TLP:AMBER

BOARDROOM EXECUTIVE REPORT

MIBUS

March 19, 2026

MIBUS 03/19/2026

TLP AMBER BOARDROOM

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.

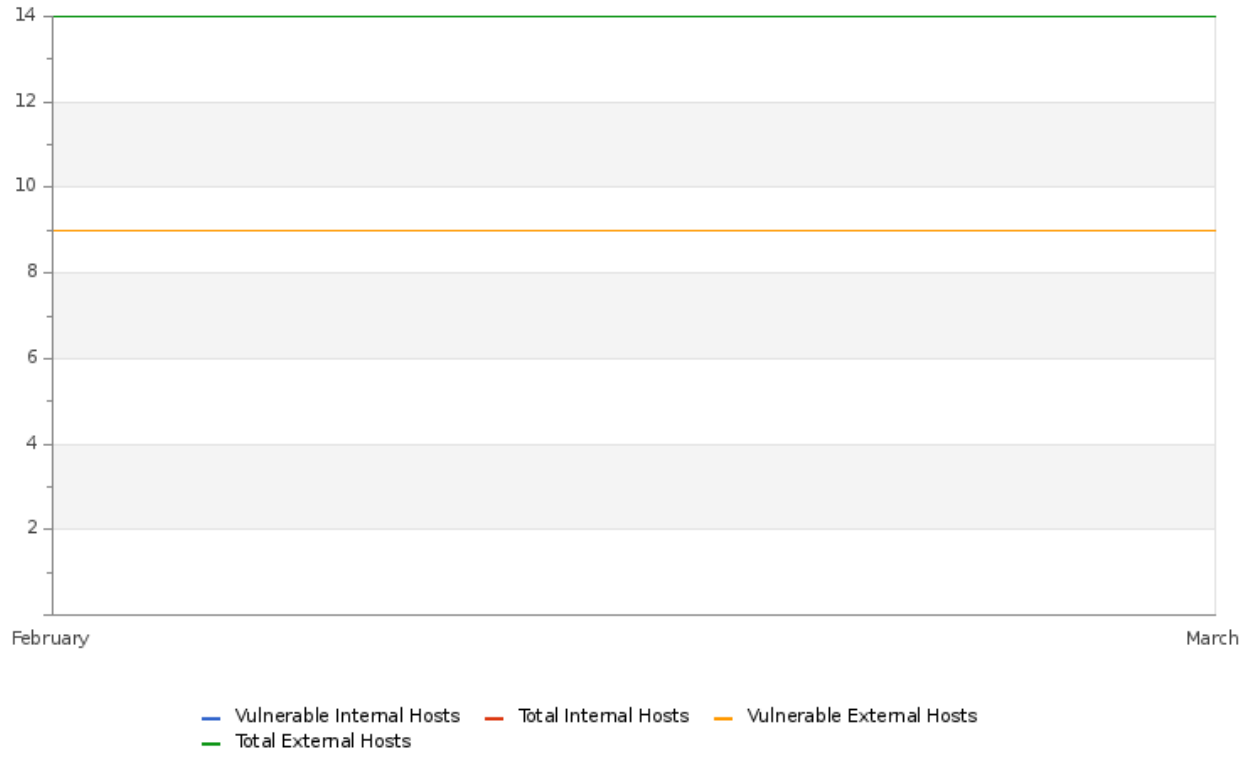
SOBRE ESTE INFORME

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.

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

MIBUS 03/19/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de febrero se identificaron un total de 14 hosts externos dentro del alcance evaluado, de los cuales 9 presentan vulnerabilidades.
Este resultado refleja que una parte importante de los activos expuestos mantiene condiciones que podrían representar un riesgo para la organización, especialmente si son identificadas y aprovechadas por actores maliciosos.
A nivel general, los hallazgos están asociados principalmente a configuraciones de seguridad que pueden mejorarse, así como a mecanismos de protección que no se encuentran completamente actualizados. Aunque no todos los casos representan un riesgo crítico de forma individual, en conjunto incrementan la superficie de exposición del entorno.
En este sentido, resulta clave continuar con el monitoreo constante de los activos externos y priorizar la corrección progresiva de estas condiciones, con el objetivo de reducir el nivel de exposición y fortalecer la postura de seguridad de la organización.

Total Attacks Successfully Blocked

782

El análisis de la distribución de los intentos de ataque durante el mes de febrero, detectados a través del servicio MSS-WAF-CLOUD, permite observar la variedad de actividades maliciosas dirigidas a las aplicaciones expuestas.
Una parte importante de estos eventos corresponde a tráfico no clasificado o de origen desconocido, acompañado de otros intentos asociados a la explotación de aplicaciones, accesos no autorizados y manipulación de solicitudes.
Este comportamiento refleja un entorno dinámico en el que múltiples tipos de ataque se presentan de forma constante

MIBUS 03/19/2026

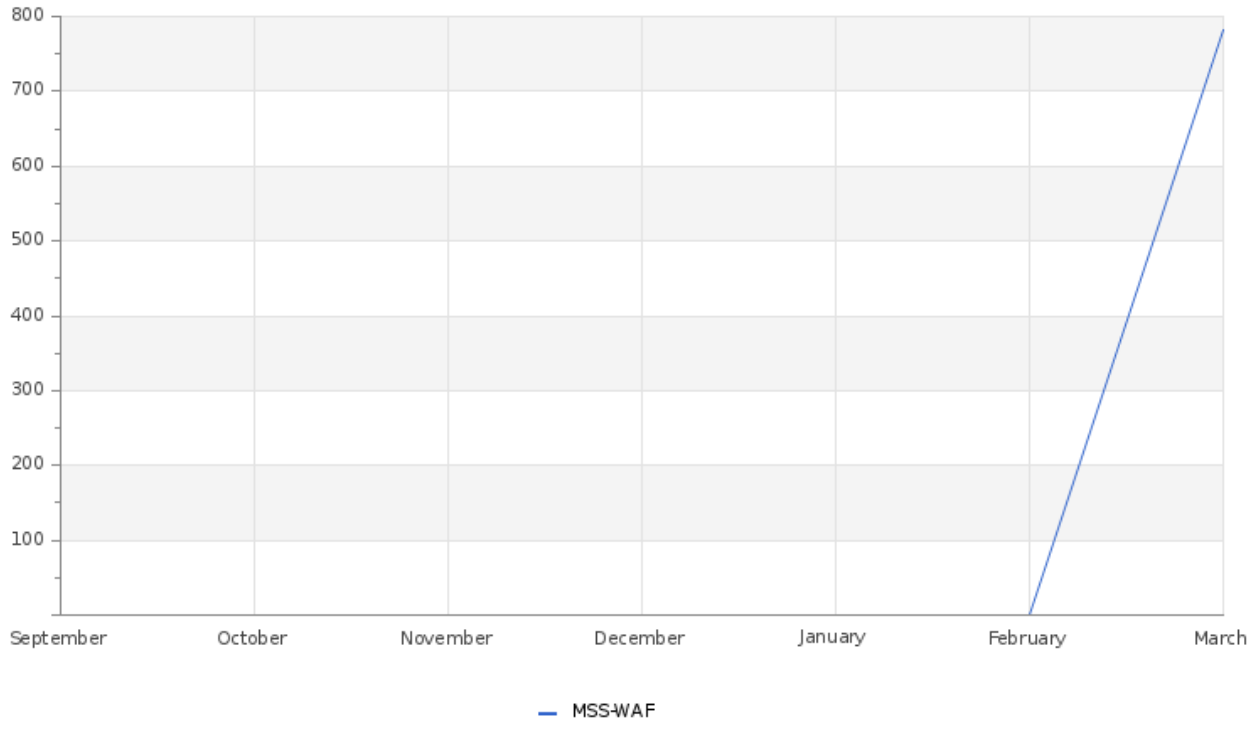
Critical Attacks Successfully Blocked

782

Durante el mes de febrero se bloquearon 782 ataques clasificados como de alto impacto, detectados a través del servicio MSS-WAF-CLOUD.

Este resultado evidencia la exposición constante a amenazas relevantes; sin embargo, los mecanismos de protección permitieron contener estos eventos de forma efectiva, evitando posibles afectaciones a las aplicaciones y servicios. La mitigación de este tipo de actividad refuerza la importancia de mantener controles activos y un monitoreo continuo del entorno.

Attacks Successfully Blocked



La gráfica correspondiente al mes de febrero muestra el comportamiento de los ataques críticos que fueron detectados a través del servicio MSS-WAF-CLOUD.
Durante este período se registraron 782 eventos de este tipo, evidenciando la presencia de intentos de ataque dirigidos a las aplicaciones expuestas, los cuales fueron mitigados de manera efectiva por los mecanismos de protección implementados, evitando posibles impactos en la disponibilidad e integridad de los servicios.

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

MIBUS 03/19/2026

Vulnerability Metric

6

El análisis del Vulnerability Metric registrado en la organización durante el mes de febrero presenta una ponderación de 6, lo que corresponde a un nivel de riesgo medio dentro del entorno evaluado. Este resultado se encuentra asociado a la identificación de 9 hosts vulnerables durante el período analizado.
Este comportamiento indica la presencia de vulnerabilidades que pueden representar un nivel de exposición relevante para la infraestructura, por lo que resulta importante mantener acciones de seguimiento y remediación orientadas a su reducción.
En este sentido, se recomienda continuar con el monitoreo constante del entorno, con el objetivo de disminuir progresivamente la superficie de exposición y fortalecer la postura de seguridad de la organización.

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

BOARDROOM 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