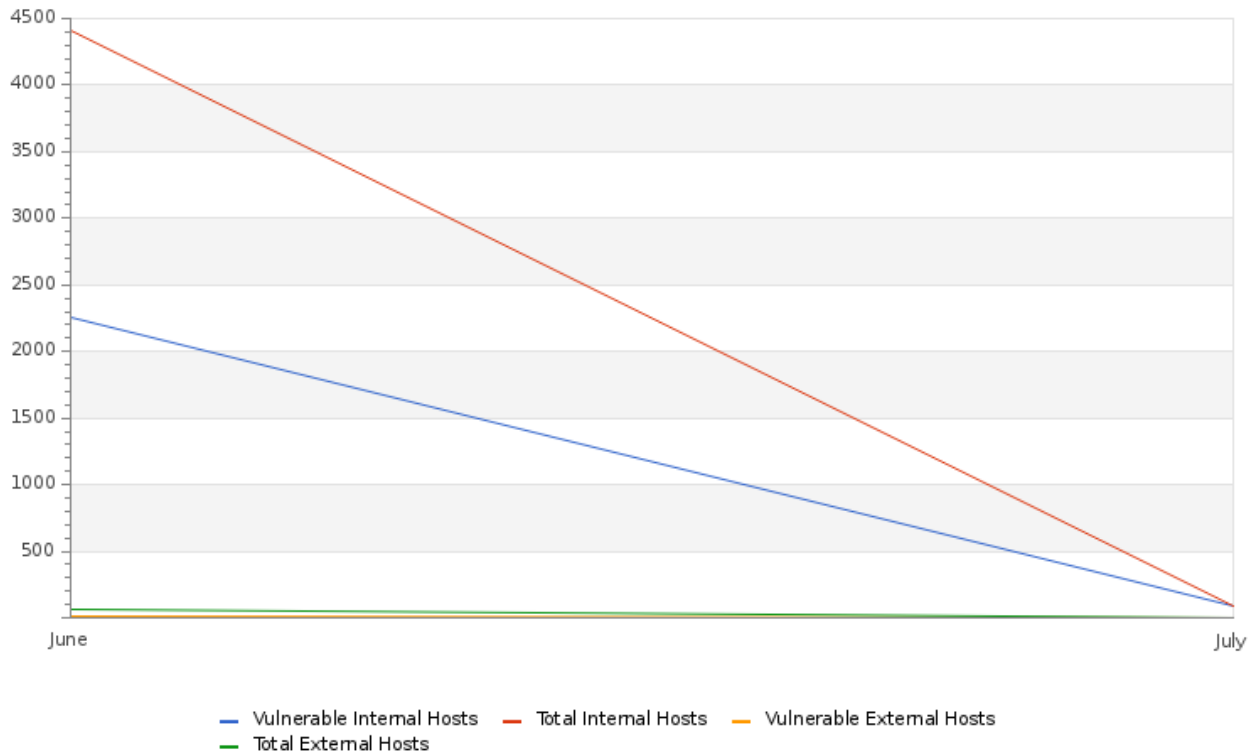
**Riesgo Aceptado:**

El indicador de riesgo aceptado no presentó variaciones durante el período. Al mantenerse sin un margen de aceptación definido, resulta importante continuar evaluando los riesgos identificados de acuerdo con su criticidad y posible impacto, priorizando aquellos que puedan afectar activos o servicios relevantes para la operación.

Organo Judicial 08/18/2026

# VULNERABILITY

## Hosts & Vulnerable Hosts In Last 6 Months



Entre marzo y junio de 2026, la evolución de los activos internos muestra una reducción progresiva de la exposición después del nivel más alto registrado en marzo. En junio se evaluaron 6,990 hosts internos, de los cuales 4,280 presentaron vulnerabilidades.

Frente a mayo, cuando se identificaron 4,715 hosts vulnerables, junio registró una disminución de 435 activos vulnerables, a pesar de que la cantidad total de sistemas evaluados aumentó ligeramente. Este comportamiento representa una mejora en la proporción de activos internos vulnerables durante el período.

La superficie externa continúa representando una proporción considerablemente menor frente al entorno interno, por lo que la principal concentración de exposición permanece dentro de la infraestructura interna. Se recomienda mantener el seguimiento de esta tendencia y priorizar los activos que concentran vulnerabilidades de mayor severidad.

Organo Judicial 08/18/2026

Total Vulnerability Counts In Current & Previous Month

|         | Current Month                      | Previous Month |
|---------|------------------------------------|----------------|
| dest    | ojbiocontrol.organojudicial.gob.pa | 0              |
| Current | 3                                  |                |

Durante junio se observaron variaciones en la cantidad de vulnerabilidades asociadas a distintos activos monitoreados. Entre los hosts que presentaron cambios durante el período destaca ojbiocontrol.organojudicial.gob.pa, donde se identificaron nuevos hallazgos respecto al mes anterior.

Este comportamiento evidencia cambios en la exposición de determinados sistemas y refuerza la importancia de mantener un seguimiento continuo sobre los activos que presentan incrementos o nuevas vulnerabilidades, con el objetivo de validar su criticidad y priorizar las acciones de remediación correspondientes.

Vulnerability Metric

5

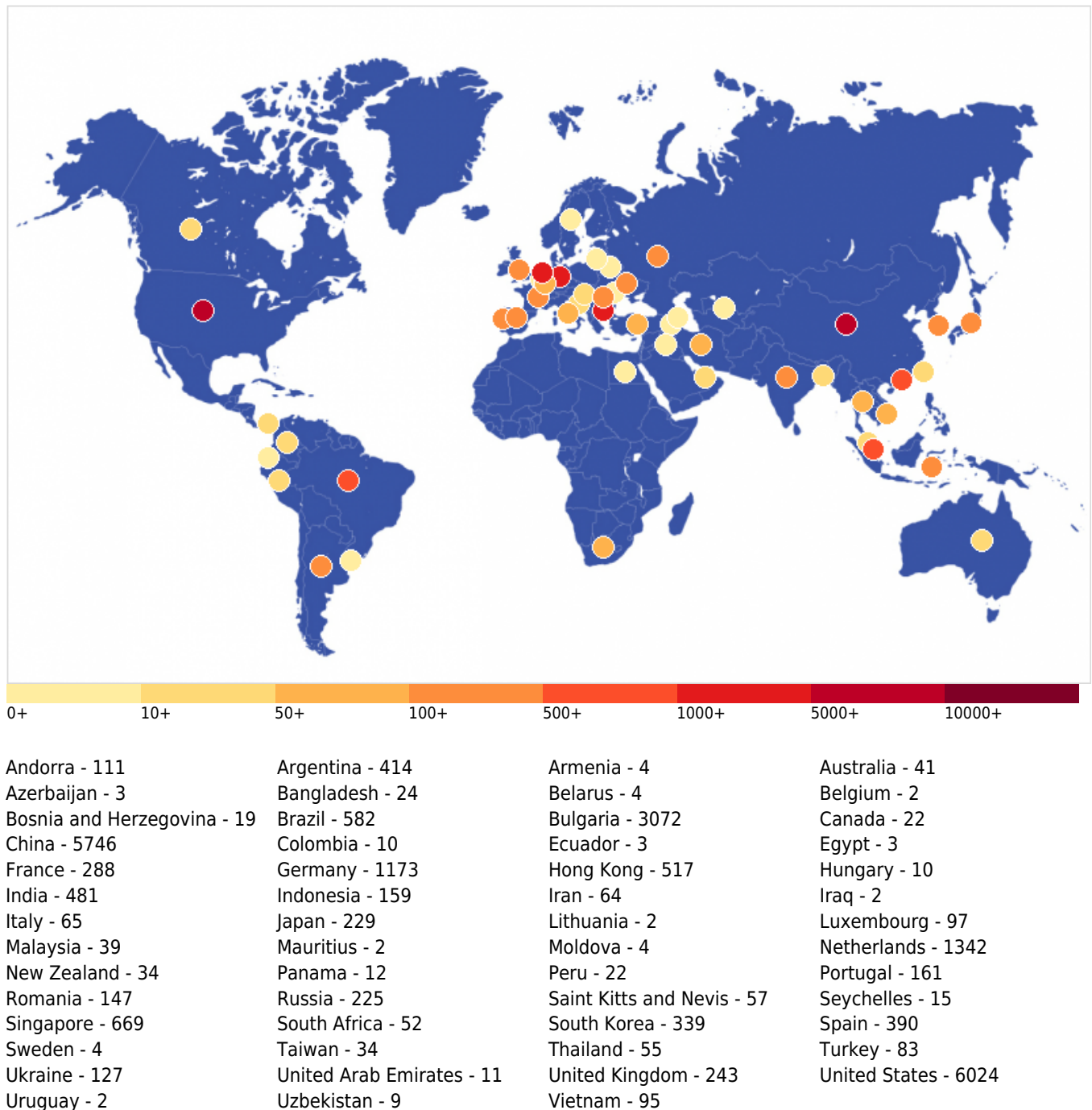
Durante junio, el Vulnerability Metric disminuyó de 8 a 5 respecto al período anterior, reflejando una mejora relevante en el nivel de exposición asociado a las vulnerabilidades identificadas.

Esta reducción es consistente con la disminución observada en la cantidad de hosts vulnerables durante el período y sugiere una evolución favorable en la postura de vulnerabilidades. No obstante, se recomienda mantener la priorización de los hallazgos críticos y altos, especialmente aquellos asociados a activos de mayor relevancia para la operación.

THREATS

Critical Attacks Per Country In Past Week

Organo Judicial 08/18/2026



Durante el período analizado se observa una distribución geográfica amplia de ataques críticos, con actividad proveniente de múltiples regiones, principalmente de Norteamérica, Europa y Asia. Este comportamiento evidencia que la exposición de los servicios publicados no se encuentra asociada a una única ubicación o fuente específica, sino a un entorno de amenazas distribuido globalmente.

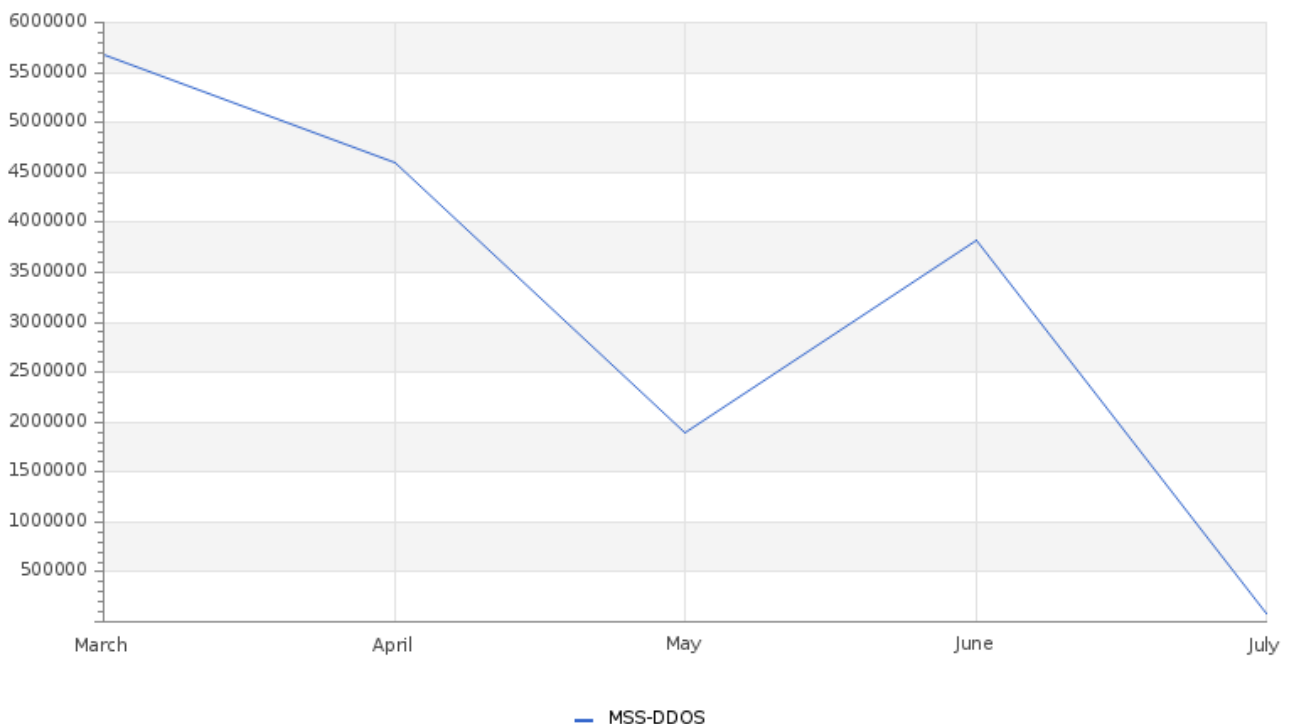
La presencia simultánea de actividad desde diferentes países es consistente con comportamientos automatizados de reconocimiento, escaneo y explotación de servicios expuestos, por lo que el origen geográfico debe considerarse como un indicador complementario y no como el único criterio para determinar el nivel de riesgo.

Organo Judicial 08/18/2026

Este panorama refuerza la importancia de mantener controles perimetrales, mecanismos de reputación y filtrado, así como monitoreo continuo sobre los activos expuestos, prestando especial atención a cambios relevantes en los patrones de origen y a incrementos dirigidos contra servicios críticos.

## Total Number of Successful MFA authentications per application

## Total Attacks Successfully Blocked Per Service

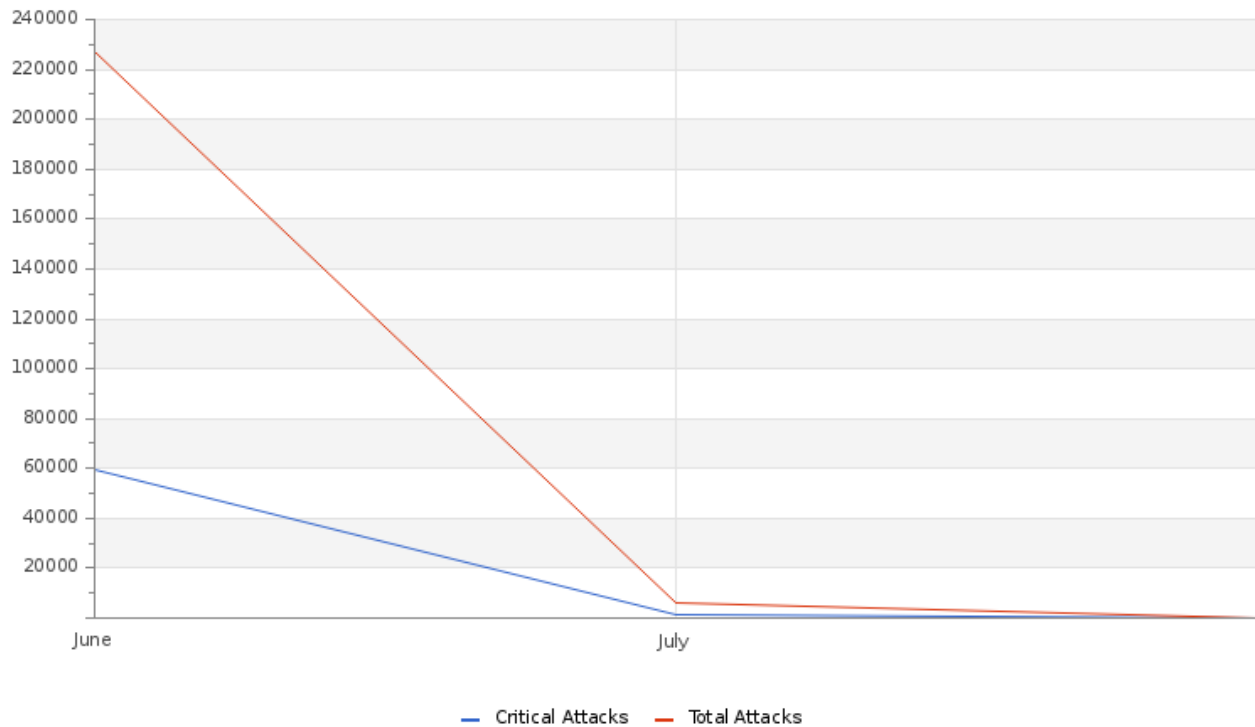


Durante junio se observó un repunte en la actividad DDoS respecto a mayo, luego de la disminución registrada en el período anterior. Aun así, el nivel de actividad permaneció por debajo de los valores observados durante marzo y abril, evidenciando un comportamiento fluctuante en los intentos dirigidos contra los servicios expuestos.

Los mecanismos de protección continuaron detectando y mitigando esta actividad, contribuyendo a reducir el riesgo de afectaciones sobre la disponibilidad de los servicios institucionales. La variación observada confirma la necesidad de mantener capacidades especializadas de monitoreo y mitigación, especialmente ante incrementos repentinos que puedan representar cambios en la presión ejercida sobre la infraestructura pública.

En términos generales, el comportamiento de junio refleja que la amenaza DDoS continúa activa y requiere seguimiento constante, aun cuando la intensidad varíe entre períodos.

Organo Judicial 08/18/2026

**Attacks Successfully Blocked by Severity**

La gráfica correspondiente al período analizado refleja una presencia relevante de actividad maliciosa clasificada como crítica dentro del total de ataques bloqueados. Este comportamiento indica que, durante junio, una parte importante de los intentos detectados tuvo un nivel de severidad elevado y pudo representar un riesgo significativo para los servicios y activos expuestos de la organización.

Los controles de seguridad implementados permitieron identificar y contener oportunamente esta actividad, reduciendo la posibilidad de afectaciones sobre la disponibilidad y continuidad de los servicios institucionales. La relación observada entre los ataques totales y los eventos críticos evidencia la necesidad de mantener especial seguimiento sobre este tipo de amenazas, ya que variaciones en su comportamiento pueden representar cambios importantes en la presión ejercida contra el perímetro.

En este sentido, la información proporcionada por estos indicadores permite evaluar la evolución de la actividad maliciosa y respaldar la priorización de medidas de protección sobre los activos con mayor exposición.



Organo Judicial 08/18/2026

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

|                         | Current Month | Previous Month |
|-------------------------|---------------|----------------|
| Total Device Outages    | 19            | 4              |
| Critical Device Outages | 0             | 0              |

Durante junio se observó un incremento significativo en los eventos de indisponibilidad respecto al período anterior, lo que refleja una mayor recurrencia de afectaciones sobre los dispositivos y servicios monitoreados.

A pesar de este aumento, no se registraron interrupciones clasificadas como críticas, por lo que no se evidenciaron afectaciones de alta severidad sobre la continuidad de los servicios esenciales.

Este comportamiento hace recomendable mantener especial seguimiento sobre los activos que presentan eventos recurrentes de disponibilidad, con el objetivo de identificar posibles patrones, causas comunes o degradaciones operativas antes de que puedan derivar en afectaciones de mayor impacto.

**Histogram of Total and Critical Device Outages**

| Device                                                  | Sensor                    | Group          | Status        | Criticality | Events | First_Seen          | Last_Seen           |
|---------------------------------------------------------|---------------------------|----------------|---------------|-------------|--------|---------------------|---------------------|
| DevConsejo de Administración de la Carrera Judicial ice | HTTP Advanced             | Web Servers    | Down          |             | 8229   | 2026-06-01 00:01:25 | 2026-07-01 09:00:47 |
| Comision de Curadores y Auxiliares Judiciales           | HTTP Advanced             | Web Servers    | Down          |             | 4600   | 2026-06-01 00:01:25 | 2026-06-18 18:00:05 |
| www.organojudicial.gob.pa                               | Sitio Web Organo Judicial | 200.46.13.0/26 | Down, Warning |             | 4493   | 2026-06-01 00:01:26 | 2026-06-18 17:54:45 |
| GMSA-OJ HyperV                                          | HTTP                      | GMSA-OJ        | Down, Warning |             | 135    | 2026-06-08 12:58:57 | 2026-06-23 15:15:41 |
| GMSA-OJ HyperV                                          | Ping                      | GMSA-OJ        | Down, Warning |             | 130    | 2026-06-08 12:58:57 | 2026-06-23 15:05:39 |
| Consulta de fallos                                      | HTTP Advanced             | Web Servers    | Down, Warning |             | 52     | 2026-06-06 18:44:08 | 2026-06-17 22:02:08 |
| Reporte biometrico                                      | HTTP Advanced             | Web Servers    | Down, Warning |             | 49     | 2026-06-06 18:44:15 | 2026-06-17 22:02:15 |
| Plataforma de Gestion de Pleno                          | HTTP Advanced             | Web Servers    | Down, Warning |             | 49     | 2026-06-06 18:44:12 | 2026-06-17 22:02:12 |
| Repositorio digital                                     | HTTP Advanced             | Web Servers    | Down, Warning |             | 48     | 2026-06-06 18:43:34 | 2026-06-20 06:00:43 |
| Plataforma Moodle Escuela Judicial                      | HTTP Advanced             | Web Servers    | Down, Warning |             | 48     | 2026-06-06 18:42:55 | 2026-06-17 22:01:54 |
| Plataforma de correo                                    | HTTP Advanced             | Web Servers    | Down, Warning |             | 42     | 2026-06-06 18:44:12 | 2026-06-30 23:34:17 |
| Gestor Documental                                       | HTTP Advanced             | Web Servers    | Down, Warning |             | 42     | 2026-06-06 18:42:45 | 2026-06-17 22:01:44 |

Organo Judicial 08/18/2026

| Device                                   | Sensor        | Group            | Status        | Criticality | Events | First_Seen          | Last_Seen           |
|------------------------------------------|---------------|------------------|---------------|-------------|--------|---------------------|---------------------|
| Sistema automatizado de gestion judicial | HTTP Advanced | Web Servers      | Down, Warning |             | 39     | 2026-06-06 18:43:51 | 2026-06-30 16:53:13 |
| Probe Device                             | System Health | Organo Judicial  | Warning       |             | 26     | 2026-06-01 03:01:51 | 2026-07-01 03:39:55 |
| 200.46.65.105                            | Ping          | 200.46.65.104/29 | Down, Warning |             | 17     | 2026-06-17 00:10:43 | 2026-06-23 11:05:01 |

Durante junio, los eventos de disponibilidad se concentraron principalmente en servicios web institucionales, observándose una mayor recurrencia de intermitencias e indisponibilidades momentáneas en el Consejo de Administración de la Carrera Judicial, la Comisión de Curadores y Auxiliares Judiciales y el portal [www.organojudicial.gob.pa](http://www.organojudicial.gob.pa).

También se identificaron eventos de menor frecuencia en componentes de infraestructura como GMSA-OJ HyperV, así como en distintas plataformas institucionales, entre ellas Consulta de Fallos, Reporte Biométrico, Repositorio Digital, Moodle, Plataforma de Correo y el Sistema Automatizado de Gestión Judicial.

A pesar del incremento general de eventos de disponibilidad durante el período, no se identificaron afectaciones clasificadas como críticas. El comportamiento observado sugiere mantener seguimiento sobre los servicios que presentan intermitencias recurrentes, con el objetivo de identificar posibles patrones y reducir la probabilidad de afectaciones prolongadas sobre la operación.

### 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       | 72,743   | 0       | 148     | 0       |

Durante junio, la actividad bloqueada se concentró principalmente en la capa de protección MSS-DDOS, lo que confirma que la mayor presión observada durante el período estuvo asociada a intentos dirigidos contra la disponibilidad de los servicios expuestos.

Por otra parte, MSS-EDR también registró actividad, aunque en una proporción considerablemente menor, reflejando la presencia de eventos detectados y contenidos a nivel de endpoints y servidores. En las demás capas de seguridad representadas no se observó actividad relevante dentro de este indicador durante el período.

En conjunto, el comportamiento evidencia que el perímetro de disponibilidad continúa siendo el principal foco de actividad maliciosa, mientras que los controles de endpoint mantienen un papel complementario en la detección y contención de amenazas internas.



Organo Judicial 08/18/2026

# OPERATIONAL

## Notable Events Active For The Last Month

| Notable Event Type                                                     | How Many # |
|------------------------------------------------------------------------|------------|
| Change in Systems Performance                                          | 125        |
| Change in Critical Perimeter Attacks                                   | 362        |
| Change in Internal High or Critical Vulnerabilities for IT, IoT and OT | 82         |
| Non Baselined Discovered System                                        | 340        |
| High Persistency Detection                                             | 89         |
| Change in External High or Critical Vulnerabilities                    | 43         |
| Change in Systems Availability                                         | 46         |
| Notable Event Alert: Vulnerability exposure from Threat Intelligence   | 3          |

Critical Perimeter Attacks y Non Baselined Discovered System continúan siendo los principales indicadores de actividad, por lo que la exposición de servicios y el control sobre activos descubiertos permanecen como áreas relevantes de seguimiento. También persisten eventos relacionados con vulnerabilidades críticas o altas, tanto internas como externas, aunque con una tendencia descendente frente al período anterior.

Los eventos de High Persistency Detection y cambios en la disponibilidad de los sistemas mantienen presencia durante el mes, lo que evidencia la necesidad de continuar correlacionando la actividad de seguridad con el comportamiento operativo de la infraestructura.

En términos generales, junio presenta una menor presión operacional, pero mantiene patrones similares a los observados previamente, con mayor concentración en exposición perimetral, descubrimiento de activos y gestión de vulnerabilidades.

**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.

