

<b>PREGUNTA CONSULTA SUBTEL</b>	<b>COMENTARIO RECIBIDO</b>
<b>Artículo 1.</b>	<p>Sugerencia de mejora al Artículo 1°. Objeto La presente norma técnica tiene por objeto establecer un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben diseñarse, instalarse y operarse las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones por parte de aquellos titulares de concesión o permiso que hayan sido declarados como operadores relevantes por esta Subsecretaría.</p> <p>De igual manera, esta norma técnica busca normar el envío de información sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deban reportar a la Subsecretaría, con el objeto de coordinar las acciones orientadas mitigar sus efectos y contribuir a una oportuna restitución de los servicios afectados.</p> <p>Propuesta/sugerencia. agregar en este Artículo:</p> <p>"Para lo anterior, SUBTEL/Organismo Ad-hoc, efectuará un levantamiento con apoyo de cada Concesionario que sea considerado, sobre el Estado del Arte inicial en que se encuentra en materia de Ciberseguridad". Lo anterior, permitiendo al Regulador visualizar la real condición de partida al sistema y evitar "Declaraciones de buenas intenciones, escritas en papel"...</p>
<b>Artículo 2.</b>	d) Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante "CSIRT": es el órgano encargado de recibir y analizar reportes de ciberincidencias, con el fin de analizarlos, monitorear el

	<p>desarrollo de éstas, emitir alertas y proponer medidas tanto de mitigación como de prevención, así como la publicación de alertas y guías de buenas prácticas. La denominación CSIRT proviene de la expresión inglesa Computer Security Incident Response Team .</p> <p>¿Sería importante decir dónde y de quién depende este CSIRT en esta definición?, queda en el aire en esta parte...</p>
<p><b>Artículo 5.</b></p>	<p>Los operadores relevantes deberán contar con planes de gestión de riesgos de seguridad formulados con arreglo a principios, estándares y directrices que guarden la debida coherencia con las características de las redes y sistemas a los cuales se aplican.</p> <p>¿Cómo se acreditará o certificarán todos los Planes ex ante?. En caso de discrepancias de criterios con la Autoridad, cuál es el proceso de "arbitraje" ...?</p>
<p><b>Artículo 16.</b></p>	<p>Sería relevante indicar que SUBTEL o el Órgano público encargado que se defina; generará una Plataforma Digital Online para controlar todo el universo de planes y redes. Pensar el control de cumplimiento con transformación digital declarada, debería ser mandatorio en esta normativa.</p> <p>Así, sería más aterrizada y/o creíble...pudiendo contar con el interés autorregulado de los distintos stakeholders.</p>
<p><b>Artículo 17.</b></p>	<p>Artículo 17. Fiscalización</p> <p>Sin perjuicio de lo establecido en el artículo 15° de la presente norma técnica, la Subsecretaría podrá fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta normativa.</p>

	<p><b>Nota:</b></p> <p>Se entiende el cuidado de la redacción jurídica aplicada a este artículo. Sin embargo, sería razonable y alineado con lo propuesto por el suscrito en Art. 16, que se explicitara no un "podrá", si no más bien, un "Controlará 24/7 en digital...", o algo similar". Así forma parte del deber diario del Regulador/fiscalizador, esta relevante área de la Ciberseguridad...</p>
<p><b>Comentarios Generales.</b></p>	<p>Notable aporte del Regulador de Telecomunicaciones. Se agradece la oportunidad de poder efectuar sugerencias, las que pudieran ser objeto de revisión o consideración. Muchas gracias y lo mejor en los pasos a seguir, un abrazo afectuoso.-</p>