**Ahora más que nunca, los modelos de seguridad Zero Trust son vitales en América Latina**

**Octubre de 2025 –** Este octubre marca el vigésimo año consecutivo de la celebración del Mes de la Concientización sobre Ciberseguridad, lo que hace muy oportuno recordar la importancia de adoptar una arquitectura de confianza cero (Zero Trust).

Desde la pandemia, cada vez más empresas en América Latina han adoptado el trabajo remoto, los servicios en la nube y una mayor digitalización. Aunque esto representa un avance positivo en términos de productividad, también ha ampliado la superficie de ataque de estas compañías.

Dicha ampliación, combinada con una infraestructura de ciberseguridad aún en desarrollo y una escasez de profesionales calificados, ha dado lugar a una avalancha de ataques a la infraestructura tecnológica en toda la región. De hecho, según el Informe Anual del [LatAm Cyber Summit](https://latam.cs4ca.com/wp-content/uploads/LatAm-Cyber-Summit-2024-Annual-Report.pdf), actualmente se reportan más de 1.600 ciberataques por segundo en América Latina. Brasil, México y Colombia son los más afectados, aunque todos los países de la región sufren las consecuencias.

En resumen, las nuevas presiones regulatorias, los sistemas de seguridad obsoletos y la falta de talento especializado han creado una tormenta perfecta en América Latina. Es momento de adoptar, sin demora, la arquitectura de confianza cero.

**Nuevas presiones regulatorias**

Desde que el Reglamento General de Protección de Datos (GDPR) de la Unión Europea entró en vigor en mayo de 2018, una serie de leyes de protección de datos similares han sido promulgadas en América Latina.

La Lei Geral de Proteção de Dados ([LGPD](https://insights.manageengine.com/privacy-compliance/brazil-data-privacy/)) de Brasil entró en vigor en septiembre de 2020; la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) de México comenzó a aplicarse en marzo pasado; y la nueva Ley de Protección de Datos Personales N.º 21.719 de Chile estará plenamente vigente en diciembre de 2026. Además, Perú, Uruguay, Argentina y Costa Rica también cuentan con leyes de protección de datos —ya en vigor o próximas a entrar en aplicación—.

Estas nuevas normativas están transformando la manera en que muchas empresas perciben la ciberseguridad. Más allá del daño reputacional, la pérdida de datos sensibles o los costos operativos, las compañías con debilidades en su postura de seguridad ahora enfrentan fuertes sanciones si sufren brechas y manejan incorrectamente los datos de sus clientes. Por ello, resulta esencial que cuenten con una gobernanza de datos adecuada, una gestión de riesgos efectiva y planes sólidos de respuesta ante incidentes.

**Sistemas obsoletos**

Aunque varios países latinoamericanos —como Brasil, México, Colombia y Chile— están mejorando rápidamente su infraestructura tecnológica para hacer frente a las amenazas emergentes, otros aún dependen de sistemas de TI obsoletos.

Muchos de estos sistemas heredados usan software anticuado que no soporta autenticación multifactor, cifrado ni monitoreo de amenazas en tiempo real. Además, numerosas organizaciones carecen de planes adecuados de recuperación ante desastres y respuesta a incidentes, lo que incrementa su exposición a ransomware, ataques a la cadena de suministro y filtraciones de datos.

En países como Argentina y Brasil, los sistemas tecnológicos del sector público dependen excesivamente de estas plataformas antiguas. Para agravar la situación, muchas entidades gubernamentales y hospitales públicos manejan información altamente sensible, lo que incrementa el riesgo.

**Una gran escasez de talento en ciberseguridad**

Actualmente, muchos países latinoamericanos enfrentan una falta crítica de profesionales en ciberseguridad. Según el [Cybersecurity Workforce Study](https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen) del año pasado de ISC2, México y Brasil juntos presentan una escasez de más de 328.000 especialistas. El LatAm Cyber Summit Annual Report eleva esta cifra a 516.000 personas. En cualquier caso, el déficit es significativo, especialmente en México y Brasil.

Esta carencia dificulta que las empresas detecten amenazas, cumplan con las nuevas regulaciones y protejan los datos dentro de sus organizaciones.

**La solución: adoptar la arquitectura Zero Trust**

Dada la creciente superficie de ataque en América Latina, es fundamental que las organizaciones mantengan sus operaciones libres de violaciones de datos y ciberataques. La forma más efectiva de hacerlo es mediante la adopción de una infraestructura Zero Trust, en la que todos los usuarios, dispositivos y entidades que intenten acceder a la red corporativa se consideren no confiables por defecto.

El acceso solo debe otorgarse una vez que la identidad del usuario, dispositivo o entidad haya sido verificada y autenticada.

Además del principio “nunca confíes, siempre verifica”, Zero Trust implica un monitoreo continuo del tráfico de red, así como del comportamiento de usuarios y entidades. Todos los usuarios deben regirse bajo el principio del menor privilegio, es decir, solo tener acceso al mínimo necesario para cumplir sus tareas y por el tiempo indispensable.

Aunque no es un componente central del modelo, también se recomienda aplicar la minimización de datos: recolectar, procesar y almacenar únicamente la información estrictamente necesaria. Esto ayuda a reducir la superficie de ataque, fortalecer el cumplimiento normativo y alinear la estrategia Zero Trust con las nuevas leyes de protección de datos.

**Conclusiones**

Según el[Informe del Banco Mundial](https://openknowledge.worldbank.org/server/api/core/bitstreams/719698c9-b21b-4dd4-a875-bfc34b2961ce/content) sobre Economía de la Ciberseguridad en Mercados Emergentes, América Latina es la región del mundo con mayor crecimiento en ciberataques reportados: ha experimentado un aumento anual del 25% en la última década. Además, es la región menos protegida, con una puntuación promedio de [10,2 sobre 20](https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe) en ciberseguridad.

Esta situación, agravada por la falta de talento especializado, las nuevas presiones regulatorias y una infraestructura aún en desarrollo, hace que sea más urgente que nunca para las organizaciones en América Latina adoptar el modelo Zero Trust.

**Acerca de ManageEngine**

ManageEngine es la división de gestión de TI empresarial de Zoho Corporation. Las empresas establecidas y emergentes -incluyendo 9 de cada 10 organizaciones de la lista Fortune 100- confían en las herramientas de gestión de TI en tiempo real de ManageEngine para asegurar un rendimiento óptimo de su infraestructura de TI, incluyendo redes, servidores, aplicaciones, puntos finales y más. ManageEngine tiene oficinas en todo el mundo, incluyendo los Estados Unidos, los Emiratos Árabes Unidos, los Países Bajos, la India, Colombia, México, Brasil, Singapur, Japón, China y Australia, así como más de 200 socios globales para ayudar a las organizaciones a alinear estrechamente su negocio y TI. Para más información, visite [manageengine.com/latam](https://www.manageengine.com/latam/), siga el [blog de la empresa](http://blogs.manageengine.com/espanol) y conéctese en [Instagram](https://www.instagram.com/manageenginela/), [LinkedIn](https://www.linkedin.com/showcase/manageengine-latam/about/), [Facebook](https://www.facebook.com/ManageEngineLA/) y [Twitter](https://twitter.com/ManageEngineLA).