Kaseya®

Seguridad del correo electrónico en LATAM

El cambio con IA que no puedes ignorar

El correo electrónico sigue siendo el canal de comunicación más crítico y más explotado por las empresas de todo el mundo, y América Latina no es la excepción.

A medida que las organizaciones de LATAM aceleran su transformación digital, también están ampliando su superficie de ataque. Sin embargo, muchas aún dependen de defensas de correo electrónico obsoletas, diseñadas para amenazas predecibles y patrones de ataque estáticos.

Los atacantes de hoy operan a escala, utilizando automatización e IA generativa para elaborar mensajes convincentes y localizados, apuntando cada vez más al punto de entrada más eficiente disponible: el correo electrónico.

La IA está transformando las ciberamenazas en LATAM

Más del 80% de los correos electrónicos de phishing incluyen ahora contenido generado o asistido por IA.[1]

Los atacantes ya no dependen de campañas de phishing de plantilla única. Usando IA, generan múltiples variaciones del mismo ataque —incluyendo solicitudes de facturas, alertas de buzón de voz, mensajes de fax y confirmaciones de pago— todas desde el mismo dominio y a menudo vinculadas al mismo payload malicioso.

Cada mensaje difiere en tono, formato y diseño, lo que hace que la detección sea mucho más difícil. Este nivel de variabilidad socava los modelos de seguridad tradicionales que dependen del reconocimiento de patrones o del contenido repetido.

El problema: El phishing impulsa pérdidas financieras

El phishing es ahora el principal impulsor de pérdidas financieras; el FBI reportó un aumento de $18.7 millones en 2023 a $70 millones en 2024, un incremento del 274% en las pérdidas relacionadas con phishing.[2]

Para las pymes, el impacto es aún más grave, ya que un solo ataque exitoso de BEC o ransomware puede interrumpir el flujo de caja, retrasar los pagos a proveedores, paralizar las operaciones y dañar la confianza de los clientes.

A diferencia de las grandes empresas, muchas organizaciones de LATAM carecen de la resiliencia necesaria para absorber estos impactos. Al mismo tiempo, los sistemas de correo electrónico heredados, la experiencia interna limitada y la dependencia de proveedores externos aumentan aún más la exposición.

Lo que ha cambiado: La nueva anatomía de las amenazas por correo electrónico

La IA ha cambiado la economía del phishing

Los correos electrónicos de phishing generados por IA tienen una tasa de clics del 54%, en comparación con el 12% de las campañas tradicionales.[3]

La IA generativa ha eliminado las barreras de entrada. Lo que antes requería tiempo, habilidad e iteración, ahora puede producirse de forma instantánea y a escala, en múltiples idiomas y con alta precisión contextual.

La suplantación de marcas ha alcanzado nuevos niveles de realismo

Según el **Informe de Seguridad de Correo Electrónico de Kaseya**, INKY, una empresa de Kaseya, detectó más de 6.6 millones de correos electrónicos de suplantación de marcas solo en el segundo semestre de 2025. También encontró que casi 5.3 millones de correos electrónicos de phishing estaban vinculados a las 25 principales marcas.

Estos ataques replican el tono, los flujos de trabajo y la identidad visual con una precisión casi perfecta.

Las plataformas de confianza están siendo utilizadas como armas

Los atacantes incorporan cada vez más intenciones maliciosas dentro de ecosistemas legítimos, incluyendo Microsoft Teams, Power BI, plataformas de documentos en la nube, formularios en línea y herramientas de colaboración.

En lugar de dirigir a los usuarios a dominios sospechosos, los atacantes ocultan los payloads en enlaces incrustados, instrucciones de contacto alternativas y números de teléfono dentro de interfaces de confianza.

Por qué las empresas de LATAM están en mayor riesgo

Varios factores estructurales hacen que LATAM esté especialmente expuesta:

- Rápido crecimiento digital sin madurez de seguridad equivalente
- Mercado dominado por pymes, con inversión limitada en ciberseguridad
- Herramientas heredadas diseñadas para modelos de amenaza obsoletos

Al mismo tiempo, los atacantes se están adaptando. La IA ahora permite:

- Phishing altamente localizado en español y portugués
- Mensajes contextuales alineados con las prácticas comerciales regionales
- Suplantación escalable de bancos, proveedores de telecomunicaciones y plataformas SaaS ampliamente utilizadas en toda LATAM

El cambio necesario: De la seguridad reactiva a la seguridad basada en la intención

El panorama actual de amenazas exige un cambio fundamental en la forma de abordar la seguridad del correo electrónico.

De las reglas a la defensa impulsada por IA

Las reglas estáticas y la detección basada en firmas ya no son suficientes. La seguridad moderna debe aprovechar la IA para analizar patrones de comunicación, detectar anomalías de comportamiento y adaptarse continuamente a las amenazas en evolución.

De la detección a la intención

Los correos electrónicos de phishing se asemejan cada vez más a comunicaciones legítimas. La detección ya no puede basarse en palabras clave, enlaces maliciosos conocidos o patrones repetitivos. En cambio, debe centrarse en el contexto, el comportamiento y la intención.

La detección basada en la intención analiza el propósito u objetivo de un correo electrónico en lugar de basarse en la repetición de contenido o en patrones de amenazas conocidas.

Obtén el informe completo de seguridad de correo electrónico 2026

Descubre información más detallada, inteligencia sobre amenazas y cómo la solución de seguridad de correo electrónico con GenAI de Kaseya, INKY, está ayudando a las organizaciones a pasar de la seguridad reactiva a la protección basada en la intención. **Descargar** el informe completo.

¿Listo para ver cómo INKY bloquea los intentos de phishing? Solicita una demostración hoy.

Ver INKY en acción

Sources
1 https://www.brside.com/blog/ai-generated-phishing-vs-human-attacks-2025-risk-analysis
2 https://www.mikegingerich.com/blog/small-business-cybersecurity-checklist-2026-essentials/
3 https://www.brside.com/blog/ai-generated-phishing-vs-human-attacks-2025-risk-analysis

Kaseya®