TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

August 18, 2026

Organo Judicial 08/18/2026

TLP AMBER CISO
EXECUTIVE REPORT

Este informe corresponde "EDIT MONTH" 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 el período evaluado no se identificaron amenazas activas asociadas a los activos vulnerables monitoreados. Aunque permanecen vulnerabilidades en los entornos interno y externo, los controles de seguridad implementados continúan reduciendo la exposición observada, manteniendo el Riesgo Real dentro de un nivel bajo.

Accepted Risk

n/a

el análisis continúa realizándose con base en el Riesgo Real identificado y en las mejores prácticas de ciberseguridad aplicables.

Confidence

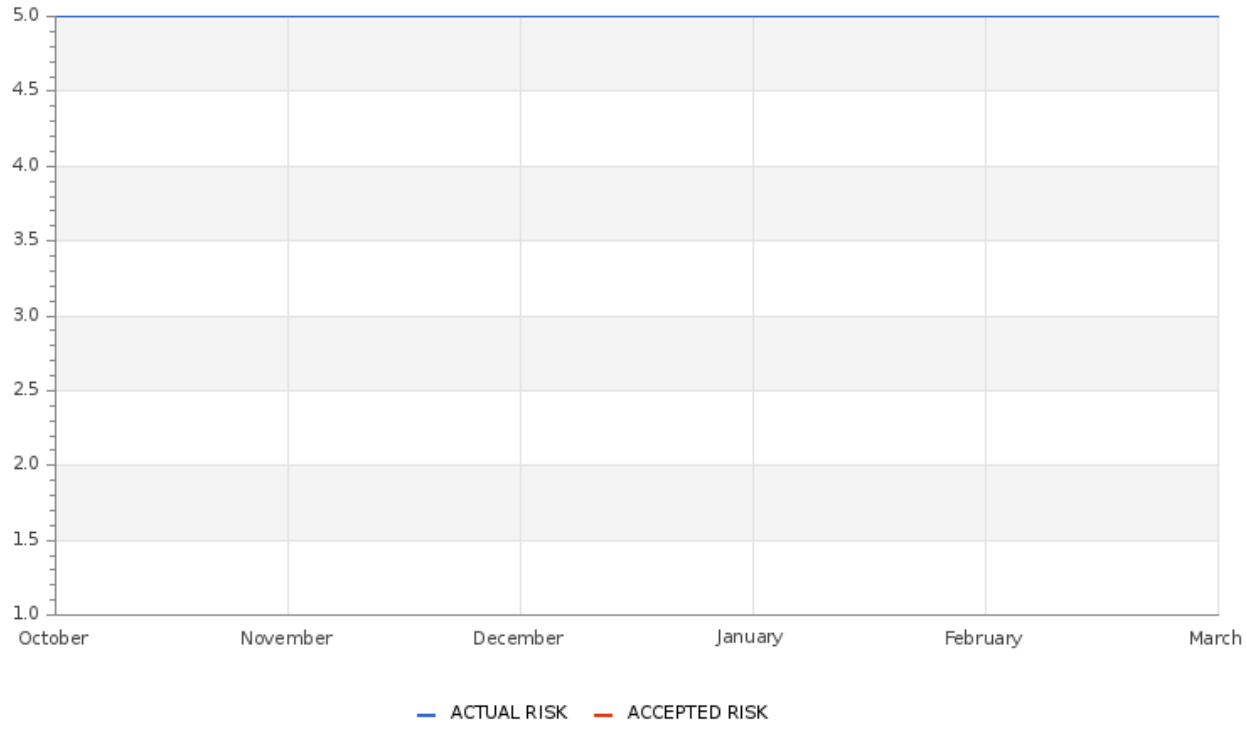
Low

El nivel de confianza de la evaluación se mantiene en Low, sin cambios respecto al período anterior, debido a que la visibilidad del entorno continúa siendo parcial y no se dispone de una integración completa de todas las fuentes de información necesarias para realizar una evaluación integral del riesgo.

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

Organo Judicial 08/18/2026

Accepted & Actual Risk



Durante mayo de 2026, los indicadores de Actual Risk y Accepted Risk se mantuvieron sin variaciones respecto al período anterior, por lo que no se identificaron cambios relevantes en el nivel de riesgo representado en el dashboard.

La actividad observada continúa asociada principalmente a intentos de acceso y reconocimiento sobre servicios expuestos, especialmente tráfico dirigido a servicios web y otros activos publicados. Los controles de seguridad implementados continúan mitigando gran parte de esta actividad, manteniendo bajo control la exposición identificada.

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 (5%):
Durante el período evaluado, el nivel actual de riesgo se mantuvo en 5%, sin variación respecto al mes anterior. Este comportamiento refleja estabilidad en la exposición identificada y no evidencia un incremento del riesgo durante el período. Se recomienda mantener el monitoreo continuo y el seguimiento de los hallazgos que puedan generar cambios en este indicador.

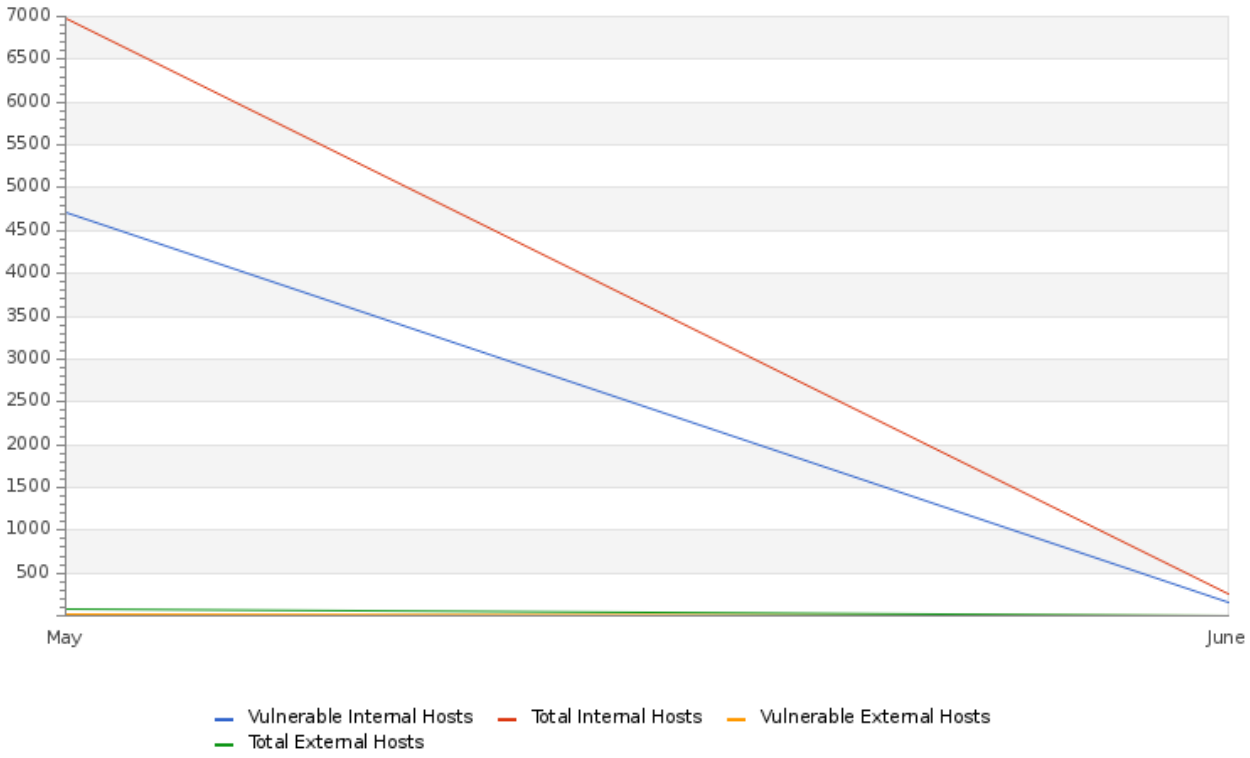
Riesgo Aceptado (0%):
El valor de riesgo aceptado se mantuvo en 0%, sin cambios respecto al período anterior.

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

Organo Judicial 08/18/2026

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



Entre marzo y mayo de 2026, la cantidad de hosts evaluados y vulnerables presentó variaciones dentro de la infraestructura interna. En marzo se identificaron 5,061 hosts vulnerables de 7,186 evaluados, representando el mayor volumen del período analizado.

Durante abril se observó una disminución, con 4,484 hosts vulnerables de 6,063 evaluados. Posteriormente, en mayo la cantidad de activos evaluados aumentó a 6,975 hosts, de los cuales 4,715 presentaron vulnerabilidades, lo que representa un incremento de 231 hosts vulnerables respecto a abril.

En términos generales, luego de la reducción observada en abril, durante mayo volvió a incrementarse la cantidad de sistemas vulnerables. Por este motivo, se recomienda mantener el seguimiento continuo de estos activos y priorizar la remediación de aquellos que concentran vulnerabilidades de mayor severidad.

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

Organo Judicial 08/18/2026

Vulnerability Metric

8

Durante mayo, el Vulnerability Metric disminuyó de 9 a 8, reflejando una ligera reducción en el nivel de exposición respecto al período anterior. Aunque el indicador presenta una mejora, se mantiene la necesidad de continuar con las actividades de gestión y remediación de vulnerabilidades, especialmente sobre los activos internos donde se concentra la mayor cantidad de hallazgos.

En términos generales, la variación observada indica una mejora moderada en la postura de vulnerabilidades, sin representar todavía una reducción suficiente para disminuir la prioridad de las acciones correctivas.

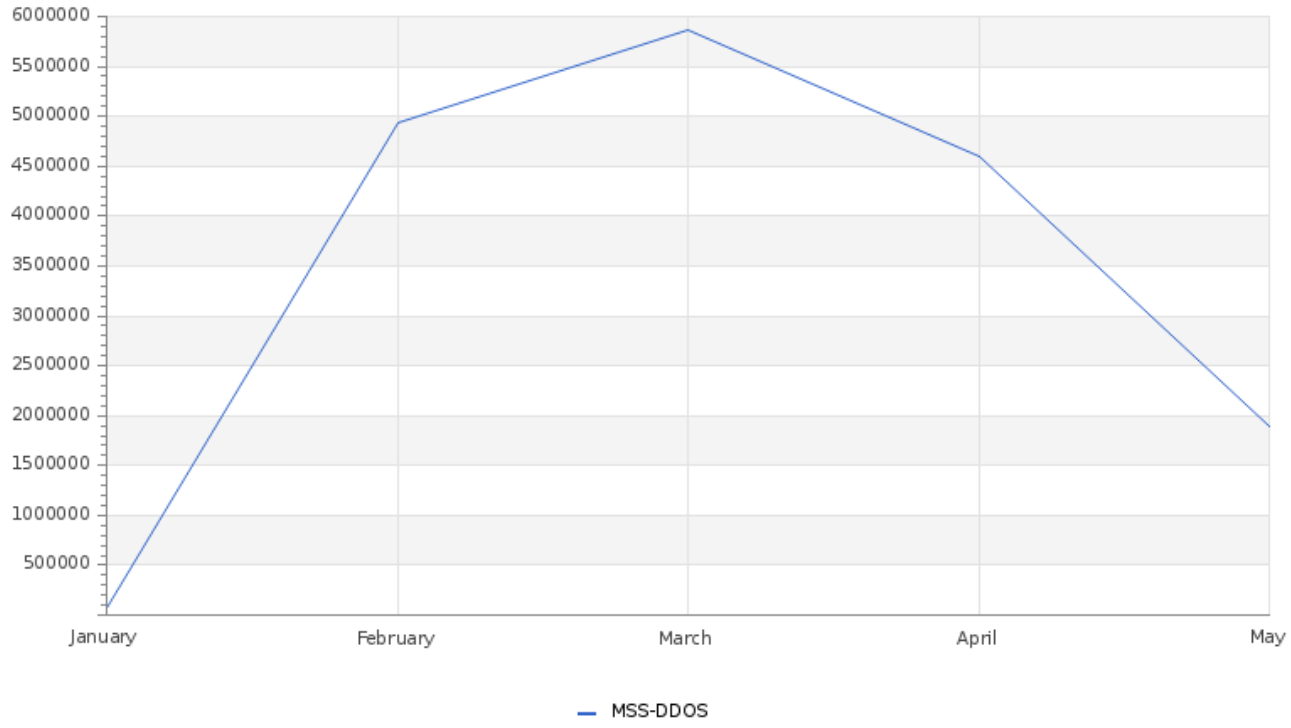
THREATS

Total Number of Successful MFA authentications per application

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

Organo Judicial 08/18/2026

Total Attacks Successfully Blocked Per Service



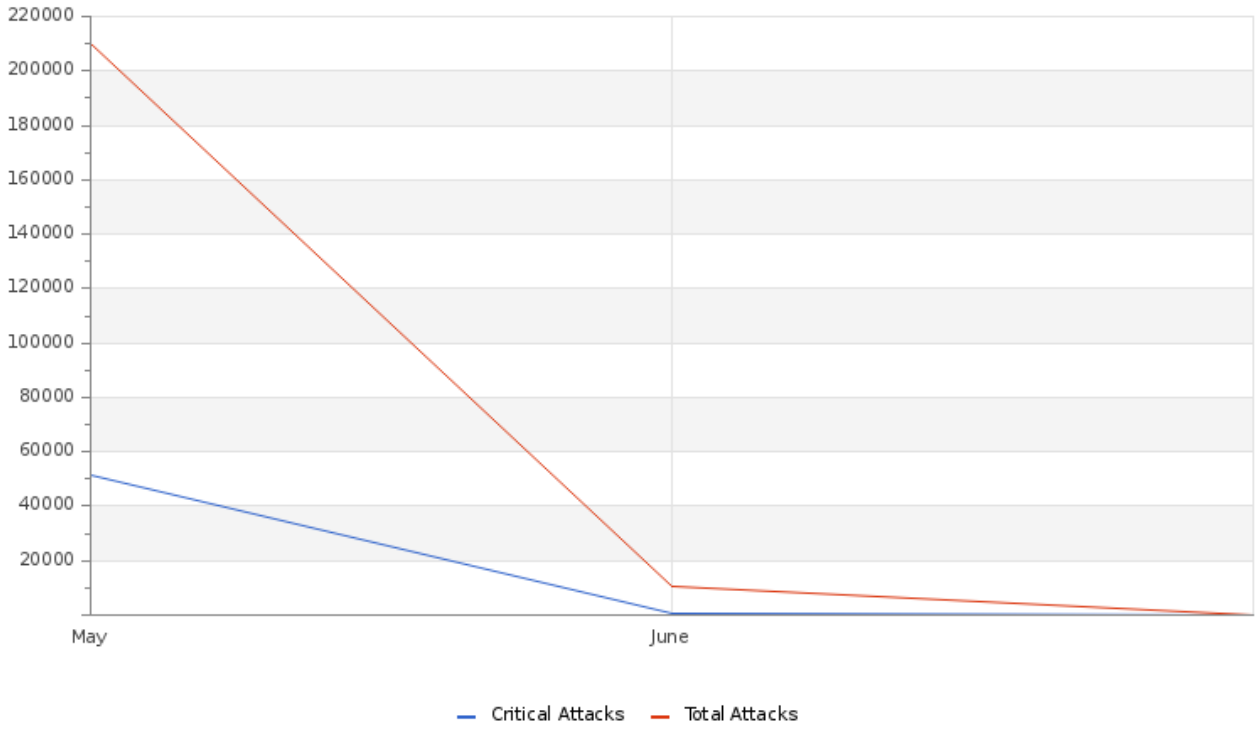
Durante el mes de Mayo se observó actividad asociada a intentos de ataques DDoS dirigidos contra los servicios expuestos de la organización. Este tipo de comportamiento continúa representando un riesgo relevante, principalmente por su capacidad de afectar la disponibilidad de recursos y servicios institucionales.

Los mecanismos de protección implementados permitieron identificar y mitigar de forma oportuna los eventos registrados, reduciendo la posibilidad de interrupciones operativas y contribuyendo a mantener la continuidad de los servicios.

En términos generales, los resultados reflejan una respuesta efectiva de los controles especializados frente a este tipo de amenazas. La actividad observada durante el período confirma la importancia de mantener capacidades continuas de monitoreo, detección y mitigación sobre los servicios expuestos a Internet, fortaleciendo así la resiliencia operativa de la organización.

Organo Judicial 08/18/2026

Attacks Successfully Blocked by Severity



La gráfica del período evaluado muestra un nivel considerable de actividad maliciosa dirigida contra la organización, incluyendo una participación relevante de eventos clasificados con severidad crítica. Durante Mayo, los controles de seguridad implementados permitieron detectar y bloquear oportunamente los intentos identificados, reduciendo la posibilidad de impacto sobre los activos y servicios institucionales.

La distribución de los eventos por severidad confirma la presencia constante de amenazas con distintos niveles de riesgo, lo que refuerza la importancia de mantener capacidades de monitoreo y protección de forma continua. La respuesta observada durante el período permitió gestionar tanto actividades críticas como eventos de menor severidad, contribuyendo a preservar la postura de seguridad de la organización.

Estos indicadores proporcionan visibilidad sobre el comportamiento y la evolución de las amenazas, facilitando la identificación de tendencias y apoyando la toma de decisiones orientadas a proteger los activos críticos, fortalecer los controles existentes y mantener la continuidad operativa.

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

Organo Judicial 08/18/2026

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	13	8
Critical Device Outages	0	0

Durante mayo, la disponibilidad de los servicios tecnológicos se mantuvo en niveles adecuados. Aunque se observó un incremento en los eventos de indisponibilidad respecto al período anterior, no se registraron interrupciones clasificadas como críticas.

Este comportamiento indica que, pese a las variaciones operativas identificadas, los servicios esenciales mantuvieron su continuidad sin afectaciones de alta severidad. Se recomienda continuar con el monitoreo de la disponibilidad y el seguimiento de los eventos recurrentes, con el objetivo de identificar posibles patrones, reducir interrupciones y fortalecer la resiliencia operativa de la infraestructura tecnológica.

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

Organo Judicial 08/18/2026

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		8435	2026-05-02 00:02:14	2026-06-01 08:52:40
DevConsejo de Administración de la Carrera Judicial ice	HTTP Advanced	Web Servers	Down		7103	2026-05-06 15:17:31	2026-06-01 08:52:40
Sistema Integral de Gestión de Recursos Humanos	HTTP Advanced	Web Servers	Down, Warning		4543	2026-05-02 00:02:14	2026-05-17 19:29:54
www.organojudicial.gob.pa	Sitio Web Organo Judicial	200.46.13.0/26	Down, Warning		1965	2026-05-23 22:06:06	2026-06-01 08:52:40
https://www.sigerh.organojudicial.gob.pa	sigerh.organojudicial.gob.pa	Web Servers	Down, Warning		1590	2026-05-17 19:39:55	2026-05-23 21:55:59
www.organojudicial.gob.pa	HTTP	200.46.13.0/26	Down, Warning		1071	2026-05-06 04:51:01	2026-05-23 21:56:01
Consejo de Administración de la Carrera de la Defensa Pública	Ping v2	Web Servers	Down		78	2026-05-24 15:39:01	2026-05-29 15:38:13
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Down, Warning		54	2026-05-24 15:19:02	2026-05-25 00:00:02
GMSA-OJ HyperV	Ping	GMSA-OJ	Down		49	2026-05-24 15:23:32	2026-05-24 23:55:32
GMSA-OJ HyperV	HTTP	GMSA-OJ	Down		49	2026-05-24 15:23:24	2026-05-24 23:55:24
Probe Device	System Health	Organo Judicial	Warning		19	2026-05-02 09:43:33	2026-06-01 03:01:51
200.46.65.105	Ping	200.46.65.104/29	Down, Warning		5	2026-05-09 06:51:13	2026-05-23 04:09:00
Repositorio digital	HTTP Advanced	Web Servers	Warning		5	2026-05-07 23:56:58	2026-05-21 16:48:35
Gestor Documental	HTTP Advanced	Web Servers	Down, Warning		4	2026-05-08 17:04:19	2026-05-22 18:27:42
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		4	2026-05-13 19:31:30	2026-05-20 15:14:38

Durante mayo, se registraron eventos de indisponibilidad y advertencia en distintos servicios y componentes tecnológicos de la organización. La mayor concentración de actividad se observó en servicios web institucionales, destacándose la Comisión de Curadores y Auxiliares Judiciales, el Consejo de Administración de la Carrera Judicial, el Sistema Integral de Gestión de Recursos Humanos y el portal www.organojudicial.gob.pa.

También se identificaron eventos puntuales asociados a componentes de infraestructura y conectividad, incluyendo sistemas GMSA, dispositivos de monitoreo y otros servicios institucionales. A pesar de la recurrencia observada en algunos de estos recursos, no se registraron interrupciones clasificadas como críticas durante el período.

El comportamiento registrado refuerza la importancia de mantener el monitoreo continuo sobre los servicios que presentan mayor recurrencia de estados Down o Warning, con el objetivo de identificar posibles patrones, reducir afectaciones repetitivas y fortalecer la continuidad operativa de los servicios institucionales.

Organo Judicial 08/18/2026

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	0	0	2,514	0

La actividad observada estuvo relacionada principalmente con intentos dirigidos contra servicios expuestos y con eventos detectados en endpoints y otros componentes de la infraestructura. La respuesta de los controles permitió contener estas amenazas y mantener la continuidad operativa de los servicios monitoreados.

En términos generales, los resultados obtenidos durante mayo refuerzan la importancia de mantener una estrategia de seguridad basada en múltiples capas de protección, combinando capacidades de prevención, detección y respuesta que permitan reducir el impacto potencial de nuevas amenazas y fortalecer la postura de seguridad de la organización.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Critical Perimeter Attacks	538
Non Baselined Discovered System	514
High Persistency Detection	100
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	95
Change in Systems Availability	57
Change in Systems Performance	246
Change in External High or Critical Vulnerabilities	69
Monitoring for open ports	11
Notable Event Alert: Endpoint Configuration Management High Priority Event	3
Targeted Campaign Alignment	8
Notable Event Alert: Vulnerability exposure from Threat Intelligence	3

los eventos relacionados con Critical Perimeter Attacks y Non Baselined Discovered System continúan concentrando la mayor parte de la actividad, lo que mantiene como áreas prioritarias la supervisión de los servicios expuestos y el control sobre activos incorporados o detectados fuera de la línea base establecida.

También se mantiene una actividad relevante vinculada al rendimiento y disponibilidad de los sistemas, así como a cambios en vulnerabilidades críticas o altas de la infraestructura interna y externa. En conjunto, el comportamiento del período refleja una menor presión operacional, pero sin eliminar la necesidad de mantener seguimiento sobre la exposición perimetral, el descubrimiento de activos y la evolución de las 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.**

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