entel pcs telecomunicaciones s.a.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Se solicita definir: “Sistemas”: (¿sistemas TI necesarios para la entrega de los servicios? ¿Los sistemas para la Provisión de Servicios? ¿Facturación, cobro? ¿Venta y Post Venta? Se solicita aclarar a qué se refiere con operadores relevantes, que efectos conllevará. Quiere decir que los otros no estarán afectos. Creemos que la definición del artículo 4 siguiente establece criterios que son poco específicos y claros
Artículo 2.	Se solicita especificar en la letra b) si corresponde a un evento que afecta la disponibilidad de los Servicios de Telecomunicaciones (Voz, datos, TV, todo lo que tenga una concesión o permiso entregado por Subtel). Se solicita aclarar letra g) cuando menciona infraestructura crítica, el alcance es toda la red fija y móvil o se refiere sólo a la Red mínima que se estableció post 27F?. Es relevante distinguir la infraestructura crítica desde la continuidad operacional de los servicios respecto a aquella que es crítica para la seguridad de información en el ciberespacio, que, si bien en algunos casos puede coincidir, no necesariamente es la misma.
Artículo 3.	Remisión puntos 1, 2 y 3 de los comentarios generales
Artículo 5.	En cuanto a los conceptos: Indeterminación al establecer las obligaciones. Estas debieran ser objetivas, medibles y claramente determinadas. Cuando hablamos de estándares internacionales como una obligación, esta debe ser específica, concreta y

	determinada, indicándose expresamente a que estándares se refiere la norma. Inciso 4to: Se solicita aclarar, ¿esto significa que la compañía de telecomunicaciones deberá auditar a los fabricantes y/o proveedores de equipamiento y/o software, como también a los contratistas? inciso 6to: Se solicita aclarar si las recomendaciones serán mandatorias Se solicita aclarar de qué forma se entregará esta información, ¿cómo?, ¿dónde?, si existirán plazos establecidos inciso 8vo: Se solicita aclarar a qué se refiere, ¿cómo se definirá, ¿cómo se entregará la información, plazos asociados? Se solicita aclarar "los estándares", ya que deben ser objetivos e indiscutibles, toda vez que tendrán impacto en la inversión.
Artículo 7.	El criterio no es congruentes con las normas en materia de telecomunicaciones y abordan materias como seguridad de datos personales que no son propias de la LGT. Por otra parte, también están poco determinadas. Se solicita aclarar, cuál es la herramienta que se va a disponibilizar para esto.

Artículo 9.	Se estima que el periodo establecido es excesivo y tampoco establece una determinación clara de lo que debiese reportarse, toda vez que las redes de telecomunicaciones por su propia naturaleza generan varias alteraciones e interacciones de forma diaria que muchas veces no afectan de forma alguna los servicios de telecomunicaciones. Se considera que el DS 60 ya regula de forma satisfactoria la industria. Se estima poco viable en el cumplimiento debido a la por la naturaleza misma de la red de telecomunicaciones.
Artículo 10.	Se solicita aclarar cómo se regulará el buen uso y cuidado de la confidencialidad de los reportes.
Artículo 11.	Se debe considerar siempre el resguardo de información estratégica o comercial de las compañías en esta materia. Asimismo, deben tomarse las más altas medidas para mitigar cualquier tipo de impacto reputacional, por ello no debiera revelarse el nombre de la empresa que informa una ciberincidencia, salvo que sea estrictamente necesario.
Artículo 12.	Se solicita especificar quien es (sería) el CSIRT de referencia, contacto, canal de comunicación, etc. Se solicita especificar a quien se le solicitará, y el alcance (declaración de principio de finalidad de uso de información).
Artículo 13.	Remitirse al punto 1 y 3 de los comentarios generales Se solicita especificar declaración de principio de finalidad de uso de información. Se sugiere eliminar este artículo. En el reporte no se debería abordar información personal, menos de carácter sensible, la que no se puede entregar por temas legales. La información debe ser la necesaria para transparentar el riesgo /afectación respondiendo a lo requerido de manera agregada (del artículo 9°):

	a. Estimación de la cantidad de usuarios y clientes actual y/o eventualmente afectados. b. Grado de afectación a usuarios y clientes. c. Alcance geográfico actual y eventual de la ciberincidencia.
Artículo 14.	Se solicita informar ¿cuál es alcance de lo que se tiene que informar?
Comentarios Generales.	1) Si bien nos encontramos de acuerdo con la necesidad de generar un marco jurídico claro en materia de Ciberseguridad, creemos que, previo a la dictación de normas sectoriales, se hace necesario en Chile definir una institucionalidad que precise el marco legislativo en términos generales y sistémicos. Si bien a la fecha se encuentra en vigencia la Política Nacional de Ciberseguridad, y variados anteproyectos que tienen por finalidad que el país avance en esta materia, no contamos con una legislación ni con un órgano definido para estos efectos, lo que creemos necesario para otorgar certeza jurídica y evitar una potencial superposición de funciones en materia de Ciberseguridad. Sin perjuicio de lo anterior, en el caso de que se dicte una norma como la propuesta bajo el amparo de la Ley General de Telecomunicaciones (LGT) y otra normativa pertinente de telecomunicaciones , esta debiera aplicarse estrictamente a los concesionarios o permisionarios de servicios de telecomunicaciones en lo relativo a la seguridad de dichas redes en cuanto exista algún riesgo de seguridad de información por afectaciones de la continuidad de los servicios y no por otras materias no contempladas en la LGT.. 2) Conforme a lo antes señalado, creemos que el presente reglamento en consulta debe necesariamente enmarcarse en las atribuciones otorgadas a Subtel por la Ley General de Telecomunicaciones, el DL 1762 y sus

	respectivos reglamentos, y no vincularse, por ejemplo, con materias de privacidad y protección de datos personales, lo que se regula expresamente por la Ley N° 19.628, y que además ha sido ampliamente discutido en el proyecto de ley que se encuentra actualmente en tramitación en el Congreso y por la cual se creara toda una institucionalidad que abordara dicha materia . En efecto, la Subsecretaria de Telecomunicaciones debiese velar especialmente por la disponibilidad e interrupciones de los servicios que regula, y no de aquellas materias relativas a la vulneración de la información ni la protección de datos personales, que debiese quedar al amparo de un marco regulatorio general en materia de Ciberseguridad y Protección de Datos Personales , de forma tal de evitar la multiplicidad y diversidad de regulaciones de los órganos del Estado en esta materia, de modo tal que el marco normativo sea un todo orgánico y sistémico. 3) Es relevante limitar la responsabilidad de los concesionarios y permisionarios del servicio de telecomunicaciones específicamente a lo relativo al uso y administración que ellos mismos realicen respecto de su propia red de telecomunicaciones, y no extender dicha responsabilidad a los servicios que puedan desarrollarse por terceros proveedores de servicios utilizando la misma red, como es de esperar que ocurra con el IoT y otros prestadores de servicios montados sobre la red de telecomunicaciones, debiendo estos últimos asumir la responsabilidad de la seguridad de los dispositivos y todas las herramientas requeridas para la prestación de sus servicios, que escapan al alcance de un concesionario de servicios de telecomunicaciones. La debida protección y seguridad debe exigirse a todos los agentes que intervengan en la cadena de valor, los que deberán estar sometidos a las mismas reglas, y no sólo respecto de los concesionaros o permisionarios de telecomunicaciones. Es necesario profundizar en la seguridad como una solución de extremo a extremo.