Mario del Carmen Troncoso Rojas

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	El denominado ciberespacio no sólo ha traído avances a la humanidad, sino también está causando un aumento en crímenes tecnológicos, con hackers cada vez más sofisticados a la hora de generar estafas, espionaje entre naciones, entre otros. A ello se suma el peligro al que está expuesta la infraestructura crítica del Estado, el cual puede verse seriamente colapsado por un ataque cibernético, agitación social u otros motivos. Por ello, es que la Ciberseguridad ha dejado de ser un tema circunscrito al ámbito técnico, pasando a ser parte de la Política Pública. Por las características propias del Ciberespacio, sus Normas deben ser objeto de evaluación y actualización constante, a fin de garantizar un ciberespacio libre, abierto, seguro y resiliente. La presente propuesta debe promover una gestión de mejora continua en el tiempo.
Artículo 2.	Nada que agregar, solo deberia estar en linea con los estandares internacionales.
Artículo 3.	Si bien la Continuidad Operacional o Disponibilidad es un factor importante, también lo es la Seguridad de la Información, debiese ser considerara la Confidencialidad e Integridad.
Artículo 4.	Nada que agregar.
Artículo 5.	La ciberseguridad por su naturaleza se da en un contexto globalizado, además de ser

	una industria muy dinámica (tecnologías de la información y telecomunicaciones). Ello supone actualizar continuamente aspectos que pueden afectar la ciberseguridad. La Norma técnica debería establecer explícitamente que todas estas exigencias de seguridad estén en conformidad con los estándares internacionales, especialmente aquellos contemplados en los Convenios a los que el país ha adscrito. En el caso de la infraestructura critica, dada su naturaleza estratégica para el país y que aún no se cuenta con una norma chilena que la defina y regule (Ley de Infraestructura Critica), debería tomarse como referencia y explicitar estas medidas de seguridad de acuerdo a los estándares internacionales y que este alineada con la estrategia nacional de seguridad y defensa. Se supone que el objetivo es "contar con medidas que garanticen la continuidad del servicio de la infraestructura critica", por lo tanto, se deben tener en cuenta los diferentes grados de madurez en ciberseguridad de los distintos sectores.
Artículo 6.	En este punto, sería más explícito (dado que es una Norma Técnica) en las funciones, atribuciones y responsabilidades de los encargados de seguridad de los operadores relevantes. No basta con decir "con las competencias suficientes", dado que no se encarga a ninguna entidad u organismo que certifique esas competencias.
Artículo 7.	La "obligación" de reportar "oportunamente" es lo que ocurrió con el

	sector financiero y sus consecuencias en los ciberataques y ciberdelitos, que no todos "entendían" la obligación e importancia de informar el incidente. Si no existe una exigencia "mayor", entiéndase multas, cese de concesión del servicio, etc. Se queda en una declaración de buenas intenciones. Si bien es cierto que debería ser a la Subsecretaría de Telecomunicaciones que se reporte directamente, lo centraría en el Csirt de esa cartera, dado que esto posteriormente podría escalar al Csirt de Gobierno (Según las implicancias de que se trate). Tomar como referencia la misma lógica con que fue creado el Comité Interministerial de Ciberseguridad.
Artículo 8.	Sugiero ver la experiencia ganada en el sector financiero y aplicar algo parecido, como asimismo tomar la experiencia que lleva el Csirt de Gobierno en estas materias.
Artículo 9.	Misma situación anterior, sugiero ver la experiencia ganada en el sector financiero y aplicar algo parecido, como asimismo tomar la experiencia que lleva el Csirt de Gobierno en estas materias.
Artículo 10.	Si hay algo que aprendió el sector financiero de estos ciberincidentes, es que en "Ciberseguridad no se debe competir si no cooperar" y una forma de garantizar el prestigio y reputación de los "afectados" es justamente manteniendo las reservas que amerita cada situación.
Artículo 11.	Este es un tremendo punto, dado que la "Cultura en Ciberseguridad" no se ha

	entendido como cooperación, tanto en lo público como privado y esto ha hecho que no se pueda intercambiar oportunamente este tipo de información (Mucha resistencia y cada uno con sus propios intereses). Incluso uno de los inconvenientes es que en el sector público no existe interoperabilidad y menos un estado digital. Concuerdo que debe hacerse con una legislación "robusta" en materias de ciberseguridad, por ejemplo, la ley 19.223 "Delitos Informáticos" que aún no ha podido ser modificada.
Artículo 12.	Nuevamente aquí la clave es "Cooperación", no "Competir". La Norma técnica debe orientar hacia ese esquema de Cooperación y no Competencia en Ciberseguridad.
Artículo 13.	Otra vez nos vemos enfrentados a la "voluntad" de los encargados de Ciberseguridad. Estimo que el camino es hacerlo con una legislación "robusta" en materias de Protección de los Datos de la Vida Privada de las Personas y como lo consagra la Constitución.
Artículo 14.	Insistir en el punto, debiera ser más explícito y taxativo en la exigencia, fijar estándares, metodologías, plazos, etc. Dado que la Ciberseguridad es un ámbito muy dinámico y las organizaciones tanto público como privadas deben ser objeto de evaluación y actualización constante.
Artículo 15.	No encuentro pertinente este artículo, lo podría "encasillar" en el artículo 7, siempre haciendo la diferenciación, entre los operadores relevantes y no relevantes, pero ambos con obligación de reportar incidentes.

Artículo 16.	Este artículo de mucha relevancia para "prevenir" y "minimizar" los ciberincidentes, y dada la lógica de la gestión de riesgos de los servicios de redes. Para contar con una infraestructura de la información robusta y resiliente (recordar que es un objetivo de la Política Nacional de Ciberseguridad), la Norma debería estipular medidas técnicas tendientes a prevenir, gestionar y superar los riesgos cuando estos se verifican; identificar y jerarquizar las infraestructuras críticas; implementar mecanismos estandarizados de reporte, gestión y recuperación de incidentes; y finalmente fijar estándares diferenciados en materia de Ciberseguridad. Otro aspecto que considero de suma importancia es la vinculación más estrecha en el traspaso de información orientada al análisis de riesgos y amenazas de la infraestructura critica; con el Sistema de Inteligencia Nacional y/o Sistema de Defensa Nacional.
Artículo 17.	Nada que agregar.
Artículo 18.	Nada que agregar.
Comentarios Generales.	Encuentro una obligación ciudadana el poder exponer mis puntos de vista en está Norma Técnica de Ciberseguridad y una responsabilidad ineludible como usuario de un Ciberespacio donde estan ocurriendo muchos hechos positivos y negativos. Me permito nuevamente sugerir que en "Ciberseguridad se Coopera y no se

	Compite”, debería incorporarse en forma explícita en algún párrafo de esta.