

El costo de un clic: Por qué el phishing sigue venciendo a la inteligencia artificial en LATAM



52% de las empresas en LATAM sufrió ciberataques en 2026

Según el ESET Security Report 2026, más de la mitad de las organizaciones en la región fue víctima de incidentes de ciberseguridad este año. Y el dato que debería preocupar a toda la junta directiva: **73% de estos ataques comenzó con phishing.**

Fuente: enfasys

No fue ransomware avanzado. No fue un hackeo de película.

Fue un correo que parecía legítimo, un enlace que generaba confianza, un adjunto que no levantó sospechas.

Mientras las organizaciones en LATAM aceleran su transformación digital, adoptan IA y migran a la nube, **la puerta de entrada sigue siendo la misma de hace 20 años: el factor humano.**

El contexto que importa:



El phishing se mantiene como el vector de ataque #1 en la región.



Sectores más afectados: financiero, retail, salud y servicios profesionales.



El costo promedio de un incidente incluye: tiempo de inactividad, pérdida de datos, multas regulatorias y daño reputacional.

La pregunta incómoda pero necesaria:

¿Tu plan de continuidad del negocio incluye un protocolo real de respuesta a ciberataques?

Porque cuando el sistema cae:

- No hay IA que funcione.
- No hay automatización que salve el día.
- No hay productividad que mantener.

Solo hay tiempo perdido, clientes sin servicio, datos comprometidos y una reputación que puede tardar años en recuperarse.

Tres acciones que separan a las empresas preparadas de las vulnerables:

Capacitación continua

No basta con un taller anual. El phishing evoluciona cada mes.

Simulacros reales

Prueba a tu organización con correos de phishing controlados. Los resultados suelen sorprender.

Plan de respuesta documentado y probado

¿Quién decide? ¿Quién comunica? ¿Quién contiene el daño? Si la respuesta es “lo vemos cuando pase”, ya es tarde.

La ciberseguridad ya no es un tema exclusivo de TI. Es un tema de gestión de riesgos, continuidad operativa y protección del valor de la empresa.

En un momento donde la confianza digital es el activo más frágil, la pregunta no es si puedes permitirte invertir en prevención. La pregunta es: **¿puedes permitirte no hacerlo?**

¿Tu organización está realmente preparada o solo cumple checklist de compliance?

MOORE LATAM REPORT

