Grupo Gtd

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Las industrias y la sociedad actual demandan nuevas prestaciones y aplicaciones en línea con la introducción de las nuevas tecnologías (Internet de las cosas, IA y otras), que incorporan factores como ubicuidad de las personas y equipos que facilitan la actividad diaria de las personas. Lo anterior, demanda mayor seguridad y confiabilidad para el bienestar de las personas en la salud pública, seguridad ciudadana, teleeducación, teletrabajo, entretención y otras. La tendencia internacional en materia de servicios de telecomunicaciones se orienta hacia la desregulación, por lo que no parece adecuado agregar un nuevo marco regulatorio sobre la materia en consulta, toda vez que los temas de seguridad de la información y ciberseguridad son exigencias propias de los usuarios y clientes, los cuales son normados mediante contratos de servicios suscritos por ambas partes. Actualmente el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, lleva adelante una agenda para definir la Política Nacional de Inteligencia Artificial, entre cuyas iniciativas incluye “Desarrollo de guías en materias de ciberseguridad, derechos del consumidor y propiedad intelectual”, que en nuestra opinión es transversal a todas las industrias, incluidos

	los operadores de servicios de telecomunicaciones. Por lo anterior, la normativa sobre ciberseguridad debe ser parte de una política transversal, armónica con los principios y buenas prácticas para proteger a la comunidad contra actos ilícitos, contenidos inadecuados o usos indebidos; un marco normativo para propiciar el diseño de un entorno seguro y confiable que permita apoyar el desarrollo de las distintas áreas de la economía de nuestro país Además, dado que en Chile aún no están claramente tipificados los delitos informáticos, la definición de responsables en la cadena de infraestructura, de los diferentes proveedores y capas tecnológicas, hasta la última milla en el cliente final, hace difusa la asignación de responsabilidades. Las ventajas de contar con un CSIRT es que promueve el intercambio de información de ataques y establece una línea base de seguridad que permite gestionar oportunamente los riesgos a nivel sectorial. Sin embargo, para lograr tal objetivo se sobrepasa la frontera actual de propiedad y confidencialidad de la información de cada operador, como son los riesgos y vulnerabilidades detectadas durante las pruebas; y la hace parte de un sistema mayor que de ser a su vez expuesto o vulnerado, durante su tránsito o almacenamiento, pueden afectar

	gravemente la seguridad y reputación de una compañía. Respecto a este artículo, consideramos que toda norma técnica debe ser de aplicación general para todos los operadores de telecomunicaciones – concesionarios de servicios de telecomunicaciones y permisionarios de servicios de telecomunicaciones-, sin diferenciación ya que prestan servicio a la comunidad en general y sus redes, junto con las facilidades que entregan, están interconectadas directa o indirectamente. Por lo anterior, toda la red debe operar y contar con las medidas para que los sistemas de telecomunicaciones sean seguros y eficientes, pues los ciberataques pueden realizarse desde cualquier elemento de la red de telecomunicaciones, y con equipos o sistemas que cumplan con estándares nacionales e internacionales que permitan disponer de servicios de telecomunicaciones eficientes, seguros y continuos.
Artículo 2.	En línea con las recomendaciones de ITU, se debe incluir la definición de Internet de las Cosas (IoT), que considera aplicaciones que integran el quehacer de organismos públicos y privados, cuyas aplicaciones requieren contar con redes de telecomunicaciones modernas, eficientes y seguras.

	b) Los principios de autenticidad y confidencialidad no forman parte de los servicios públicos de telecomunicaciones (MPLS/ISP).
Artículo 3.	Se requiere mayor claridad en la normativa propuesta, respecto del ámbito de aplicación. En efecto, dado el rol de los concesionarios de telecomunicaciones, la toma de decisiones de inversión, normalmente ocurre con anterioridad a la entrada en vigencia de la norma técnica que incorporaran nuevas tecnologías para proveer más y mejores servicios a la comunidad. Se propone en este artículo, que la normativa incorpore una pronunciamiento que propicie la incorporación de los últimos adelantos a nivel mundial que contribuyan a lograr una mayor seguridad en la operación de las redes de telecomunicaciones, es decir, la normativa que dicte Subtel sobre este tema, debe evitar que ésta constituya un freno u obstáculo para incorporar nuevos desarrollos, por el contrario, debe facilitar la incorporación de sistemas que importen mayor ciberseguridad de todos los sistemas que operen en el país, incluyendo entre éstos la instalación y operación de las redes de telecomunicaciones. Concordante con lo anterior, se propone en el ámbito de aplicación de la normativa se incluya, en forma expresa, que ésta tiene por objeto lograr en el país una gestión eficiente y eficaz para armonizar las prácticas y facilitar la coordinación y la interoperabilidad en materia de ciberseguridad de las redes de los distintos operadores de telecomunicaciones que

	proveen servicio en el país.
Artículo 4.	La tipificación de “operador relevante” no está contemplada en la LGT y se considera que sólo importa una nueva diferenciación entre operadores de telecomunicaciones, que considera a los operadores que tienen una mayor participación de mercado, en desmedro de nuevos entrantes. La tipificación de operador relevante y de concesionario o permisionario de servicios de telecomunicaciones que opere redes y sistemas que hayan sido declarados como infraestructura crítica, podría constituir una tipificación redundante. Se reitera lo señalado en el artículo 1°, en cuanto a que toda norma técnica debe ser de aplicación general para todos concesionarios de servicios de telecomunicaciones y permisionarios de servicios de telecomunicaciones, sin diferenciación. En relación con “Criterios de relevancia” se propone que se señale con mayor claridad el rol que le competerá a Subtel en cuanto a “fomentar y proponer políticas de ciberseguridad” para todos los organismos públicos y privados, incluyendo entre éstos a los operadores de telecomunicaciones que operan en el país.

	Un aspecto observado en el documento propuesto es que no se hace distinción entre los problemas de seguridad que afectan a las redes, producto de las acciones sobre los sistemas de comunicación, causados por los ciberataques, que alteran directamente el funcionamiento de las redes en su lógica operacional, respecto de aquellos casos en se afecta a las redes como consecuencia de las acciones que se realizan sobre equipos y elementos de los clientes, servidos por estas redes. Esto último ocurre, por ejemplo, cuando las redes y/o equipos de uno o varios clientes sufren ataques de denegación de servicio (DDoS: Distributed Denial of Service), en cuyo caso, el efecto de degradación de las redes de comunicaciones de los operadores es producto de las condiciones anómalas del tráfico que circula por las redes, pero no por una falla de los sistemas de comunicación en sí. Respecto a esto último, la normativa no dice nada de las atribuciones de los "operadores relevantes" para intervenir el tráfico de un cliente que está bajo la acción de un ciberataque y que afecta (o puede afectar) el servicio a otros usuarios o a toda la red.
Artículo 5.	Para tener certeza jurídica, se propone definir el objeto de la normativa de ciberseguridad, a fin de evitar confusión en cuanto a que la ciberseguridad es aplicable sólo a la operación de las redes de telecomunicaciones, excluyendo a otros organismos públicos y privados en la integración por ejemplo a Internet de las

	Cosas, IoT. Por cierto, la ciberseguridad debe abarcar a las distintas capas y aplicaciones que permiten la conexión a un gran número de dispositivos conectados a Internet a través de las redes de telecomunicaciones. En el inciso segundo de lo propuesto se refieren a "seguridad física", materia que ya está incorporado en los planes preventivo y correctivo que se refiere el Decreto N° 60, de 2012. Compartimos lo indicado en el inciso 4°, dado que, entre los cuales se incluye el criterio de minimizar los riesgos de ciberseguridad durante las distintas fases de sus proyectos desde su diseño, planificación, evaluación, selección de proveedores, adquisición, instalación y puesta en operación. Concordante con lo señalado precedentemente, se considera que lo propuesto es genérico que no requiere ser incluido en la norma ya que está incorporado en el quehacer de cualquier de los operadores de telecomunicaciones. En el inciso 5°, se refiere a que los operadores deberán contar con planes de gestión de riesgos de seguridad con arreglo a principios, estándares y directrices que guarden la debida coherencia con las características de las redes y sistemas. En relación con lo indicado se considera que lo indicado en esta normativa ya está

	incorporado en el decreto 60, de 2012, en cuanto a los planes de mantenimiento preventivo y correctivos. En relación con lo señalado en el inciso 7° sobre la obligación de considerar en sus planes el estado de la técnica y la tecnología disponible en los ámbitos de seguridad de sistemas, se estima necesario para certeza normativa que esta condición se refiera exclusivamente a la tecnología y estado del arte de los sistemas y equipos que el operador está usando o que integrara a su red al amparo de su concesión o permiso, lo que es de su exclusiva responsabilidad para proveer servicios de telecomunicaciones. Respecto a lo indicado en el último inciso, en cuanto a la facultad que se autoasigna Subtel de poder establecer, en consideración a circunstancias particulares de vulnerabilidad, que determinados operadores relevantes deban adoptar los estándares que la autoridad le indique, se considera que tal acción no le corresponde al rol de regulación de Subtel, ya que consideramos que es propio del rol de empresa de adoptar estándares establecidos en normas nacionales y/o en recomendaciones internacionales según su interés empresarial y de su disponibilidad financiera para incorporar los últimos adelantos alcanzados a nivel mundial. Finalmente, la ventaja de contar con un

	CSIRT es que promueve el intercambio de información de ataques y establece líneas base de seguridad que permiten gestionar oportunamente los riesgos a nivel sectorial. Sin embargo, en el camino a lograr tal objetivo, se sobrepasa la frontera actual de propiedad y confidencialidad de la información de cada operadora, como son los riesgos y vulnerabilidades detectadas durante las pruebas; y la hace parte de un sistema mayor que de ser a su vez expuesto o vulnerado, durante su tránsito o almacenamiento, pueden impactar gravemente la seguridad y reputación de una compañía.
Artículo 6.	Se comparte lo propuesto por Subtel respecto de la designación de un representante en calidad de titular y otro suplente de cada operador de telecomunicaciones que opere en el país. En cuanto a las competencias que deba cumplir el titular y/o suplente, consideramos que es de exclusiva competencia de la empresa calificar la o las competencias que deberá reunir sus representantes para reportar sus designaciones. El modo de enviar y recibir información de Subtel, debe aprovechar la experiencia de comunicaciones mediante sistema SGE de Subtel, medios electrónicos durante la crisis sanitaria, a fin de implementar aquellas que han sido exitosas a fin de prevenir errores de notificación u otras a los representantes de las distintas

	empresas.
Artículo 7.	Se requiere realizar inversiones para disponer de un centro de operación de seguridad de redes (SOC) 7x24. Consideramos que el plazo propuesto para reportar un alcance ciberincidencia "Alta" según la "Obligación de reportar ciberincidencia" de 30 minutos, es demasiado breve para calificar si la ciberincidencia es Alta o Media o Baja. Esto es particularmente crítico se está en fase de investigación del ciberincidente. En dicho plazo la gestión se debe centrar principalmente en realizar un buen diagnóstico, determinar la causa, su alcance y posibles soluciones para subsanar la ciberincidencia. Lo anterior, permitirá entregar información de calidad a Subtel. Consecuente con lo expresado precedentemente, se proponen los siguientes plazos: Alta: Las redes o sistemas están fuera de operación; datos personales están siendo extraídos o expuestos; o procesos críticos están siendo alterados o manipulados: 2 horas Media:Las redes o sistemas están parcialmente fuera de operación; datos personales están en riesgo de ser extraídos o expuestos; o los procesos críticos están

	en riesgo de ser alterados o manipulados: 3 horas Baja:Redes o sistemas en operación con fallas reducidas o limitadas: 5 horas En cuanto a lo propuesto sobre la obligación de reportar se entenderá formalmente cumplida, solamente después de que se haya acusado recibo a través de los mecanismos dispuestos para ello, excepto si éstos no se encontrasen disponibles. Se propone que el acuso de recibo sea automático ya que no es responsabilidad de los operadores que se comunique la debida recepción del reporte según el mecanismo y procedimiento establecido por Subtel. Conjuntamente con reportar ciberincidencias, estimamos conveniente que tal información debiera formar parte del intercambio específico y normado de información según el mecanismo o procedimiento de intercambio de información entre organismos públicos y privados para compartir datos útiles para enfrentar posibles ciberincidencias.
Artículo 8.	Para los reportes de ciberincidencias que se extiendan por un período de tiempo que exceda lo establecido en el artículo 7° precedente, se estima necesario que existan informes de avance, no obstante, no es recomendable remitir reportes muy seguidos, sin avances en la solución de la ciber incidencia, por cuanto se restan recursos de la empresa que debieran estar

	asignados a la solución de la ciberincidencia. En el caso de eventos que ocurran en las redes internacionales, los que no son de responsabilidad del operador nacional, se deberá reportar a Subtel según la información que reciba el operador nacional.
Artículo 9.	Lo propuesto implica realizar inversiones y un sistema de gestión de incidentes de seguridad y registro de evidencias. En relación con el contenido de los reportes, se propone tener en consideración la experiencia de la Agencia Europea de la Unión para la Ciberseguridad, ENISA, que ya ha desarrollado reportes que recopilan toda la información gestionada durante los ejercicios de ciberseguridad y la elaboración de informes post-acción, identificando retos y principales acciones. Igualmente, dependiendo del activo de información incidentado, será conveniente evaluar otros marcos internacionales de ciberseguridad como pueden ser NIST, CIS, etc.
Artículo 10.	Estimamos que la calificación propuesta por Subtel de información reservada, debería elevarse también a de uso restringido, a fin contar con el máximo de medidas para prevenir que se pueda revelar cualquier información del contenido del reporte. Será conveniente evaluar quizá en algunos casos utilizar

	mecanismos de encriptación de la misma, especialmente en el resguardo y almacenamiento seguro de la información que se comparte. Concordante con lo anterior, estimamos conveniente que Subtel defina protocolos de seguridad y perfiles de acceso restringido para el contenido de los reportes para cautelar el buen uso de la información para potenciar la seguridad de las redes y continuidad de los servicios de telecomunicaciones. Se sugiere establecer un control de acceso a la información de los reportes debido a su carácter reservado y a importancia de dar seguridad a la operación de las redes. Lo anterior para velar por la integridad de la información, en el sentido de proteger la información, contra la modificación, supresión, creación o reproducción no autorizada.
Artículo 11.	Los criterios para difundir información de ciberincidentes al público general o a terceros, deben cumplir los máximos estándares posible, para resguardar la identidad de la entidad afectada a fin de evitar daño a la imagen reputacional. Se requiere contar con un sistema de comunicaciones privado – encriptado - que resguarde la confidencialidad del intercambio de información entre partes.

	La información histórica de ciberincidentes que almacene la entidad gubernamental debería considerar medidas de seguridad para asegurar la integridad y confidencialidad de la información a fin de evitar fuga de información sensible hacia terceros. En relación con lo propuesto en este artículo sobre la difusión por parte de Subtel de aquellas ciberincidencias, en nuestra opinión, la difusión debiera estar orientada al ámbito técnico o, establecer mecanismos específicos para determinados casos de ciberseguridad, abarcando requisitos técnicos y operacionales, concordantes con las directrices de política de ciberseguridad para organismos públicos y privados. En cuanto al intercambio de información entre organismos públicos y privados en materias de seguridad física y de ciberseguridad de redes y sistemas de telecomunicaciones, se propone que la información sea calificada de uso restringido y confidencial. Sobre el particular, estimamos necesario que Subtel defina protocolos de seguridad y perfiles de acceso restringido al contenido de información con el objeto de cautelar su buen uso y para potenciar la coordinación entre los distintos organismos públicos y privados. Además, se propone a Subtel establecer un control de acceso a la información debido a su carácter reservado y a importancia de prevenir cualquier mal uso por parte de terceras

	personas. La información histórica de ciberincidentes que almacene la entidad gubernamental debería considerar medidas de seguridad para asegurar la integridad y confidencialidad de la información a fin de evitar fuga de información sensible hacia terceros.
Artículo 12.	Conjuntamente con la obligación de los operadores de telecomunicaciones de efectuar de manera oportuna las gestiones para la resolución de ciberincidencias, se estima que la compartición de información entre los organismos públicos y privados, es una herramienta que podrá ayudar a fomentar la coordinación eficaz durante el procedimiento de restablecimiento y respuesta a los incidentes; al contar con mecanismos y/o procedimiento de intercambio rápido de información sobre las amenazas entre los distintos organismos públicos y privados; a fin de detener oportunamente la propagación y, mejorar cómo y qué sectores se han visto afectados; difundir los métodos utilizados para mitigar los daños en los sistemas afectados y finalmente para reducir las vulnerabilidades y la exposición a situaciones de riesgos que conllevan las ciberincidencias. En relación con la resolución de ciberincidencias, reiteramos nuestra sugerencia de tener en consideración la experiencia de la Agencia Europea de la Unión para la Ciberseguridad, ENISA, y de

	otros organismos internacionales que ya han desarrollado experiencias que recopilan información gestionada durante ejercicios de ciberseguridad y la elaboración de informes post-acción, identificando retos y principales acciones.
Artículo 13.	Para la reserva de los datos personales de nuestros clientes y usuarios, Gtd cuenta con procedimientos y protocolos que permite asegurar la privacidad de los datos, los que, bajo ninguna circunstancia o condición genérica, el encargado de Gtd está facultado para incluirlo en un informe de ciberincidencia. Para proporcionar datos personales de clientes y usuarios, es indispensable que su entrega sea exclusivamente por requerimiento expreso de la autoridad competente. Subtel debe definir protocolos de seguridad y perfiles de acceso restringido para cautelar el buen uso de la información de los repostes, a fin de potenciar la seguridad de la red y continuidad del servicio. Subtel debe definir programas de intercambio de información entre organismos públicos y privados, que estipulen un procedimiento de coordinación y divulgación de vulnerabilidades que hayan ocurrido o que puedan ocurrir, establecer pautas mínimas de atención, diseñar programas para la observancia y de notificación de incidentes cibernéticos

Artículo 14.	Estamos de acuerdo con los reportes sean los mínimos necesarios, a fin de no recargar con más obligaciones a los operadores, considerando que a la fecha son numerosos los reportes que los operadores de telecomunicaciones remiten al Regulador. Cabe señalar que toda petición de reportes tiene por objeto lograr soluciones a vulnerabilidades detectadas por un operador o por Subtel.
Artículo 15.	Se considera que no procede establecer que los titulares de redes de servicios de telecomunicaciones, que no sean considerados operadores relevantes, puedan de manera discrecional enviar reportes de ciberincidencias a Subtel. No se condice con el objeto de esta Consulta. En el inciso 2°, no queda claro a que operador se refiere lo propuesto si se aplica a un operador relevante o a otros operadores que no sean calificados de relevantes. El inciso final de este artículo es ambiguo y demasiado amplio en su aplicación. Se podría prestar para interpretaciones erróneas.
Artículo 16.	Las medidas de supervisión y pruebas de seguridad deben ser definidas por cada operador, no impuestas por normativa, lo anterior, teniendo en consideración que

	normalmente la regulación va detrás de los desarrollos e innovación tecnológica a nivel mundial. Para implementar lo propuesto, se requiere de importantes inversiones, que aseguren la recolección de información sensible a vulnerabilidades sistémicas de los operadores, que no deben ser conocidas por terceros.
Artículo 17.	Según la Ley General de Telecomunicaciones, corresponde al Ministerio de Transportes y Telecomunicaciones, a través de la Subsecretaría de Telecomunicaciones, la aplicación y control de normativa legal y reglamentaria sectorial.
Artículo 18.	Es mediante la Ley General de Telecomunicaciones, que se sancionan las infracciones, según lo dispuesto en el Titulo VII de la Ley.
Comentarios Generales.	Sin perjuicio de lo expuesto en el documento en comento, nos parece que la Consulta, no logra definir claramente los principios del documento ni los objetivos que se persiguen con esta normativa. En nuestra opinión, la normativa propuesta debiera estar inserta en un plan nacional sobre políticas de ciberseguridad para entidades tanto públicas como privadas, incluyendo entre estas últimas a los operadores de telecomunicaciones, estableciendo orientaciones y/o mecanismos específicos para prevenir y resolver situaciones de ciberincidencias.

	Estimamos que la normativa técnica debiera propender a que los operadores adquieran las capacidades de respuesta a incidentes cibernéticos, a fin de contar con redes de telecomunicaciones que provean servicios de calidad, seguros, continuos y a costos razonables para las personas. - Se sugiere que en la normativa propuesta se incluyan medidas sobre la protección de la infancia en temas como contenidos inadecuados. - En relación con la entrada en vigencia de la normativa en consulta, se sugiere establecer a fin de dar certeza normativa, que esta norma entrará en vigencia contados seis meses desde su publicación en el Diario Oficial. En ese plazo los operadores de telecomunicaciones podrán coordinar y proceder a su habilitación en lo que corresponda, en forma gradual, teniendo presente factores técnicos y económicos. - Aprovechar entre otros informes de la ITU el denominado Informe Final "Seguridad de la información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad ".