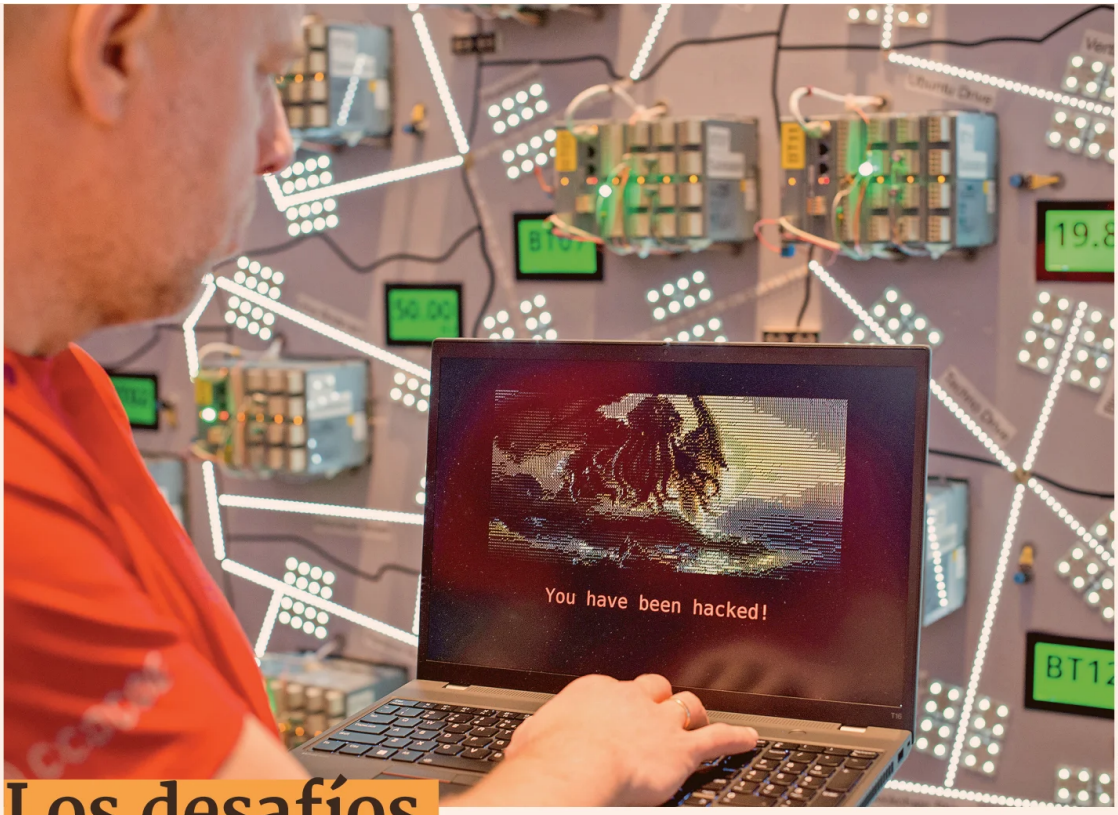
DIARIO FINANCIERO®

Fecha: 28/02/2025 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $5.808.673 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 78,04%

A días de ser calificados por la Agencia Nacional de Ciberseguridad, expertos y representantes de la industria advirtieron sobre la falta de preparación de algunas empresas ante la normativa, los costos de adecuación y los retos asociados a su fiscalización.



BLOOMBERG

Los desafíos que enfrentan los Operadores de Importancia Vital con la Ley Marco de Ciberseguridad

POR MARCO ZECCHETTO

A partir del 1 de marzo entrarán en vigencia las normas relativas al proceso de calificación de Operadores de Importancia Vital (OIV), a la obligación de notificación de incidentes de ciberseguridad y el régimen sancionatorio, establecidas en la Ley N°21.663 Marco de Ciberseguridad, que regula y coordina las acciones de ciberseguridad para los órganos del Estado y particulares, y crea la Agencia Nacional de Ciberseguridad (ANCI), ente regulador, fiscalizador y sancionador que inició sus actividades el 1 de enero.

La normativa regula el funcionamiento de los Servicios Esenciales (SE), es decir, organismos de administración del Estado y el Coordinador Eléctrico Nacional; los servicios prestados bajo concesión de servicio público y aquellos proveídos por privados -como sector eléctrico, telecomunicaciones, agua potable, servicios financieros, entre otros- y también a los Operadores de Importancia Vital. A dos días de ser calificados estos últimos por la ANCI, aún existen desafíos que van desde la preparación de las empresas para cumplir con las nuevas obligaciones, hasta los retos de fiscalización que tendrá la Agencia.

La Ley establece que la ANCI podrá calificar como OIV a quiénes la provisión de sus servicios dependa de redes informáticas, y que la interrupción de sus servicios "tenga un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer o garantizar". Además, las infracciones por incumplimiento en el caso de los OIV van desde UTM 10 mil ($ 672 millones) a UTM 40 mil ($ 2.690 millones).

"Pasividad", costos y fiscalización

Entre los deberes específicos que establece la normativa (Artículo 8°), en el caso de los OIV estos deberán: implementar un sistema de gestión de seguridad de la información continuo para determinar los riesgos que puedan afectar sus sistemas informáticos; implementar planes de continuidad operacional certificados; realizar continuamente revisiones, análisis de sus sistemas y simulacros; contar con programas de capacitación para trabajadores; informar sobre la ocurrencia de incidentes o ciberataques; designar un delegado de ciberseguridad; entre otros.

En esa línea, la socia de Cyber en Deloitte, María Luisa Acuña, advirtió que muchas empresas han tomado una actitud "pasiva" ante su preparación para cumplir con la Ley, y que si bien algunas compañías han avanzado gracias a normativas sectoriales previas, otras han dado "tímidos pasos" para cumplir con los estándares exigidos, especialmente respecto de los planes de continuidad operacional y de ciberseguridad, que deberán ser certificados y sometidos a revisiones periódicas.

Acuña enfatizó en que hay aspectos de la ley que ya están vigentes desde el 1 de enero. "Hay una absoluta pasividad en términos de que ya hay aspectos que se aplican a los prestadores de servicios esenciales, y lo que viene a normar ahora la ANCI es el procedimiento de cuáles de estos prestadores adicionalmente van a tener una categoría de Operadores de Importancia Vital", afirmó.

Por otro lado, la líder de la Mesa de Ciberseguridad de la Asociación de Empresas Chilenas de Tecnología (Chiletec), Myriam Pérez, dijo que cumplir con la regulación implica costos elevados, especialmente para las pequeñas y medianas empresas, que deben invertir en tecnología, certificaciones y talento especializado, pero indicó que "no hay ningún incentivo para esto", como subsidios, beneficios tributarios o apoyo financiero.

HASTA UTM **40** MIL

SERÁN LAS MULTAS POR INCUMPLIMIENTO PARA LOS OIV.

Además, señaló que hay incertidumbre sobre la calificación de los OIV, y que hay empresas que están esperando a ser notificadas antes de tomar acción.

Por su parte, el director de Consultoría en Riesgo y TI de Forvis Mazars, Darío Rojas, sostuvo que otro desafío es la escasez de talento en ciberseguridad, ya que "las estadísticas del Gobierno señalan que existe una brecha de aproximadamente 28.000 profesionales en este ámbito y se estima que esto se va resolver el 2033. Entonces, cómo vamos a poder cubrir esta necesidad de profesionales de aquí a los próximos diez años".

Pérez también se refirió a la capacidad de fiscalización que tendrá la ANCI, dada la falta de certeza ante el número de Servicios Esenciales que serán calificados como Operadores de Importancia Vital. "Algunos dicen que serán 10 o 15 empresas, pero otros estiman hasta 500. De ser así, ¿cuál va a ser la capacidad de la Agencia para fiscalizar a tantas empresas al mismo tiempo, sobre todo al inicio de la ley?", comentó.

En ese contexto, Rojas agregó que el desafío es "cómo la Agencia va a lograr no solamente emitir este marco regulatorio, sino cómo ir a verificar de manera preventiva en las empresas declaradas como esenciales o aquellas que realizan algún servicio relevante, que se están cumpliendo las cosas de manera adecuada".