Haciendo doble-click sobre la Ley Marco de Ciberseguridad:

Motivaciones, desafíos y oportunidades

Eduardo Godoy Vega

Magíster en Docencia para la Educación Superior por la Universidad Andrés Bello e Ingeniero Civil en Computación por la Universidad De Chile. Profesor Adjunto del Departamento de Ciencias de la Computación de la Universidad de Chile. Además, es consultor senior en seguridad de la información y ciberseguridad, implementador líder y auditor de la norma ISO27001 al frente de su empresa, CISOVirtual, además de perito judicial en temas relacionados.

egodoy@dcc.uchile.cl

Resumen / La existencia de una ley de ciberseguridad es fundamental porque los ataques informáticos representan hoy un riesgo real para el funcionamiento del Estado, las empresas y la vida cotidiana. Incidentes recientes —como el ocurrido en la Subsecretaría de Prevención del Delito en septiembre de 2025— evidencian que el país requiere una estructura formal para coordinar su protección digital.

Aunque podría pensarse que basta con el "sentido común", este no es suficiente: la industria tecnológica ha generado una falsa sensación de seguridad al afirmar que ciertos servicios, como la nube o ciertos teléfonos, son "muy seguros". Esto ha llevado a que muchas personas e instituciones subestimen los riesgos reales.

La Ley Marco de Ciberseguridad (Ley 21.663), promulgada en 2024, crea la Agencia Nacional de Ciberseguridad (ANCI) y define obligaciones, estándares y protocolos para los sectores críticos —como electricidad, agua, telecomunicaciones, finanzas y transporte— con el fin de que operen de forma segura y continua. Esta normativa invita a todos los actores del Estado, incluidas empresas y ciudadanos, a elevar su conocimiento y conciencia sobre los riesgos digitales, entendiendo que los atacantes actuales son organizaciones criminales complejas y no simples aficionados.

Para las ingenieras y los ingenieros en computación, la ley abre oportunidades laborales en áreas como cumplimiento regulatorio, análisis de riesgos, aseguramiento de la continuidad operativa, respuesta a incidentes, consultoría y desarrollo de tecnologías seguras.

Introducción

¿Por qué un país requiere una ley de ciberseguridad?, ¿no debería bastar con el "sentido común"?, ¿qué oportunidades presenta esta ley para las ingenieras y los ingenieros en computación? En este artículo pretendo dar algunas luces y sembrar algunas dudas en el lector.

Demos algo de contexto... Según el reporte de riesgos globales del Foro Económico Mundial 2025 [1], temas relacionados con ciberespionaje y guerra cibernética están dentro de los *top 10* riesgos con mayor impacto que podrían afectar gobiernos y estabilidad social, entre otros.

Entonces, el estado debe tomar medidas para protegerse frente a ataques cibernéticos que puedan poner en riesgo su continuidad operativa. Acá debemos entender, según Carré de Malberg [2], que define al Estado como "una comunidad humana, fijada sobre un territorio propio, que posee una organización que resulta para ese grupo, en lo que respecta a las relaciones con sus miembros, una potencia suprema de acción, de mando y coerción", entonces, como Estado, es decir todos los actores que participamos de él, debemos tomar acciones concretas en la ciberseguridad; de ahí la importancia de la Ley Marco de Ciberseguridad, ya que define criterios y prioridades al momento de definir qué, quiénes y cómo deben coordinarse estas acciones.

Hago hincapié en el mensaje de "todos los actores". Aún es común escuchar en empresas e instituciones que la ciberseguridad es un problema del área TI, cuando en realidad es un problema de *continuidad de negocio*, por lo tanto es un problema o preocupación transversal a toda la institución o empresa. Una falla en ciberseguridad te puede dejar fuera de operación o incluso puede significar el cierre de las operaciones.

El 11 de septiembre de 2025 leíamos esto en los medios de comunicación:

> *La Subsecretaría de Prevención del Delito (SPD), institución liderada por Carolina Leitao, registró un "incidente informático" que afectó a equipos institucionales y está generando intermitencia en servicios virtuales.*[1]

Espero haber dejado meridianamente claro el porqué necesitamos de esta ley.

¿Y por qué el sentido común no es suficiente?

Interesante pregunta, si tengo una actividad que depende fuertemente de la computación, debería ser obvio que debo preocuparme de cuidarla, pero acá aparecen algunos vicios. Para bien o para mal muchas veces nosotros mismos, los ingenieros, damos certezas de cosas que no lo son —entre ellas, "no se preocupe, la nube es *muy* segura", delegando la seguridad en el proveedor de servicios de cómputo en la nube; otro ejemplo, "esa marca de celular es inviolable, es *muy* segura", sin revisar que en la lista de Apps con algún tipo de *malware* también aparecen listados. Es así como hemos sembrado, entre los técnicos y el marketing, una falsa sensación de seguridad y eso es muy malo; es peor sentirse seguro, cuando realmente no lo está, a tener conciencia de las inseguridades o vulnerabilidades que poseo.

Entonces, a ese "sentido común" lo hemos ido bloqueando con siglas y tecnologías difíciles de explicar y aún más difíciles de entender para la gente que está fuera del rubro.

Resumen, no, no basta con el sentido común.

1 Fuente: Emol.com https://www.emol.com/noticias/Nacional/2025/09/11/1177644/equipos-institucionales-spd-incidente-informatico.html

Aún es común escuchar en empresas e instituciones que la ciberseguridad es un problema del área TI, cuando en realidad es un problema transversal a toda la institución o empresa.

Vamos a lo más concreto.... La Ley 21.663 es la Ley Marco de Ciberseguridad [3]; luego de una larga discusión iniciada en marzo de 2022, fue promulgada en abril de 2024 y coloca a Chile al día en cuanto regulación en este tema.

Crea la Agencia Nacional de Ciberseguridad (ANCI), que tiene por objetivo, entre otros, definir protocolos, estándares técnicos y regulaciones obligatorias para los servicios esenciales y Operadores de Importancia Vital; es decir, le dirá a los sectores que son fundamentales para que el país funcione cómo deben protegerse, existiendo el principio de proporcionalidad, es decir, no puede ser más cara la protección que lo protegido; ahora este tema toma tonos éticos en este punto, cuando lo que protegemos es la vida de un ser humano o los derechos de niños, niñas y adolescentes, eso tiene un valor infinito.

¿A qué nos obliga o invita la ley de ciberseguridad? Lo primero y más importante es a crear conciencia en el tema; todos los actores del estado, es decir, empresas, instituciones y por cierto los ciudadanos debemos incrementar nuestro saber en ciberseguridad. Acá un primer gran problema: para el común de las personas, si escuchan hablar de ciberseguridad, imaginan a un hacker —típicamente un o una joven poco sociable, que durante la noche y usando conocimientos de las artes oscuras, se mete a los computadores de las empresas para robar datos, modificar información e incluso apagar complejos sistemas informáticos— cuando sabemos que existen verdaderas empresas dedicadas a este delito... son organizaciones criminales. Si tomamos conciencia que los atacantes no son esta parodia de joven en su dormitorio, rodeado de cajas de pizza que está intentando romper un sistema, sino que son verdaderas corporaciones, entonces tomaremos conciencia que para protegerse no basta con la buena voluntad o apostar a la suerte de "a mí no me pasará".

¿Cuáles son los servicios esenciales?

Corresponden a los siguientes:

- Generación, transmisión o distribución eléctrica.
- Transporte, almacenamiento o distribución de combustibles.
- Suministro de agua potable o saneamiento.
- Telecomunicaciones.
- Infraestructura digital, servicios digitales y servicios de tecnología de la información gestionados por terceros.
- Transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de la infraestructura respectiva.
- Banca, servicios financieros y medios de pago.
- Administración de prestaciones de seguridad social.
- Servicios postales y de mensajería.
- Prestación institucional de salud (hospitales, clínicas, consultorios, centros médicos).
- Producción y/o investigación de productos farmacéuticos.

Si la empresa o institución está dentro de alguna de estas categorías, tienen la obligación de registrarse en la ANCI y de informar cada vez que sufran algún ataque de ciberseguridad que sea considerado relevante.

¿Qué pasa si la empresa no informa?

Quizás lo primero que debemos pensar es ¿por qué una empresa no querría informar? Generalmente es por el temor a que su imagen se vea dañada o incluso a potenciales efectos legales de ciudadanos u otras empresas que pudieran verse afectados por este ataque. Pues bien, en el caso de no hacerlo, la ANCI está facultada para cursar multas, que en el peor de los casos supera los 1.600 millones de pesos. Importante, el mal informar, es decir, disfrazar el evento por otro de manera consciente, también es constitutivo de falta; por ejemplo, sufrí el robo de mis datos y reporto que me hicieron un ataque de Denegación de Servicios Distribuido (DDoS).

Sin duda que para cada uno de estos sectores se nos pueden ocurrir ejemplos claros de empresas o instituciones que las entendemos como esenciales. Por ejemplo, en salud, podríamos pensar desde hospitales de alta complejidad hasta la atención primaria; en telecomunicaciones, todos los operadores de conectividad de datos y voz —de sólo pensar (o recordar) caídas, suspensiones o incluso intermitencias en sus servicios ya podemos ver el caos que eso generaría: no poder usar el banco, pagar el metro y un largo etcétera... la vida de muchos ciudadanos se vería alterada... no en vano somos un país con una alta adopción tecnológica. Ahora bien, dentro de estos sectores hay operadores que son más relevantes que otros, no es lo mismo que un pequeño prestador de transporte terrestre tenga una suspensión en sus servicios a que lo haga la principal línea área nacional o aquella que tiene ruta única, como puede ser Santiago–Rapa Nui. A ellos,

la ANCI los podrá nominar como Operadores de Importancia Vital (OIV); y con ese nombramiento vienen más responsabilidades y mayor control de sus cumplimientos.

Pero, ¿qué significa en la práctica ser un OIV?

Pues bien, al ser OIV, la ANCI tiene facultades para poder exigir algunos estándares más altos de protección. También contarán con la supervisión y ayuda de la ANCI frente a situaciones de ataques que puedan o estén colocando en riesgo la continuidad operacional. Y aunque no todo es garrote, hay que estar claros que, en el caso de los OIV, las multas se pueden llegar a duplicar con respecto a un servicio esencial.

Las empresas e instituciones que han aparecido en las primeras nóminas de OIV se lo han tomado de dos formas muy marcadas, algunas lo consideran un elogio, un reconocimiento al servicio que prestan y el valor que este tiene para el Estado; otras, lo han percibido como una mochila, que significará mayor inversión, aumento de costos de operación e incluso, que los podría dejar fuera de negocios al perder competitividad.

Muchas veces nosotros mismos, los ingenieros, damos certezas de cosas que no lo son: "no se preocupe, la nube es muy segura".

Aún falta ver cómo reacciona el ecosistema: si valora que una empresa potencialmente proveedora sea un OIV, o simplemente será un dato sin relevancia al momento de evaluar ofertas.

Ahora bien, ¿qué oportunidades trae esta ley para las ingenieras y los ingenieros en computación?

Las empresas deberán comenzar a implementar protocolos y estándares de ciberseguridad. Algunos sectores van más adelantados que otros. En el mundo de la energía eléctrica llevan 5 años (desde 2020) implementando medidas de ciberseguridad y definieron el estándar NERC-CIP para su infraestructura crítica; la banca, a través de regulaciones de la CMF, ha hecho lo propio; el mismo Estado en el pasado cercano

Las empresas e instituciones que han aparecido en las primeras nóminas de Operadores de Importancia Vital se lo han tomado de dos formas muy marcadas: algunas lo consideran un elogio; otras, lo han percibido como una mochila.

definió a ISO27001 como la norma de referencia y varios servicios, ministerios e instituciones avanzaron en la definición de políticas y procedimientos según dicta ese estándar. Lo que se espera es que a cada vertical se le encuentre el estándar que le sea más apropiado. Pero lo realmente interesante, es que estos estándares traen, generalmente, requerimientos para toda la cadena de proveedores de estos OIV, quienes deberán cumplir con las exigencias que sus clientes les pidan. Esto será interesante de observar, veremos negociaciones de contratos, revisiones de costos, etc. —pero sin duda, tendremos una mejora en la ciberseguridad de todo el ecosistema, sin importar si eres OIV, servicio esencial o simplemente un proveedor de alguno de ellos. Así que se van a necesitar ingenieros e ingenieras que sepan implementar estos estándares, implementar soluciones de ciberseguridad e ingenieros/as que sepan gobernar esta nueva realidad. A este último se le llama CISO (Chief Information Security Officer), que tiene por desafío principal hacer conversar las necesidades de la empresa, su estrategia con las soluciones de ciberseguridad que el mercado está ofreciendo.

Sin duda que esto recién comienza... La Ley Marco de Ciberseguridad no ha dejado a ningún actor de la industria indiferente y eso ya es un gran logro: hacer que se pregunten si realmente deben invertir en ciberseguridad, incluso preguntarse si son candidatos a ser OIV. El solo hecho de abrir la discusión, sacándola del área de TI y colocándola en la mesa de directorios, juntas de gerentes o en la preocupación del pequeño empresario es sin duda el primer gran aporte de esta ley. B

Referencias

[1] World Economic Forum (2025). *Global Risks Report 2025, 20th Edition*. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.

[2] Carré de Malberg, R. (1998). *Teoría general del estado* (J. Ferrándiz & A. Orihuela, Trads.). Fondo de Cultura Económica.

[3] Biblioteca del Congreso Nacional de Chile. Ley 21663: Ley Marco de Ciberseguridad. https://www.bcn.cl/leychile/navegar?idNorma=1202434.