Derechos Digitales

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Se limita la aplicación de la norma técnica exclusivamente a aquellos titulares de concesión o permiso que hayan sido declarados como "operadores relevantes" por SUBTEL. Resultaría conveniente que el ámbito de aplicación de la norma técnica sea más amplio, para así ser aplicable a eventuales servicios de telecomunicaciones que no estén en el marco del sistema de concesiones. Por ejemplo, el servicio de notificación de emergencias debería cumplir con estos estándares. Al mismo tiempo, conviene definir de forma más precisas bajo qué circunstancias los incidentes informáticos en materia de telecomunicaciones deberán ser notificados a SUBTEL, el CSIRT de gobierno, o ambos conjuntamente.
Artículo 2.	En general, las definiciones deben ser concordantes con las establecidas con la Política Nacional de Ciberseguridad, a modo de mantener la sistematicidad de enfoques en materia de ciberseguridad. La definición de infraestructura podría tener un numeral propio. Asimismo, no corresponde limitar la infraestructura a aquellos componentes de transmisión de información, ya que también pueden cumplir otros propósitos, como su almacenamiento y procesamiento, se sugiere utilizar el término "soporte" de la información. Respecto de las ciberincidencias, no corresponde limitar su definición exclusivamente al término "acciones". Se

	sugiere su reemplazo por el término “eventos”, capaz de cubrir situaciones como el deterioro de un componente que también pueden constituir un ciberincidente. Al mismo tiempo, no solo la información puede verse afectada, sino también la capa lógica y la infraestructura, de acuerdo a las definiciones de ciberespacio y de ciberseguridad contenidas en la normativa. En cuanto a la gestión de incidentes, la definición debería mencionar que el objetivo es prevenir la ocurrencia de incidentes, detenerlos cuando ocurran y promover la recuperación expedita de los sistemas o servicios, mitigando el impacto de dichos incidentes. Se recomienda definir el concepto de “gestión de riesgos” en los términos establecidos en la Política Nacional de Ciberseguridad, ya que el documento hace referencia al concepto en diferentes artículos.
Artículo 3.	Al igual que en el caso del artículo 1, existe una delimitación del ámbito de aplicación de estas reglas que se limita a los operadores relevantes, dejando fuera la aplicación respecto de incidentes que se susciten por los sistemas u operaciones no incluidos, aun cuando ciberincidentes pudieren afectar a otros sistemas.
Artículo 4.	El artículo se refiere tanto al mecanismo de declaración de un titular de servicios de telecomunicaciones como “operador relevante”, como a los criterios. El título del artículo es insuficiente como referencia para esa actuación de la SUBTEL. Reiteramos que esa operación relevante, si bien puede ser útil para la formulación de obligaciones especiales respecto de estos operadores relevantes, no puede servir para obviar o preterir ciberincidentes que puedan afectar al sistema sin provenir de los sistemas de los operadores relevantes.

	Dentro del listado de los criterios relevantes para esa declaración, se podría considerar incorporar: Capacidad de recuperación (resiliencia) del servicio Número de potenciales afectados por ciberincidentes Respecto del criterio “participación de mercado”, vale la pena mencionar que dicha circunstancia está sujeta a modificarse en el tiempo, por lo cual debe ser revisada periódicamente por el regulador. El artículo debería asegurar la revisión de los criterios por la Subtel.
Artículo 5.	Dentro de las obligaciones de seguridad por cumplirse por los operadores relevantes, se podrían agregar: La designación de un encargado de ciberseguridad que haga las veces de punto de contacto. El cumplimiento del deber de protección de la información desde el diseño y por defecto en todo sistema de información utilizado. Si bien los servicios de telecomunicaciones no necesariamente son considerados como responsables de bases de datos en materia de protección de datos personales, en su calidad de intermediarios corresponde que velen por la integridad, confidencialidad y disponibilidad de la información que transita por sus redes, sea esta personal o no. En este sentido, corresponde el establecimiento de responsabilidades conducentes a la aplicación de medidas técnicas y organizativas apropiadas con anterioridad y durante el la transmisión de la información. Estas medidas deben considerar el estado de la técnica, los costos de implementación y los riesgos

	asociados. De esta forma, las medidas implementadas por el operador deben garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de información, así como evitar evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado.
Artículo 6.	Los encargados de seguridad no solo deben tener las competencias suficientes, sino que gozar de cierto nivel de autonomía al interior de su organización para cumplir su rol, por lo que no basta con una designación dentro de un organigrama existente si no se cuenta con las competencias y atribuciones referidas en el artículo. Se recomienda que, para cumplir con este objetivo, se establezca que deberán ejercer como asesores directos del director ejecutivo u otro alto cargo del operador relevante respectivo.
Artículo 7.	Resulta cuestionable que la obligación de reportar ciberincidencias solo pesen sobre aquellos operadores que fueron declarados relevantes, y no simplemente respecto de todos los operadores de telecomunicaciones. Aunque las sanciones o el estándar de cuidado puedan ser diferenciados, es necesario no excluir al resto de los operadores de la capacidad de reportar, pues puede resultar perjudicial. De esta forma, se podría excluir a los operadores no relevantes de tener un punto de contacto, pero sí establecer el deber de reportar ciberincidencias, aun cuando esta obligación no tenga una sanción aparejada. Por otro lado, la categorización de gravedad de los reportes (alta, media y baja) está establecida en función de si existen o no datos personales comprometidos. Si bien la protección de datos personales es un criterio relevante para estimar el daño actual o potencial, el

	carácter de la información como personal no puede ser un criterio primordial para diferenciar incidentes, puesto que existe información crítica que no necesariamente reviste esta naturaleza (como información estratégica, información confidencial, información agregada que sea conducente a la estabilidad de los servicios, información de carácter técnico de los servicios, etcétera). Por lo demás, en general a los operadores les corresponde ser neutrales y no conocer el contenido que transita por sus redes, por lo cual no les corresponderá a ellos determinar si existen o no datos personales comprometidos. Al mismo tiempo, dentro de los criterios para establecer la gravedad del incidente debe agregarse la probabilidad de poder contenerlo, y la capacidad del operador para recuperar el servicio y atenuar los daños que puedan producirse. Es necesario que el artículo aclare que la obligación de reportar de ciberincidentes respecto de Subtel no obsta a la necesidad de reportar a otras instituciones de ciberseguridad con competencia en su funcionamiento. Es menester crear instancias de coordinación entre distintas entidades para uniformar criterios de reporte de incidentes, esto es relevante para evitar la duplicidad de esfuerzos y los posibles desincentivos por parte de la industria para reportar incidentes de ciberseguridad.
Artículo 8.	El contenido del artículo es adecuado pero no se justifica su separación respecto del resto de las reglas asociadas al procedimiento de reporte contenidas en el artículo 7º.
Artículo 9.	Al igual que respecto del artículo 7º, se recomienda agregar como ítem de reporte la probabilidad de contener el incidente de seguridad (informando así de la estimación de éxito de las medidas), así como la capacidad del operador para recuperar el servicio y de mitigar los daños producidos.

	Por otro lado, al igual que respecto del artículo 7º, resulta necesario mencionar que ciertos sectores podrán verse a notificar los incidentes a distintos organismos públicos (Subtel, CSIRT de gobierno, Comisión para el Mercado Financiero, etcétera), por lo cual sería positivo establecer criterios coordinados para la realización de dichos reportes.
Artículo 10.	Si bien corresponde establecer criterios de reserva respecto de los reportes, es importante establecer de forma explícita, limitada y rigurosa ciertas excepciones para la coordinación y cooperación entre otros organismos dedicados a materias de ciberseguridad. Particularmente, si a futuro se crea una institucionalidad de la ciberseguridad a nivel central. Al respecto, debe encontrarse un equilibrio entre la posibilidad de que las empresas encuentren incentivos para realizar dichos reportes y el hecho de que el ecosistema de la ciberseguridad se beneficia en su conjunto cuando los distintos actores del mismo mantienen un mismo nivel de información sobre las fallas de seguridad que afectan a la industria en su conjunto. Al respecto, resultaría positivo el establecimiento de lineamientos general susceptibles de revisión periódica, similares a los establecidos en el capítulo 20-8 del compilado de normas de la Superintendencia de Bancos e Instituciones Financieras, en particular a lo referido a la información a la industria.
Artículo 11.	En lo relativo a la información que se entrega al público, los reportes que se hagan públicos deben verificar que la información liberada dé cuenta de elementos objetivos y pertinentes, pudiendo mantener de forma reservada determinados elementos del incidente que no resulten relevantes para la finalidad del reporte. La no afectación de la reputación del operador es un

	criterio apenas secundario y no debe incluirse como un requisito para la información al público, sino más bien como criterio para la entrega de información sobre las medidas de mitigación según ya está dispuesto. Lo relativo a la promoción de intercambio de información entre actores públicos y privados en materias de seguridad cumple un objetivo distinto de la gestión de información sobre ciberincidencias puntuales en el resto del artículo 11, y debería ser separado del mismo.
Artículo 12.	La obligación relativa a subsanar las vulnerabilidades que permitan o faciliten ciberincidencias debe concebirse como una obligación de medios y no de resultado. La facultad del inciso segundo de solicitar cooperación al CSIRT de referencia para la resolución de una ciberincidencia debe extenderse a la solicitud de cooperación para subsanar vulnerabilidades, sin alterar la responsabilidad de los operadores por hacer todos los esfuerzos disponibles por subsanar cada vulnerabilidad. A ello debe agregarse la obligación de informar de las medidas adoptadas para subsanar vulnerabilidades, adicionales a la información de las medidas de mitigación de efectos y de restablecimiento de servicios. Como obligación adicional, sería positivo establecer que, en caso de ocurrir incidente de seguridad, el operador tenga la obligación de acreditar haber implementado las medidas de seguridad establecidas en esta norma técnica, en función de los niveles de riesgo y a la tecnología disponible.
Artículo 13.	El artículo debe reflejar al inicio la obligación general de reducir la cantidad de información personal agregada a un informe a aquella estrictamente necesaria para la identificación y contacto de las personas interesadas. Lo

	referido al tratamiento de datos sensibles debe incluir una referencia expresa a las disposiciones que regulan tales datos a modo ejemplar. La obligación de remitir los informes pertinentes a la autoridad pública de control de datos personales debe incluir un plazo máximo para tal remisión, que debe ser breve.
Artículo 14.	No se justifica que la obligación de presentar reportes trimestrales de ciberseguridad se limita a dos capas de ciberespacio (física y lógica), y no a las tres capas establecidas en el artículo 1º. Esto es particularmente relevante respecto a muchas medidas de seguridad relativa a datos personales, que ocurren en la capa de contenidos. A pesar del título del artículo, no está dispuesta de forma explícita la frecuencia de los informes ni las fechas en que se entregarían. Esto último, junto con el período que abarcaría cada informe, debe expresarse como parte del contenido que estará regulado por las instrucciones pertinentes
Artículo 15.	Al igual que en el artículo 7º, se recomienda extender la obligación de reportes sobre ciberincidentes a todos los operadores de telecomunicaciones y no solo a aquellos declarados como relevantes. Si ha de existir alguna obligación diferenciada ella debe referirse al detalle de su contenido y las sanciones asociadas, y no así a la circunstancia de informar ciberincidencias.
Artículo 16.	Hace falta definir de forma más precisa qué entenderá la norma técnica por “planes de gestión de riesgo”. Al mismo tiempo, estos deben enfocarse evitar, reducir y también mitigar los efectos de los incidentes informáticos. Se utiliza el término “gestión de riesgo”, que no ha sido definido, por lo que sería positivo hacer una remisión a la Política Nacional de Ciberseguridad, o

	bien incluirlo con precisión en el artículo 2º. A la vez, es necesario disponer –directamente o remitiendo a instrucciones– cómo se acredita la actualización de los planes y con qué periodicidad mínima ellos deben actualizarse. Respecto de la obligación de realizar pruebas de seguridad, el estándar necesario para entender que estas han sido realizadas a cabalidad debería evaluarse periódicamente por el regulador, el cual podrá basarse en estándares internacionales en la materia. Debe especificarse –directamente o remitiendo a instrucciones– cuál es la regularidad exigida para las pruebas de seguridad. Debe asimismo considerarse un mecanismo de retroalimentación para las observaciones de la Subsecretaría a los reportes de las pruebas de seguridad.
Artículo 17.	Si bien resulta acertado que la norma declare que la Subtel cuenta con la competencia para fiscalizar el cumplimiento de esta normativa, probablemente sea necesario el establecimiento de ciertas competencias relativamente intrusivas para cumplir efectivamente este propósito (por ejemplo, la revelación de algoritmos que pueden estar protegidos por propiedad intelectual), las que necesariamente deberán estar establecidas a nivel legal.
Artículo 18.	Debe hacerse explícito que las sanciones aquí referidas por la infracción de esta propuesta normativa procederán sin perjuicio de las que procedan por infracción de ley, ante la eventualidad de concurrencia de sanciones
Comentarios Generales.	Derechos Digitales valora la iniciativa de la SUBTEL de generar una normativa de ciberseguridad aplicable al sector de las telecomunicaciones. Respecto al documento, adscribimos al grueso de su espíritu y el contenido del articulado. Independiente de los comentarios específicos a cada artículo, los principales elementos que consideramos importante subsanar o

	precisar son los siguientes: 1) Consideramos importante que la norma sea aplicable a todos los actores que participen del sector de las telecomunicaciones, incluyendo a los organismos públicos y no sólo a aquellos operadores que cuenten con una concesión o permiso de telecomunicaciones. 2) Respecto a las definiciones, se recomienda sólo definir aquellos conceptos que son atingentes al ámbito de las telecomunicaciones. Respecto de otros conceptos generales, como ciberseguridad o evaluación de riesgo, corresponde replicar o remitirse a las definiciones contenidas en otros documentos, como la Política Nacional de Ciberseguridad. De lo contrario, se puede generar una falta de armonía en los enfoques que distintos organismos aplican en la materia. 3) Resulta necesario establecer de forma más precisa como la SUBTEL estará coordinada con otros organismos que tengan atribuciones en materia de ciberseguridad. Esto es particularmente relevante respecto a las obligaciones de notificación de incidentes. 4) Es necesario reformular la reserva de información entregada por los operadores respecto a los ciberincidentes reportados. El énfasis debe estar puesto en mantener un equilibrio entre la necesidad de compartir información que resulte pertinente y relevante relativa a incidentes de ciberseguridad en materia de telecomunicaciones, con los incentivos necesarios para que dichos reportes efectivamente se presenten ante la autoridad. 5) La obligación de reportar incidentes de ciberseguridad debe extenderse a todos los operadores de telecomunicaciones, no sólo a aquellos que son declarados relevantes por el regulador.

	6) Es importante establecer criterios de coordinación y uniformar criterios de reporte de incidentes, con el objetivo evitar la duplicidad de esfuerzos y los posibles desincentivos por parte de la industria para reportar incidentes de ciberseguridad