VTR

Propuesta Subtel	Comentarios VTR
Artículo 1	Se debiese explicitar si un objetivo es adicionalmente resguardar la información sensible de los usuarios, en cuyo caso, resulta contraproducente aplicar una norma exclusivamente a algunos operadores pues los usuarios de ISP menos relevante también podrían verse afectados. Si por el contrario el objetivo es exclusivamente resguardar la continuidad operacional del país frente a ciberincidencias, tiene sentido acotarlo a los ISP de mayor envergadura. Aun así, ciertas obligaciones puntuales, como la asociada a reportar incidentes, puede ser conveniente aplicarlas transversalmente a todos los operadores.
Artículo 2	En relación a la definición de Ciberincidencias creemos que se debería hacer referencia a un hecho de facto que generó un impacto y no a los hechos que sólo tienen la potencialidad de afectar el normal funcionamiento ya que esos podrían ser demasiados. En términos generales, se recomienda que las definiciones se apeguen a los términos y normativas estándares aplicables, como por ejemplo: ISO-27001. – ISO-27032
Artículo 3:	Creemos conveniente explicitar que el ámbito de aplicación se acota exclusivamente a resguardar la infraestructura y continuidad operacional de las redes, servicios e información que mantienen los ISP y que no incluye garantizar la seguridad de la información u operación de equipos de propiedad de los clientes del ISP. Los ISP no tienen herramientas para controlar la información que cada abonado pone a disposición de terceros sea voluntaria o involuntariamente o las medidas de protección que implementan para salvaguardar la integridad de sus equipos.
Artículo 4	Los criterios para establecer un operador relevante son vagos, si bien se enumera una serie de criterios, no se establecen los

	umbrales concretos que permitirían calificar a un operador como relevante. Sugerimos indicar cuales serían los "sectores estratégicos" a los que se hace referencia.
Artículo 5	Las definiciones aquí presentadas deben ser explicitas sin cabida a imprecisiones. En ese sentido no resulta conveniente utilizar criterios como "niveles adecuados de seguridad" ya que ello no establece un límite preciso para la definición. Asimismo no resulta conveniente definir que las medidas deban tomar en cuenta "normas y estándares internacionales", "determinaciones nacionales e internacionales" o "de amplia aceptación" en términos generales, sin definir con precisión cuales son. Se recomienda que las obligaciones se apeguen a modelos y a procesos enmarcados en estándares como por ejemplo: ISO-27001/2. – ISO 27005- ISO 27032, enfocadas a la gestión de la ciberseguridad en lo que respecta a la protección de las infraestructuras relevantes para la información. En general proponemos que las obligaciones generales se definan en un proceso consultivo con la industria y se revisen cada 2 años, para mantenerlas actualizadas frente al cambio tecnológico. En relación a las obligaciones específicas que se mencionan: 1) No resulta evidente cuales serían las responsabilidades concretas en relación a la integridad de la cadena de suministros de equipos y software. En general los ISP Chilenos no intervienen en la manufactura de los equipos ni necesariamente en su transporte. La instalación y puesta en marcha normalmente se subcontrata a terceros y en ese sentido debiesen especificarse

	concretamente las condiciones o certificaciones que debiesen cumplir dichos proveedores. 2) Debe especificarse las condiciones para mantener disponible la documentación y demás antecedentes que dan cuenta del detalle de los planes de gestión de riesgos en caso de inspección, por ejemplo, ¿debe estar impreso en el NNOC de cada operador? 3) La obligación de "adoptar los estándares que la autoridad indique" es demasiado genérica, debería especificarse qué estándares se pueden imponer y en qué condiciones. 4) En relación a tener en consideración, a lo menos, las recomendaciones de esta Subsecretaría y del CSIRT en el diseño de las redes y sistemas como la elaboración de los planes de gestión de riesgos, es importantes tener presente que una recomendación de Subtel no es un acto administrativo que obligue al operador relevante de acuerdo con la normativa sectorial vigente. Ni el DL N°1762 ni la Ley N°18.168 le atribuyen a Subtel la facultar de hacer "recomendaciones".
Artículo 6	Estamos de acuerdo con lo establecido en el artículo, todo proveedor debiese tener establecidos los roles y responsabilidades en materia de ciberseguridad y contar con encardados responsables definidos de acuerdo a lo establecido por la norma ISO 27001:2017
Artículo 7	Creemos que se deben establecer los niveles de criticidad de los activos de información y su nivel de riesgo considerando buenas prácticas como la ISO 27005:2018, contando con una buena gestión de incidentes basado en la ISO 27035:2016, con los niveles de escalamiento apropiado (SLA). Además se deben estimar mejor los tiempos de envió de reportes, ya que los indicados pueden causar complicaciones en la atención de incidentes, ya que en la práctica los tiempos de análisis de los ciberincidentes

	requieren mayor tiempo que los propuestos en la normativa. Adicionalmente, creemos que los "umbrales de gravedad", como los demás elementos centrales planteados en esta normativa, debiesen definirse en un reglamento, como ocurre en el "Reglamento para la interoperación y difusión de la mensajería de alerta y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones" En relación a las "instrucciones específicas, tanto de carácter contingente, temporal o periódico que las autoridades competentes impartan en relación a determinadas categorías de ciberincidencias", creemos que es necesario avanzar en especificar concretamente qué tipo de medidas pueden ser solicitadas y bajo qué condiciones.
Artículo 8	Se deben establecer los niveles de criticidad de los activos de información y su nivel de riesgo considerando buenas prácticas como la ISO 27005:2018, contando con una buena gestión de incidentes basado en la ISO 27035:2016, con los niveles de escalamiento apropiado. Pensamos que se deben estimar mejor los tiempos de envió de reportes, ya que los indicados pueden causar complicaciones en la atención de incidentes. En la práctica el análisis preliminar de los ciberincidentes, requiere mayor tiempo que el indicado de 30 minutos.
Artículo 10	Se sugiere que los operadores firmen un acuerdo de confidencialidad en caso de recibir información de cualquier otro operador por parte del CSIRT o Subtel, de manera de resguardar la confidencialidad de dicha información.

Artículo 11	Se sugiere que los operadores firmen un acuerdo de confidencialidad en caso de recibir información de cualquier otro operador por parte del CSIRT o Subtel, de manera de resguardar la confidencialidad de dicha información. Se sugiere establecer criterios con arreglo a los cuales Subtel podrá difundir al público ciertas ciberincidencias. En nuestra opinión la facultad de difundir aquellas ciberincidencias "cuyo conocimiento por parte del público general contribuya a reducir su ocurrencia" debiesen ser ejecutadas por cada ISP, salvo casos excepcionales, como por ejemplo, cuando la ciberincidencia afecte a varios ISP en conjunto.
Artículo 12	Se deben establecer niveles de criticidad de los activos de información y su nivel de riesgo considerando buenas prácticas como la ISO 27005:2018, contando con una buena gestión de incidentes basado en la ISO 27035:2016, con los niveles de escalamiento apropiado.
Artículo 13	Se sugiere que los operadores firmen un acuerdo de confidencialidad en caso de recibir información de cualquier otro operador por parte del CSIRT o Subtel, de manera de resguardar la confidencialidad de dicha información. Los datos personales no sensible (v.gr., cédula nacional de identidad, dirección, etc.) también debiesen quedar sujeto a la obligación relativa a incluirlos en el informe sólo si resulta estrictamente necesario para aquel fin. Asimismo, en caso de que su tratamiento por parte de eventuales terceros sea indispensable, su transferencia debería estar sujeta a que los terceros no pueden comunicarlos a personas naturales o jurídicas externas ni realizar ningún tratamiento de los datos que se aparte del encargo recibido y la finalidad de éste. Lo dispuesto en el inciso segundo es poco claro, considerando que actualmente no existe

	un órgano o entidad encargada en materia de protección de datos. Asimismo, no se indica qué acción debería tomar el órgano en cuestión
Artículo 14	Nos referimos a este artículo en nuestros comentarios realizados al artículo 8 Nos parece que el periodo de los reportes debe fijarse en la norma técnica. Subtel no es competente para crear obligaciones a través de instrucciones.
Artículo 16	Se deben aplicar controles en la seguridad en las operaciones gestionando los análisis de vulnerabilidades a través de estándares como OWASP, OSSTM.
Comentarios Generales	Concordamos en la relevancia de avanzar en buenas prácticas y coordinaciones para mejorar el desempeño de la industria frente a la ciberseguridad. Creemos también que el ámbito de responsabilidad de los ISP debe estar enmarcado en mantener la continuidad de servicio de las redes y resguardar los datos que almacenan de sus clientes, teniendo presente que ningún ISP puede garantizar la seguridad informática de cada uno de sus abonados. Asimismo valoramos la posibilidad que exista una instancia de reporte de incidencias que permita compartir riesgos y avanzar hacia mayores niveles de coordinación de ciberindicencias. Sin embargo, no resulta evidente que Subtel pueda, sin una norma legal que establezca la obligación general de adoptar medidas de ciberseguridad en las redes y sistemas de telecomunicaciones, regular los aspectos tratados en esta norma técnica. Incluso, en el caso de que existiese una norma legal que obligue a los concesionarios y permisionarias a adoptar medidas de ciberseguridad en sus redes y sistemas, los aspectos básicos de aquella obligación legan debiesen contemplarse en un reglamento y no en una normativa técnica. Así, por lo demás, fue lo

	que sucedió con respecto a las obligaciones asociadas a infraestructuras críticas (Ley N°20.478 y Decreto No. 60 de 2012). En atención a lo anterior, estamos a su disposición para participar de una mesa de trabajo permanente para acordar un procedimiento de operación, coordinación y un manual de buenas prácticas con el objetivo de avanzar en la implementación de medidas específicas para toda la industria. Creemos que varias de estas iniciativas pueden ser implementadas basadas en un modelo de autorregulación. Es más, los lineamientos que se puedan obtener de un trabajo conjunto entre empresas y Subtel podría sentar las bases para presentar un Proyecto de Ley que agregue la experiencia de empresas y autoridades. En relación al contenido de la normativa técnica sujeta a consulta, consideramos importante avanzar en definir una normativa sin ambigüedades y siendo específicos en las obligaciones que se soliciten a los operadores. Nos preocupa que desarrolle una normativa donde no estén claros todos los conceptos y alcances de la misma, en ese sentido, consideramos necesario establecer con mayor precisión el alcance y estándares que regirán la normativa. El marco regulatorio que establezca las buenas prácticas de un SGSI debería aspirar a basarse en estándares concretos, ejemplo de ello pueden ser estándares internacionales ISO-27001 – ISO 27005, para resguardar la integridad, disponibilidad, confidencialidad y privacidad de la información.