DIARIO FINANCIERO®

Fecha: 11/02/2026 Audiencia: 40.297 Sección: CIENCIA Y TECNOLOGIA
Vpe: $3.777.303 Tirada: 13.432 Frecuencia: 0
Vpe pág: $5.442.800 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 69,4%

Cómo se preparan las fintech calificadas como OIV para prevenir y reportar ciberataques

Los directores de seguridad de Fintual, Flow y Fintoc -parte de las 915 entidades declaradas clave para la operación del país-, abordaron sus avances en protocolos de gestión de incidentes, medidas de protección y adopción de tecnologías.

El 17 de febrero vence el plazo para que los operadores de importancia vital cumplan con las obligaciones de la Agencia Nacional de Ciberseguridad (ANCI).

POR LAURA FLORES

El 17 de diciembre pasado, la Agencia Nacional de Ciberseguridad (ANCI) presentó la primera lista de operadores de importancia vital (OIV) que establece la Ley Marco de Ciberseguridad. Son 915 entidades, de las cuales 413 pertenecen a infraestructura digital, servicios digitales y servicios de tecnología de la información, categoría que incorpora a un grupo de fintech, entre ellas, Fintual, Flow y Fintoc, las que si bien apelaron para salir de la lista, registran avances para cumplir con la regulación.

Según la ley los OIV son entidades cuya continuidad es clave para el funcionamiento del país, por lo tanto deben cumplir una serie de obligaciones, protocolos y estándares para asegurar el servicio, reducir riesgos y reportar incidentes, de lo contrario arriesgan multas de hasta 40 mil UTM (unos $ 2.780 millones).

En este contexto, el próximo 17 de febrero, se cumple el plazo de 60 días para implementar las medidas contenidas en dos instructivos publicados por la ANCI. El primero establece la designación del delegado de ciberseguridad -que será la contraparte de la Agencia e independiente del área TI de la entidad- y el segundo, medidas para reducir el impacto y la propagación de un incidente.

Este último, instruye una serie de medidas como cambiar contraseñas y eliminar cuentas no utilizadas; proteger comunicaciones y sistemas; deshabilitar accesos remotos o administrativos expuestos; usar herramientas de seguridad para detección y contención; instalar cortafuegos y segmentar redes y contener la propagación lateral. Además de restringir el uso y aislamiento de los sistemas afectados; coordinación interna y registrar las medidas adoptadas.

Fintual: "Solo nos faltaba la obligación de reportar y ya está"

La fintech chilena Fintual - que entrega soluciones de inversión a través de fondos de inversión, APV y acciones- es una de las OIV definidas por la ANCI.

El director de seguridad de la información (CISO, su sigla en inglés), de Fintual, Francisco Casado, señaló que, al momento de ser designados, los requisitos "estaban prácticamente 100% contenidos, salvo por la obligación de reportar", ya que tienen la certificación ISO 27001 del Global Information Security Management System (ISMS), pero esta no exige comunicar los incidentes.

Entre las medidas que han implementado, destacó la automatización de respuesta a incidentes, sistemas de monitoreo, un gestor de identidades para contraseñas, controles de acceso automáticos y planes de recuperación ante desastres.

El ejecutivo comentó que para determinar el grado de avance, usaron inteligencia artificial (IA) para contrastar las nuevas obligaciones con las políticas de seguridad de la empresa.

Si bien ya tienen un encargado de ciberseguridad, aún no designan al delegado de ciberseguridad que establece la normativa, lo que "pronto resolveremos".

Flow: gestión "casi automática" de incidentes y capacitación

Una de las primeras medidas que tomó Flow -plataforma chilena de pago en línea para empresas- fue designar al subgerente de Ciberseguridad de la fintech, Leonardo Jerves, como delegado de ciberseguridad.

El ejecutivo comentó que Flow está regulada por la Comisión para el Mercado Financiero (CMF) y la norma ISO 27001, lo que le permitiría cumplir con las instrucciones establecidas por la ANCI.

Entre los avances, Jerves destacó la detección y remediación "casi automática" de incidentes, el uso de cortafuegos y un equipo de respuesta de ciberataques que tiene "un *playbook* (protocolo) definido de cómo seguir, qué hacer, cómo ir escalando y cómo ir reportando (...) Casi toda la operación ante incidentes está en la nube".

Comentó que cuando salió la ley elaboraron un plan de acción "para cubrir las brechas y lo que nos faltaba era la capacitación de toda la organización", dijo.

Flow apeló a la calificación de OIV y está a la espera de la resolución. Jerves explicó que la solicitud de salir de la lista se debe al riesgo que significan las multas: "Para cualquier empresa o PYME, las multas a las que estamos expuestos hacen casi inviable el negocio posterior a los incumplimientos", afirmó.

Fintoc: protocolo de incidencias y tecnología

El *Information Security Lead* de Fintoc, Vicente Soto, señaló que la fintech de infraestructura de pagos ya contaba con un "avance sólido" previo a su designación como OIV.

Comentó que un primer paso fue su designación como delegado de Ciberseguridad.

Entre los avances, Soto resaltó el protocolo de gestión de incidencias, el que permite al momento de detectar una ciberamenaza, tener un "proceso definido de cómo se investiga, se contiene y se comunica, si es necesario, un incidente de ciberseguridad".

También destacó la implementación de medidas como la autenticación a los sistemas por parte de funcionarios; *password managers* para la creación de claves robustas; el uso de IA para la detección de patrones anómalos, y el sustento del sistema en la nube.

Soto dijo que apelaron para salir de la lista de OIV, pero no lograron. "Siendo operador íbamos a tener el mismo estándar (...), pero con el doble de exigencias en la regulación como tal".