DIARIO FINANCIERO®
Fecha: 24/01/2025 Audiencia: 48.450 Sección: CONTRAPORTADA
Vpe: $6.231.664 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 83,72%

DF DIARIO FINANCIERO® DF LAB INNOVACIÓN, STARTUPS Y TRANSFORMACIÓN DIGITAL

HERNÁN ORELLANA, EXPERTO EN TRANSFORMACIÓN DIGITAL Y DIRECTOR DE BCI:

"Hay que sofisticar las herramientas de detección y prevención, pero también la capacitación"

■ El experto en transformación digital dijo que la Ley Marco de Ciberseguridad no agrega mayores requerimientos a la normativa de la CMF para la banca y que ante la evolución de las ciberamenazas la clave es generar "una cultura de ciberseguridad en la sociedad".

POR ALEJANDRA RIVERA

Los bancos son uno de los prestadores de servicios esenciales que establece la nueva Ley Marco de Ciberseguridad, que crea la Agencia Nacional de Ciberseguridad, una nueva regulación que entra en vigencia este 1 de marzo de 2025, y que establece obligaciones para las organizaciones reguladas en prevención, reporte y resolución de incidentes, y multas y sanciones en caso de incumplimiento.

En este contexto, el consultor y director de Bci, Hernán Orellana, comentó que la "preocupación real" en torno a la ciberseguridad en los directorios de la industria partió en 2020-2021 y "ha ido aumentando". "La ciberseguridad es un tema estratégico, hoy no puedes concebir la estrategia de negocios de una empresa sin ciberseguridad, sobre todo, si un banco quiere ser digital, porque sin ciberseguridad no hay estrategia digital perfecta", dijo.

Afirmó que, en el caso de la banca, la nueva regulación no agrega mayores requerimientos a los que ya contempla la RAN 20-10, la normativa sectorial que dicta la Comisión del Mercado Financiero (CMF) en términos de obligaciones y trabajo, pero sí hay una preocupación a nivel de directorios, que va más allá de lo que dice la norma, "de entender cuáles son los principales riesgos y las amenazas".

"Una vez al mes recibimos un informe que detalla las amenazas. El directorio tiene un comité específico que ve el riesgo de continuidad operacional y el riesgo tecnológico, que tiene que ver con la ciberseguridad. Hay instancias específicas que se encargan de definir la política, de que se cumpla, de hacer seguimiento mensual de lo que está pasando en el tema, preocuparse de que estén los recursos, las personas y los presupuestos necesarios para las actividades de ciberseguridad", dijo Orellana.

Amenazas con IA

Bci recibe alrededor de 10 millones de ataques al mes, la mayoría son automatizados, es decir, no es un *hacker*, sino programas que se dedican a recorrer todos los puertos y sitios web buscando vulnerabilidades. De ellos, entre 2.000 y 3.000 son campañas de suplantación de identidad, donde uno de los más frecuentes son correos de *phishing* (suplantación de identidad), los que indican que llegó una encomienda y piden acceder a un link.

Orellana explicó que en su mayoría son correos simples, amenazas automatizadas que usan *machine learning* (aprendizaje automático), es decir, que aún no incorporan inteligencia artificial generativa para generar audio o videos sintéticos.

"Ya se pueden hacer ataques más sofisticados de suplantación de identidad, tipo *deep fakes*, que usan herramientas de audio y video que hacen ver muy creíbles a un ejecutivo o personas que tienen poder de decisión dentro de las organizaciones. Un ejemplo, es que un empleado recibe un audio donde el gerente supuestamente le pide que pague cierta cantidad de dinero", contó.

Orellana comentó que en el mundo ya se empieza a ver una sofisticación de amenazas por el uso de herramientas de IA generativa, como audio o video, que hacen más creíble al interlocutor. "Hoy puedes escuchar la voz de tu jefe en mensaje de audio y con las herramientas de IA son indistinguibles".

También señaló que se comenzarán a ver *ramsomware* (secuestro de datos a cambio de un rescate) automatizado, entonces "en vez de realizar un ataque a una o cinco empresas, van a atacar a mil de una vez. El número de ataques de *ransomware* va a subir muchísimo".

Respecto de si los directorios están preparándose para los futuros ataques potenciados por inteligencia artificial, señaló que en la banca se usan muchas herramientas basadas en esta tecnología para hacer detección y prevención de estos nuevos ataques con IA, como "modelos predictivos que detectan anomalías de comportamiento", pero la clave, afirmó es la capacitación.

"Las personas son el eslabón más débil"

Orellana comentó que al mismo tiempo que avanza la tecnología, los ciberataques se sofistican porque van incorporando las nuevas herramientas. Por eso hace hincapié, que hay que generar una "cultura de ciberseguridad en la sociedad", sensibilizar a los trabajadores en este tema y ejecutar un programa de capacitaciones.

"En el Bci se realizan jornadas de conciencia de ciberseguridad, donde siempre debe haber un director. Por ejemplo, en la última invitaron a un *hacker* ético que los hizo escuchar una voz generada por IA y otra humana y la mayoría identificó a la falsa como la real. Por eso es muy importante la capacitación, mi consejo es que si se tiene una duda siempre es mejor consultar a una segunda fuente antes de realizar cualquier acción", dijo Orellana.

Explicó que las capacitaciones son obligatorias y que es importante que el directorio vea los indicadores de cuántas campañas y capacitaciones se están haciendo y cuántos trabajadores han participado.

"Por ejemplo, hacemos Disaster Recovery Process (DRP), que consiste en simular una falla catastrófica como podría ser un ataque de *ransomware* que dejará inhabilitado al banco para operar. Hacemos ejercicios y estamos preparados para poder responder a ese tipo de incidentes. La Ley Marco también establece que los prestadores de servicios esenciales deban realizar estas simulaciones", comentó.

Respecto de alzas en los presupuestos de los bancos en 2025 para enfrentar los nuevos ataques, señaló que "definitivamente hay que fortalecerlo, tanto para sofisticar las herramientas como también para capacitar mejor a la organización, porque las amenazas son crecientes y el eslabón más débil de toda la cadena son las personas", afirmó.

Agregó que un presupuesto de ciberseguridad de cualquier organización debería ser entre un 10% y 20% del presupuesto total de TI, "entonces si una entidad está en 5%, tiene que duplicarlo". Si bien no puede compartir el incremento que realizará Bci, señaló que está "más cerca del 20%".