CIBERSEGURIDAD:

# Nueva ley busca fortalecer la institucionalidad en temas de seguridad informática

Miguel Gutiérrez, director de la carrera de Ingeniería en Ciberseguridad UNAB, explica que la nueva institucionalidad también definirá estándares que tendrán impacto directo en las empresas que forman parte de la economía digital.

El 13 de diciembre de 2023 el proyecto de Ley Marco de Ciberseguridad fue aprobado por el Congreso, siendo ratificado por ambas cámaras de forma unánime.

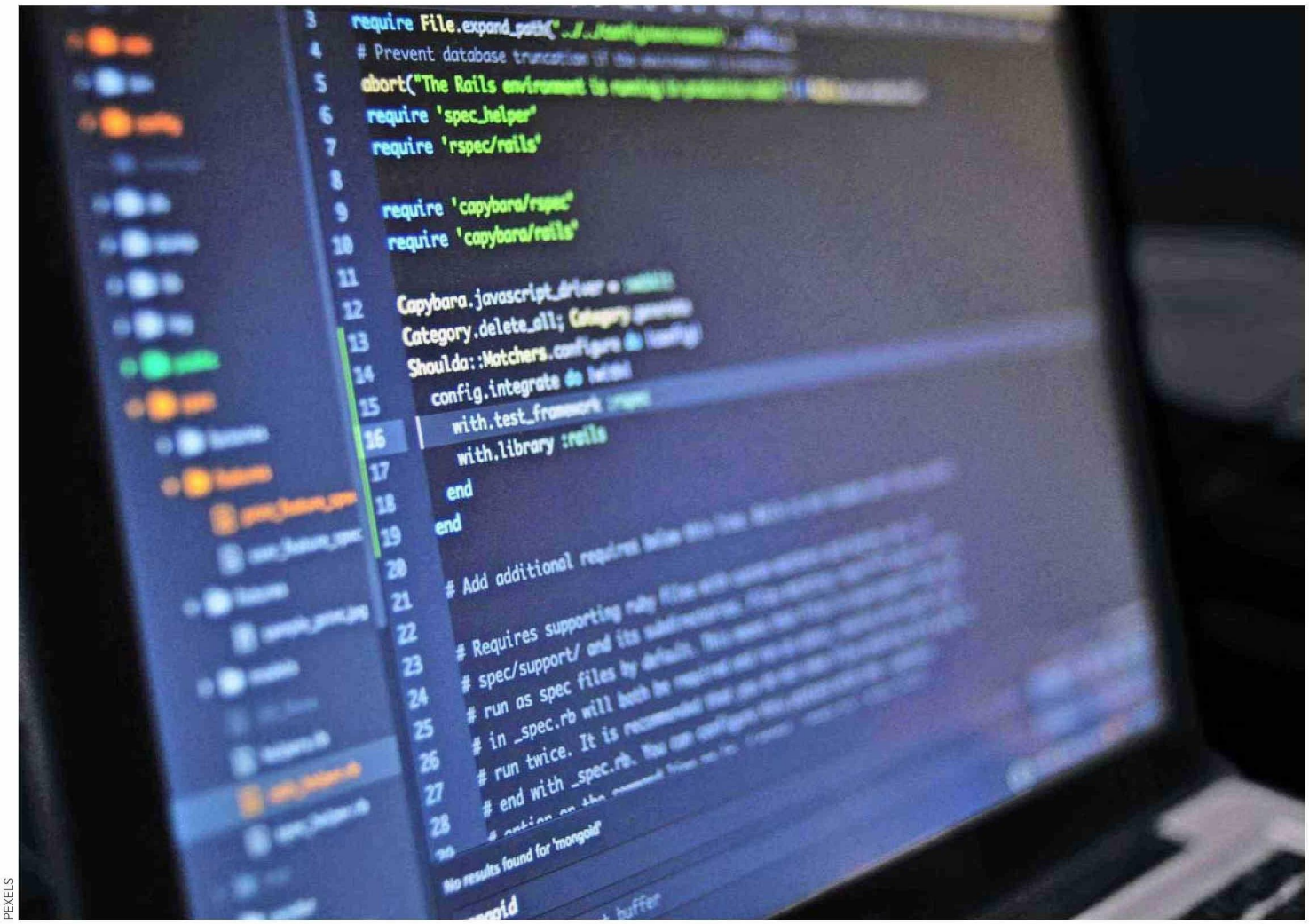
Actualmente se está a la espera de la promulgación por parte del Presidente de la República y la consiguiente publicación en el Diario Oficial.

Según información autorizada, en la instancia, la ministra del Interior, Carolina Tohá, agradeció ese alto respaldo y resaltó la importancia de la aprobación de la Ley Marco. "Este proyecto nos va a poner a la vanguardia en la región latinoamericana en esta materia. Vamos a tener una agencia encargada de la ciberseguridad, que va a definir estándares, tanto para los servicios esenciales como para los operadores que tienen funciones vitales, y esos estándares van a ser validados a través de instituciones certificadas especialmente para cumplir esa tarea".

Esencialmente, el proyecto busca fortalecer la institucionalidad en temas de seguridad informática, a la vez que crea la Agencia Nacional de Ciberseguridad (Anci). Este organismo contará con facultades regulatorias, fiscalizadoras y sancionatorias en esta materia.

Así lo detalla Miguel Gutiérrez Gaitán, director de la carrera de Ingeniería en Ciberseguridad de la Universidad Andrés Bello (UNAB), quien explica que la nueva institucionalidad definirá estándares que tendrán impacto directo en las empresas que forman parte de la economía digital. "Por ejemplo, más adelante las organizaciones tendrán la obligación de ocuparse de los incidentes de ciberseguridad y de informar cuanto antes a la Anci de cualquier problema serio. Lo anterior se traduce indirectamente en un impacto que siempre es de beneficio para las personas naturales", dice.

Según indican en el CSIRT, equipo de respuestas ante incidentes de seguridad informática, "la ley marco instaura así un modelo de gobernanza y mecanismos para contar siempre con los más actualizados estándares de seguridad, campañas de concientización para la ciudadanía, y los equipos necesarios para evitar y responder ante incidentes de ciberseguridad".




PEXELS

*"La ley marco instaura así un modelo de gobernanza y mecanismos para contar siempre con los más actualizados estándares de seguridad, campañas de concientización para la ciudadanía, y los equipos necesarios para evitar y responder ante incidentes de ciberseguridad".*

## INCIDENTES Y DELITOS INFORMÁTICOS

**Según el CSIRT, algunas clasificaciones de incidentes de este tipo son: contenido abusivo, código malicioso, formas de obtención de información, intentos de intrusión, intrusiones, disponibilidad, seguridad del contenido de la información, fraude, vulnerabilidades, otros (que no se puedan encasillar en la clasificación anterior), test (pruebas).**

**En tanto, el organismo detalla que los delitos informáticos no poseen una definición exclusiva estándar. Sin embargo, la legislación sanciona al que destruya, acceda o inutilice un sistema de tratamiento de información. Asimismo, protege los datos contenidos en él ya que establece penas para quienes se apoderen, intercepten, difundan o destruyan la información allí contenida.**

**"En general se ha acuñado el concepto de 'sabotaje informático' el cual está relacionado con todas aquellas acciones que un tercero realiza sobre un sistema de tratamiento de información con el fin de impedir u obstaculizar su funcionamiento normal. De igual forma, se sanciona el hecho de alterar o destruir el sistema como tal", dicen en el CSIRT.**

**Añaden que análogamente se ha designado el término "espionaje informático" para aquellas acciones maliciosas sobre los datos contenidos en este sistema de tratamiento de información. Por ello, se sanciona a quien se apropie de la información allí contenida y también a quien difunda y revele estos datos.**

**Ejemplos de delitos informáticos: sabotaje, defacement, malware, phishing.**

### RESPUESTA ANTE INCIDENTES

Existen diversos consejos de seguridad, tanto para el usuario, por ejemplo al realizar transacciones bancarias; o para las empresas, al manejar información crítica. La idea es mantenerse informados, ser responsables y así prevenir acciones que atenten contra la seguridad informática y que entreguen posibilidad al ciberdelincuente de acceder a ciertos datos.

Actualmente, el CSIRT es el organismo que cumple un rol fundamental educando e informando en esta materia. En el sitio web www.csirt.gob.cl y redes sociales del CSIRT, se pueden encontrar recomendaciones generales e información actualizada acerca de alertas e incidentes de ciberseguridad en el país.

Al mismo tiempo, como se señaló anteriormente, es el ente o equipo de respuesta ante incidentes de seguridad informática. En la página web, se pueden revisar las indicaciones de cuáles son los llamados incidentes de seguridad informática, además de cómo y cuándo reportarlos. Igualmente se detalla a qué se refiere un delito informático y cómo denunciarlo. También poseen un número de contacto en donde es posible conseguir orientación al respecto.

Miguel Gutiérrez comenta que una vez promulgada y entrada en vigor la nueva ley, el CSIRT seguirá funcionando. "Sin embargo, esta vez el CSIRT actuará en coordinación con el Anci, lo que mejorará y ampliará su alcance en lo que respecta a la gestión de incidentes de seguridad informática", indica.

Añade el experto UNAB que los principales desafíos ante la nueva ley, a su juicio, estarán relacionados en lo que respecta a la coordinación internacional. "La coordinación internacional permite, por ejemplo, anticiparse a prácticas y delitos que se cometen en otros países, tanto fuera como dentro de la región. Por otro lado, es importante poner en relieve que la formación de profesionales en el área de la ciberseguridad se hará cada vez más relevante, pues serán necesarios más especialistas que cubran los puestos de trabajo que demandará la nueva legislación", concluye.