CLARO CHILE S.A.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Sin comentarios.
Artículo 2.	Sin comentarios.
Artículo 3.	Sin comentarios.
Artículo 4.	Cabe tener presente que, las TELCOs, al operar Infraestructura declarada por la autoridad como Infraestructura Crítica, siempre será considerado como operador relevante de acuerdo a la norma propuesta.
Artículo 5.	No se especifica qué criterios usará la Subsecretaría para elegir el marco a utilizar en determinadas circunstancias. Para el caso de los operadores relevantes se señala que "en consideración a circunstancias particulares de vulnerabilidad", deberán adoptar los estándares que la autoridad indique, sin especificar qué o cuales estándares se deberán cumplir. Igualmente, creemos relevante en la normativa la inclusión de planes de identificación y tratamiento de vulnerabilidades, lo cual permitirá la realización de controles preventivos estandarizados en la industria. Se sugiere las normas de Seguridad de la Información Nch 27.000 del Instituto Nacional de Normalización. En cuanto a normas internacionales, se sugiere un tipo de estándar que considere varios puntos de vista como el ISO 27001

	Asimismo, creemos que la redacción del artículo podría generar un riesgo de vulneración al principio de neutralidad tecnológica. A su vez, el artículo no es claro respecto de los estándares internacionales a los cuales hace mención, por lo tanto, esto podría atentar contra dicho principio. A nuestro entender no resulta aplicable la supervisión del proceso de manufactura de equipos, al contrario, creemos que lo que el reglamento o ley debiera hacer, es aclarar qué estándares de fabricación son los que se exigirá a insumos que cualquier operador utilice para infraestructura crítica, teniendo en cuenta que dicho estándar no atente contra el principio de neutralidad tecnológica Igualmente, nos parece recomendable revisar el articulo a la luz de la normativa de libre competencia. Finalmente, y en relación al rol que deberá desempeñar el CSIRT, creemos relevante se establezca el proceso que sustente el funcionamiento y operación del CSIRT dictando cómo y cuándo actúa, y en caso de ser necesario, cómo interactúa con los diversos stakeholders involucrados durante una crisis.
Artículo 6.	Sin comentarios.
Artículo 7.	Para este ítem se sugiere flexibilizar el envío del reporte de los operadores que trabajan en un rol de turno continuo y 24x7, así como delegar la responsabilidad en 2 personas: encargado y suplente de ciberseguridad. Es poco probable cumplir con reportar en los tiempos que se

	proponen.
Artículo 8.	Sin comentarios.
Artículo 9.	Sin comentarios.
Artículo 10.	Sin comentarios.
Artículo 11.	A pesar que el informar a terceros para prevenir, gestionar o resolver una ciberincidencia sea necesario, nos preocupa que se divulgue una brecha de seguridad del tipo “día cero”, es decir que no se conoce una medida de mitigación concreta al respecto. Toda vez que terceros podrían mal utilizar esta información. Se debe especificar qué y cómo se hará público o se compartirá este tipo de vulnerabilidades. En definitiva, se debe establecer el mecanismo por el cual se hará el intercambio de información, esto, ya que se deberá considerar la inclusión de normas internas que permitan el manejo de datos sensibles entre distintos actores.
Artículo 12.	Sin comentarios.
Artículo 13.	Creemos que debe ser más explícito a fin de proteger correctamente la vida privada de los eventuales involucrados, además no define quien es el órgano encargado para la protección de datos personales.
Artículo 14.	El título del artículo hace referencia a que los reportes son trimestrales, sin embargo, en el contenido del artículo no se especifica un período definido, más bien, se habla en forma genérica del período y

	se especifica que el período de los reportes será aquel que Subtel indique en las instrucciones pertinentes.
Artículo 15.	Sin comentarios.
Artículo 16.	Es suficiente una prueba de seguridad de forma de cumplir con las actividades de control y documentación. Lo anterior, en base a la situación actual que se vive en el contexto internacional. Creemos que es recomendable revisar el articulo a la luz de la normativa de libre competencia. Por último, vemos que este articulo podría constituir un riesgo de vulneración al principio de neutralidad tecnológica.
Artículo 17.	Sin comentarios.
Artículo 18.	Sin comentarios.
Comentarios Generales.	Sin comentarios.