La ABA destaca importancia de reforzar la cultura de prevención ante amenazas de ciberseguridad impulsadas por la inteligencia artificial

*Advirtió de los riesgos generados por deepfakes o videos falsos creados con IA con los que se intenta realizar fraudes en contra de la ciudadanía.*

**Santo Domingo, R.D. –** La Asociación de Bancos Múltiples de la República Dominicana (ABA) advirtió sobre los nuevos retos que plantea el uso de la inteligencia artificial (IA) en la evolución de los ciberdelitos, en especial los deepfakes, que se han convertido en un mecanismo de fraude y desinformación en distintos países, incluida la República Dominicana.

La ABA aseguró que la IA, utilizada en beneficio de las mejores prácticas, fortalece la detección de ataques y la protección de sistemas. Sin embargo, también ha facilitado a los ciberdelincuentes técnicas ofensivas más sofisticadas, como intentos de fraudes mediante videos y audios falsos que imitan la imagen y voz de figuras públicas, expuso.

Resaltó la circulación en el país de videos manipulados con IA, en los que se falsifica la voz e imagen de personalidades de alto perfil, con el fin de promover inversiones fraudulentas. “Este tipo de incidentes no solo afecta la reputación institucional, sino que también genera incertidumbre en la población y pone en riesgo la estabilidad económica de la ciudadanía”, planteó.

Entre las claves para distinguirlos, el gremio citó detalles como parpadeos irregulares, inconsistencias en el cuello y la cara, duración corta del video y origen dudoso. Indicó que también es importante verificar sombras, luces y sincronización audiovisual, para poder cuestionar la credibilidad de un audiovisual.

En un documento de prensa, la entidad recordó que, entre enero y junio de 2024, el Centro Nacional de Ciberseguridad (CNCS) registró más de 139 millones de intentos de ciberataques a nivel local, un dato que refleja la creciente exposición del país a amenazas digitales.

La ABA identificó entre otras amenazas más relevantes, a nivel global, los ataques de día cero, que explotan vulnerabilidades desconocidas en software o sistemas antes de que los desarrolladores puedan solucionarlas; el ransomware avanzado, con el que se amenaza con filtrar información sensible o atacar a terceros; la vulnerabilidad de dispositivos que integran internet en su funcionamiento, el riesgo en cadenas de suministro, entre otros.

La Asociación de Bancos reiteró su compromiso de educar a la ciudadanía en materia de prevención y buenas prácticas digitales, al recordar que dispone del portal Yo Navego Seguro ([yonavegoseguro.com.do](https://www.yonavegoseguro.com.do/)), a fin de orientar tanto a individuos como a empresas sobre los riesgos y ciberdelitos, así como ofrecerles recomendaciones de protección en el entorno digital.

En este sentido, el gremio llamó a mantener hábitos básicos de ciberseguridad entre los que figuran actualizar sistemas informáticos, verificar las fuentes de información, mantener contraseñas seguras y reportar anomalías a la entidad financiera u otra empresa relacionada.

**Dirección de Comunicación y Marketing**

25 de septiembre de 2025