Desafíos de la implementación de la Ley Marco de Ciberseguridad desde la profesión jurídica

Carla Illanes Contreras[1]

Juan Pablo González Gutiérrez[2]

La publicación de la Ley Nº 21.663, Marco de Ciberseguridad que crea la Agencia Nacional de Ciberseguridad, además de otros órganos, tales como el Comité Interministerial de Ciberseguridad y el Consejo Asesor, conforman una gobernanza que busca la vinculación entre el sector público y privado. Además, la regulación que establece deberes generales para aquellos servicios considerados esenciales, y deberes específicos para aquellos operadores que sean declarados operadores de importancia vital, y ambos sujetos con el deber de reportar los incidentes de impacto significativo, plantea desafíos no solo para las áreas de ciberseguridad o seguridad de la información, sino a todos los actores que conforman una organización, en especial para la profesión jurídica.

Es importante recordar que esta normativa se presenta como pionera en la región y se basa, en la Directiva Europea de Ciberseguridad (NIS2), que busca fortalecer medidas para los estados miembros de la Unión Europea, ciertas obligaciones de ciberseguridad, como es el reporte de incidentes de ciberseguridad. El proceso de transposición, es decir, la incorporación de los estados miembros de esta Directiva a su normativa interna venció el 17 de octubre del 2024.

La normativa nacional, que aún no ha entrado en vigencia, contiene una serie de obligaciones que deben cumplir los sujetos obligados, debiendo mencionar que en ciertos sectores que ya cuentan con regulaciones sectoriales (ej. financiero, eléctrico, telecomunicaciones, entre otros), además de las normas técnicas de la Ley N° 21.180 de Transformación Digital del Estado que aplican al sector público, que han permitido elevar los niveles de madurez en esta materia, particularmente en relación a la identificación de riesgos de ciberseguridad, así como la gestión de incidentes operacionales e informáticos. Esto ha exigido que áreas de ciberseguridad o seguridad de la información realicen esfuerzos adicionales para cumplir con los requisitos de dichas disposiciones con el fin de evitar posibles multas ante incumplimiento detectados por los procesos de fiscalización de las autoridades sectoriales (salvo en el caso de transformación digital del Estado, donde no existe una autoridad regulatoria que fiscalice directamente).

No obstante ello, la normativa de ciberseguridad incorpora dentro de los servicios esenciales algunas instituciones privadas que no contaban con regulaciones previas. En consecuencia una vez entrada en vigencia la normativa, estas instituciones deberán adoptar un enfoque proactivo para cumplir con los

[1] Abogada, counsel de DLA Piper.
[2] Abogado, director del Diplomado de Regulación y Tecnología UDD. Consejero del Observatorio de Derecho y Tecnología UDD.

deberes que fija la normativa, sin considerar que pueden ser declaradas como operadores de importancia vital, y que la obligación de reporte de incidentes informáticos aplica para ambos sujetos regulados. Asimismo, deberán llevar a cabo un proceso de identificación de los procesos que puedan ser un riesgo asociados al incumplimiento de la regulación, lo que a su vez representa una oportunidad, apoyándose en buenas prácticas latamente reconocidas en la industria.

Un punto interesante, es que varios de estos procesos tanto para aquellos sectores que ya cuentan con experiencia previa en la materia como aquellos que deberán abordarla tempranamente, es que han sido liderados por áreas de ciberseguridad o seguridad de la información dentro de una organización, es decir "áreas técnicas", sin incluir otras como legal o de cumplimiento. ¿Por qué este punto es relevante de mencionar? Esto se debe a que las obligaciones descritas en la normativa ya no solo contienen componentes de índole técnico como la identificación y gestión de incidentes informáticos, sino que también abarcan otros aspectos eminentemente jurídicos, especialmente cuando se convierten en obligaciones cuya infracción puede derivar en multas cuantiosas y además, procedimientos contenciosos administrativos y procesos de reclamación ante la Corte de Apelaciones. En este contexto, el enfoque de riesgo de incumplimiento normativo permitirá actualizar los principales mapas de riesgos cibernéticos e informáticos, incorporándolos a otros procesos que están viviendo las organizaciones como es la integración de los delitos económicos, especialmente, los informáticos.

Para concluir, la complejidad de los procesos que implica la implementación de la normativa de ciberseguridad, es una tremenda oportunidad para avanzar hacia el trabajo integrativo entre diversas áreas dentro de una organización y por ende, para que las áreas técnicas comprendan los riesgos informáticos, ya no solo desde su enfoque técnico, sino involucrando aspectos normativos, especialmente que éstos implican no sólo riesgo de multa de la Agencia, sino litigios por responsabilidades de índole contractual o extracontractual vinculadas a la materia.