



Datos, el oro invisible de la economía digital

● Los ciberataques ya no son un tema excepcional; en Latinoamérica, hasta 2 mil 800 cada semana

● Criminales consiguen suplantar, simular y engañar para que víctimas entreguen información

● La inteligencia artificial quita empleos y ahonda desigualdades laborales, alertan especialistas

JULIO GUTIÉRREZ Y JESSICA BECERRA / P 13 Y 15

EL ROBO DE INFORMACIÓN CUESTA 50 MDD AL AÑO

Datos, el oro del siglo XXI

La identidad es el botón por el que van los cibercriminales

JULIO GUTIÉRREZ

El mundo ha cambiado con la digitalización. Hoy el robo ya no se comete con pasamontañas: llega por medio de correos impecables, enlaces que aparentan ser legítimos y contratos que se firman con un clic. En términos prácticos, no necesita violencia; al ladrón virtual le basta con ganarse la confianza de una sola persona para provocar desfalcos multimillonarios.

Estudios publicados por diversas firmas especializadas en ciberseguridad lo confirman. En Latinoamérica, región en la que se incluye a México, los ciberataques y los fraudes dejaron de ser un tema excepcional.

Latinoamérica no sólo adoptó con rapidez las plataformas digitales, los pagos electrónicos o las firmas de contratos a la distancia; también asumió, sin dimensionarlo del todo, la exposición permanente a un ecosistema criminal que opera a la misma velocidad o incluso más rápido que la innovación tecnológica.

De la mano de los avances vino la inteligencia artificial (IA), una herramienta que en primera instancia llegó como un *chat* y luego comenzó a generar imágenes, videos y voces. En este momento, ahora mismo, es usada por muchos con fines positivos, pero por otros con objetivos maliciosos.

Aunque promete eficiencia, automatización y reducción de costos, la IA también permite fabricar identidades falsas con un grado de sofisticación que hace apenas unos

años parecía improbable, pero ahora es indetectable para el ojo humano.

La IA produce fotografías sintéticas, documentos alterados con precisión milimétrica y conversaciones que replican patrones humanos. La frontera entre lo auténtico y lo fabricado se volvió difusa y, en ese entorno, la identidad se convirtió en el nuevo botón por el que van los cibercriminales.

A los ciberdelinquentes ya no les basta con vulnerar servidores o extraer bases de datos completas, su objetivo es suplantar, simular y engañar con suficiente credibilidad para que la propia víctima entregue la información. Es como entregarle las llaves del hogar o del carro a un ladrón.

Ataques por todos lados

Una investigación de Docusing y Onfido exhibió que en México, más de la mitad de las empresas percibieron un aumento en los fraudes de identidad en el entorno digital, mismos que llegan a costar millones de dólares.

A inicios del siglo XX el petróleo fue considerado el oro negro. En México, al aguacate se le llama oro verde. En la economía digital del siglo XXI, los datos y su protección se han convertido en el *oro invisible*. Y como todo recurso valioso, hay quien vive de extraerlo y quien intenta robarlo.

El informe Ciberseguridad, habilitador de confianza y estabilidad, realizado por Incode y Endeavor, publicado recientemente, demostró que en 2025, las organizaciones que operan en AL enfrentaron, en promedio, 2 mil 803 intentos de ataques cada semana, mientras que el promedio global fue de mil 984.

El 68 por ciento de las empresas de la región consideran que el phis-

hing—el método de robar información por medio de correos y mensajes falsos—y la denominada ingeniería social—el arte de engañar por medio de las emociones—son las principales amenazas, por encima del secuestro de información, que se conoce como ransomware.

Según Incode y Endeavor, entre 2014 y 2023, los incidentes de ciberseguridad en la región aumentaron a una tasa anual de 25 por ciento, la más alta en todo el planeta.

"Latinoamérica se ha convertido en el epicentro global del crecimiento de incidentes cibernéticos, donde la vulnerabilidad humana y la explotación de identidades se han consolidado como los vectores de ataque predominantes. Las pérdidas financieras y la frecuencia de intentos superan ampliamente los promedios globales."

El informe menciona que en la región, 65 por ciento de las organizaciones creen que están listas para enfrentar amenazas, pero sólo 17 por ciento realiza evaluaciones continuas. Un 10 por ciento nunca ha llevado a cabo una evaluación formal.

"Sólo 17 por ciento de las organizaciones reportan sufrir ataques a diario, pero la evidencia sugiere que la frecuencia real es mucho mayor. La mayoría de los incidentes pasa inadvertida o no se registra formalmente. El 36 por ciento de las empresas cree que su gasto actual en ciberseguridad es insuficiente."

La joya de la corona

En el documento se detalla que en nuestro país, 54 por ciento de los corporativos utiliza IA para detectar y responder de forma automatizada los ataques. Sin embargo, 5 por ciento piensa que esta herramienta puede generar

más riesgos que soluciones, "cifra que probablemente subestima su amenaza real".

"La mayoría de los ataques diarios contra identidades de usuarios buscan comprometer contraseñas pero cuatro de cada 10 organizaciones mexicanas todavía dependen exclusivamente de contraseñas tradicionales."

Con los cambios en el entorno digital, la exposición de riesgos va al alza, eso es evidente no sólo para las personas, también para las empresas. Según la investigación de Docusing y Onfido, 57 por ciento de las organizaciones nacionales perciben un aumento de los fraudes de identidad en el entorno digital.

El mismo análisis sugirió que los ataques y las estafas *online* pueden generar pérdidas significativas para los consorcios, estimadas hasta en 50 millones de dólares al año, sin mencionar los impactos reputacionales y jurídicos.

"La seguridad debe entenderse como un ecosistema. La tecnología es uno de sus pilares, pero las prácticas organizacionales, los flujos de trabajo bien estructurados, además de la educación y formación continua de los usuarios, son igualmente determinantes", enfatizó Norbert Otten, director senior de soluciones de Docusing en Latinoamérica.

El informe de Incode y Endeavor concluye de forma contundente: "En conjunto, los datos permiten entender que el desafío de la ciberseguridad en México y Latinoamérica no se limita a poner en práctica nuevas tecnologías, sino a articular estrategias e invertir. De lo contrario, la región corre el riesgo de frenar su competitividad digital y limitar el potencial de un ecosistema económico que ya depende cada vez más de la confianza en entornos digitales".