COLUMNA DE OPINIÓN

IA generativa, banca y ciberseguridad

NICOLÁS DEINO
Director ejecutivo para la Industria Financiera de Accenture Chile

La inteligencia artificial generativa es una gran oportunidad para la reinvención de la banca. Sin embargo, al mismo tiempo, presenta riesgos de seguridad que deben ser cuidadosamente gestionados. La combinación de *deepfakes* y estafas en pagos en tiempo real está causando un aumento explosivo del fraude al consumidor a nivel global, lo que está erosionando la confianza de las personas.

La mayoría de los ejecutivos responsables de la ciberseguridad en la banca siente la presión y con razón. Cuatro de cada cinco entrevistados (80%) cree que la IA Gen empodera a los atacantes más rápidamente de lo que los bancos pueden responder, según datos de Accenture. Así también, 74% lucha por mantener la confianza digital frente a los crecientes riesgos de fraude, mientras 88% afirma que es un desafío satisfacer las demandas de experiencias fluidas de parte los clientes en todas las plataformas sin comprometer la seguridad.

Desafortunadamente, la mayoría de los bancos tiende a ver la ciberseguridad como un costo y un tema netamente de cumplimiento. Esta visión persiste a pesar de la evidencia de que una ciberseguridad robusta realmente mejora la eficiencia y ayuda a construir la confianza del cliente.

Es crucial que los bancos adopten una postura proactiva y comiencen a abordar los desafíos de seguridad de manera más anticipativa. Para lograrlo, se pueden implementar cuatro acciones fundamentales.

La primera es educar. Los bancos están cada vez más rezagados en proporcionar una comunicación efectiva a sus clientes. En una encuesta de Accenture a 1.400 clientes, 85% dijo que una comunicación clara sobre las prácticas de ciberseguridad es esencial, sin embargo, solo 28% calificó a su banco muy bien en este aspecto. La banca debería comunicar regularmente sobre medidas de seguridad, riesgos potenciales y cualquier incidente que pueda afectar los datos del cliente. También se pueden compartir estrategias para mitigar las últimas tácticas de amenazas y estafas, incluyendo videos de capacitación cortos sobre *deepfakes*, a través de sitios web, portales de clientes o aplicaciones móviles.

> "La mayoría de los bancos tiende a ver la ciberseguridad como un costo y un tema de cumplimiento. Esta visión persiste a pesar de la evidencia de que una ciberseguridad robusta realmente mejora la eficiencia y ayuda a construir la confianza del cliente".

La segunda acción clave es integrar la ciberseguridad y la seguridad operativa en el núcleo de las experiencias del cliente. Los bancos deberían incorporar más puntos de control y verificación en el proceso de pagos, para ayudar a prevenir el fraude.

En tercer lugar, es fundamental educar al personal y a todas las partes del ecosistema bancario para detectar y contrarrestar amenazas avanzadas. Más del 70% de las violaciones de datos en los bancos son causadas por terceras partes.

Finalmente, es necesario incorporar la ciberseguridad en los esfuerzos de reinvención general. Muchos ejecutivos de ciberseguridad se sienten abrumados y 83% admite que lucha por alinear las medidas de ciberseguridad con el ritmo de adopción de nuevas tecnologías. A medida que más bancos adoptan la IA Gen, necesitan contar con procesos robustos de seguridad. Esto podría significar realizar verificaciones adicionales o usar herramientas especializadas para detectar y prevenir *malware*. Esto será aún más crítico a medida que los bancos usen la IA generativa para interactuar directamente con los clientes.

Al hacer de la ciberseguridad un pilar de su estrategia, los bancos pueden impulsar tanto la confianza del consumidor como el crecimiento del negocio. Construir confianza a través de la ciberseguridad no es una opción, es esencial.