eBook

datto
A Kaseya COMPANY

Cómo fortalecer la ciberseguridad de tu empresa en América Latina

Una ola de ciberataques está recorriendo América Latina. Esta guía analiza los desafíos únicos que enfrentan las empresas en la región y ofrece estrategias prácticas para que los equipos de TI y los profesionales de TI fortalezcan sus defensas. Desde comprender cómo la inteligencia artificial está transformando el panorama de amenazas hasta adoptar herramientas más inteligentes y unificadas como las de Datto, aquí encontrarás pasos concretos para aumentar la resiliencia sin complicar tus operaciones.

El panorama de la ciberseguridad en América Latina

América Latina es una de las regiones más atacadas del mundo, con más de 1.600 ciberataques reportados cada segundo. A medida que la digitalización avanza en la región, los atacantes no se quedan atrás. Lo que antes afectaba solo a grandes corporaciones y entidades gubernamentales, hoy alcanza también a escuelas, hospitales y pequeñas empresas, que muchas veces no cuentan con los recursos necesarios para responder eficazmente.

Según el Informe *Anual del LatAm Cyber Summit 2024*:

- El ransomware es la principal amenaza y ya no se limita a grandes empresas.
- Brasil, México y Colombia son los países con mayor volumen de ataques.
- Los sectores más atacados son el gobierno (31 %), la manufactura (12 %) y el comercio (11 %).

La tormenta perfecta

Infraestructura débil, bajo nivel de conciencia en ciberseguridad y supervisión limitada han dejado la puerta abierta para los atacantes.

Factores que hacen vulnerable a América Latina

Tras la pandemia, miles de empresas en América Latina migraron al entorno digital de un día para otro, muchas veces sin contar con las herramientas ni la orientación adecuadas. El trabajo remoto, las aplicaciones en la nube y los servicios digitales se volvieron la norma, pero todo se construyó sobre sistemas obsoletos.

Hoy en día, esa transición apresurada sigue dejando huella:

- Muchas empresas aún operan con un **modelo break-fix,** reaccionando solo cuando algo falla, en lugar de construir resiliencia desde el inicio.
- Dependen de **antivirus básicos y hardware antiguo,** sin automatización ni visibilidad real de lo que ocurre en la red.
- **La seguridad suele estar fragmentada**, a cargo de equipos de TI sobrecargados… o, en algunos casos, no se gestiona en absoluto.
- **El error humano sigue siendo uno de los puntos más débiles**: los usuarios reutilizan contraseñas, hacen clic en enlaces sospechosos y no siempre detectan un correo de phishing, incluso cuando es evidente.

Además, América Latina **carece de un estándar unificado en ciberseguridad** como el que existe en Estados Unidos o la Unión Europea. Sin políticas claras ni incentivos, la seguridad suele pasar a segundo plano, especialmente en pequeñas y medianas empresas que ya operan con presupuestos ajustados.

Las pequeñas y medianas empresas también están en la mira

Con menos recursos y defensas más débiles, las pequeñas y medianas empresas (PYMEs) se han convertido en blancos fáciles para ataques automatizados y a gran escala. Muchas creen que son demasiado pequeñas para llamar la atención, pero en realidad, son mucho más fáciles de vulnerar.

Cómo fortalecer tus defensas

Con las herramientas adecuadas y un enfoque estratégico, incluso los equipos de TI más reducidos pueden construir defensas sólidas y prácticas. Comienza con estos tres pasos fundamentales:

Paso 1: Fortalece tu postura de seguridad en toda la organización

Ve más allá del antivirus. Aplica un enfoque por capas para proteger tus endpoints, usuarios y redes. El objetivo es detectar y bloquear amenazas en diferentes niveles.

Paso 2: Pasa de una gestión reactiva a una gestión proactiva de amenazas

Implementa herramientas y políticas que monitoreen actividades inusuales. Ten un plan de respuesta ante incidentes listo para actuar. No esperes a que algo falle para reaccionar.

Paso 3: Protege tus operaciones contra la pérdida de datos y el tiempo de inactividad

Hacer respaldos ya no es opcional. Todo dispositivo que almacene datos valiosos debe contar con copias de seguridad, y estas deben probarse con regularidad.

Descubre en esta guía los 10 consejos prácticos que toda empresa en América Latina debe seguir para reforzar su seguridad de TI.

La inteligencia artificial en ciberseguridad: un arma de doble filo

La inteligencia artificial (IA) es un arma de doble filo. Está ayudando a los atacantes a ser más rápidos e ingeniosos, pero también les da a los profesionales de TI una oportunidad real de contraatacar. La clave está en saber cómo hacer que la IA trabaje a tu favor.

Cómo usan la IA los atacantes

Los ciberdelincuentes están aprovechando la IA para operar de forma más rápida y eficiente. Entre sus tácticas se encuentran:

- Generadores de phishing que crean correos falsos convincentes en segundos.
- Escáneres automatizados para detectar vulnerabilidades en redes.
- Bots que imitan el comportamiento humano para pasar desapercibidos y evitar ser detectados.

Estas herramientas hacen que las amenazas sean más difíciles de identificar y detener.

Cómo pueden usar la IA los equipos de TI

La IA es una herramienta poderosa para los profesionales de TI. Ya sea integrada en una plataforma de monitoreo y gestión remota (RMM) o conectada a tus soluciones de seguridad, puede ayudarte a:

- Detectar comportamientos inusuales en los dispositivos antes de que se conviertan en un problema grave.
- Priorizar qué sistemas necesitan parches según el nivel de riesgo real.
- Automatizar la clasificación de tickets e incluso sugerir soluciones para resolverlos más rápido.
- Aislar automáticamente los dispositivos comprometidos para evitar que la amenaza se propague.
- Generar alertas inteligentes que prioricen los incidentes críticos y reduzcan los falsos positivos.

Para los equipos pequeños con recursos limitados, la IA puede eliminar el ruido, ofrecer mayor visibilidad y detener las amenazas antes de que causen daños.

Cómo funciona la seguridad en capas

La seguridad en capas funciona como una red de protección con múltiples puntos de control, cada uno diseñado para detener lo que el anterior podría haber pasado por alto. Así es como se ve en un escenario real:

Un empleado hace clic en un enlace de phishing.

- **El antivirus (AV)** es la primera línea de defensa. Si el archivo es una amenaza conocida, se bloquea de inmediato.
- **Si el archivo logra pasar**, entra en acción la solución de detección y respuesta en endpoints (EDR), que monitorea el comportamiento. Si el archivo empieza a actuar de forma sospechosa, como intentar acceder a datos sensibles o elevar privilegios, el EDR aísla el dispositivo para evitar que la amenaza se propague.
- Luego entra en juego **la detección y respuesta gestionada (MDR).** Expertos en ciberseguridad monitorean alertas 24/7. Si detectan algo fuera de lo común, investigan y contienen la amenaza en tiempo real por ti.
- Y si a pesar de todo el ataque logra causar daño, **la copia de seguridad de endpoints** garantiza que puedas recuperar tus datos rápidamente: sin pagar rescate, sin tiempos de inactividad, sin empezar desde cero.

Cada capa refuerza la anterior, creando un sistema de defensa completo y preparado para cualquier amenaza. Así es como debe funcionar una protección moderna.

Por qué funciona la seguridad en capas

Las amenazas modernas no se detienen ante el primer obstáculo. Por eso, una sola línea de defensa, como un antivirus, ya no es suficiente. Toma como ejemplo el ransomware. Ya no se limita a bloquear tus archivos; ahora también busca eliminar tus respaldos.

Si eso sucede, la recuperación se vuelve mucho más difícil, y pagar el rescate puede parecer la única salida.

Y no son solo hackers expertos los que están detrás de estos ataques. Con el modelo de Ransomware como Servicio (RaaS), cualquier persona puede lanzar un ataque, incluso sin conocimientos técnicos. Por una pequeña suma, los ciberdelincuentes pueden comprar kits de ransomware listos para usar en internet, con todo incluido: soporte al "cliente", paneles de control y herramientas de pago. Solo se necesita una tarjeta de crédito y malas intenciones.

Ahora, si a eso le sumamos malware potenciado por inteligencia artificial, capaz de adaptarse y propagarse rápidamente, queda claro por qué las defensas tradicionales ya no son suficientes.

Cómo ayuda Datto a proteger a las empresas en América Latina

La mayoría de las herramientas de seguridad no fueron diseñadas para equipos de TI pequeños. Muchas empresas se ven obligadas a comprar soluciones por separado — como antivirus, EDR y respaldo — de distintos proveedores, lo que complica la gestión y el soporte de la seguridad.

Datto ofrece antivirus avanzado, EDR, MDR y respaldo en una sola solución. Como todas las herramientas están diseñadas para trabajar de forma integrada, obtienes un sistema de seguridad completo, más fácil de administrar y con una protección más fuerte y confiable justo cuando más la necesitas.

Esto es lo que Datto integra en una única plataforma:

- **Prevención inteligente de amenazas:** Datto AV utiliza inteligencia artificial, aprendizaje automático y datos de inteligencia global para bloquear automáticamente amenazas, incluyendo malware polimórfico y ataques de día cero.
- **Eliminación de amenazas avanzadas:** La detección basada en comportamiento de Datto EDR permite identificar y detener amenazas sofisticadas que se esconden detrás de programas legítimos, como PowerShell.
- **Detección rápida de ransomware:** Nuestro motor propietario de detección de ransomware interrumpe de inmediato el proceso de cifrado de archivos y aísla el dispositivo en segundos para detener el ataque antes de que se propague.
- **Expertos en ciberseguridad 24/7:** Las amenazas evolucionan constantemente, pero con el servicio MDR de Datto, cuentas con monitoreo, detección y respuesta continua, liderados por especialistas en ciberseguridad.

Un trío poderoso

Cuando se combina con Datto EDR, Datto AV detecta y detiene el **99.62 %** de todo el malware, creando una combinación poderosa y fácil de usar para la detección de amenazas.

Y si sumas Datto MDR, cuentas con expertos vigilando tu sistema. Nuestros profesionales en ciberseguridad monitorean tu entorno 24/7, analizan alertas, buscan amenazas activamente y responden en tiempo real.

Gracias a la combinación de herramientas avanzadas e intervención humana experta, Datto ofrece una seguridad en capas inteligente, eficiente y preparada para enfrentar los desafíos del mundo real.

Agenda hoy mismo tu demostración de Datto.

Acerca de Datto

Datto es un proveedor líder global de soluciones de software de seguridad y en la nube diseñadas específicamente para proveedores de servicios administrados (MSPs). Datto, una empresa de Kaseya, cree que no hay límites para lo que las pequeñas y medianas empresas (PYMES) pueden lograr con la tecnología adecuada. Las comprobadas soluciones de Datto en Continuidad Unificada, Redes, Gestión de Endpoints y Gestión Empresarial impulsan la ciberresiliencia, la eficiencia y el crecimiento de los MSPs.Ofrecidas a través de una plataforma integrada, las soluciones de Datto ayudan a su ecosistema global de socios MSP a atender a más de un millón de empresas en todo el mundo. Desde la detección proactiva y dinámica hasta la recuperación rápida y flexible frente a incidentes cibernéticos, las soluciones de Datto defienden contra el costoso tiempo de inactividad y la pérdida de datos en servidores, máquinas virtuales, aplicaciones en la nube o cualquier lugar donde residan los datos.Desde su fundación en 2007, Datto ha recibido numerosos premios por la excelencia de sus productos, su soporte técnico superior y su rápido crecimiento, así como por fomentar un entorno laboral excepcional. Con sede en Miami, Florida, Datto cuenta con oficinas globales en Norwalk, Connecticut, así como en Australia, Canadá, Dinamarca, Alemania, Países Bajos y el Reino Unido.

datto
A Kaseya COMPANY