CORPORACION INSTITUTO PROFESIONAL INACAP.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	En rigor la criticidad está en los servicios en primer lugar, en segundo lugar, la infraestructura y en tercer lugar el operador. Al parecer se define como más importante al concesionario. En la actualidad los grandes operadores disponen de concesiones por telefonía fija, internet, televisión y servicios móviles, siendo la telefonía de mayor criticidad que la televisión. La ciberseguridad debe asegurar también un mínimo de riesgos y amenazas para los usuarios finales de los servicios, los riesgos asociados no son solamente relacionados con la infraestructura y los servicios, sino que también con los comportamientos de los usuarios. "Interrupción, destrucción, corte o fallos" también se debería agregar “perturbación" o "degradación". No siempre un incidente tiene consecuencias tan drásticas. Puede también generar molestias para los usuarios (degradación de velocidad, tiempo de acceso, por ejemplo). Probabilidad de materialización de una amenaza, implica ser capaz de cuantificar la probabilidad. Es mejor hablar de nivel de riesgo (bajo, mediano, alto, crítico).
Artículo 2.	Como pregunta general, ¿estas definiciones se encuentran alineadas a las que manejan otras instancias de Gobierno, tales como el CSIRT, Mesa Técnica de Ciberseguridad y las regulaciones en tramitación en materia de delitos informáticos y ciberseguridad. Considerando el uso de definiciones únicas para estos conceptos entre los distintos Ministerios.

	En la definición de Ciberespacio no indica a que se refiere con el término interacción social, si apunta a la comunicación, a los datos o transacciones. Además, en las infraestructuras tecnológicas que corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, el cual se ejemplifica, no indica quién o como se definen los otros equipos, por ejemplo, planta externa, sistemas de energía, clima, edificios, canalizaciones. Sólo se menciona equipamiento directo de telecomunicaciones y no la infraestructura de soporte, protección o de servicio. En Infraestructura crítica de telecomunicaciones, sólo se refiere a afectación de la disponibilidad de servicios y no considera la degradación de servicios ya sea intencional, intervención para manipulación sin interrupción y/o espionaje. En Operador relevante, un operador relevante podría comercializar servicios superfluos y transportarlos por redes e infraestructura crítica. Dichos servicios quedarían protegidos por la Ley de Ciberseguridad. La calificación aplica sobre la empresa operadora y no sobre los servicios críticos.
Artículo 3.	Al mencionar que esta norma técnica solamente se aplica al diseño, instalación y operación de redes, no queda claro si las funciones de mantención preventiva y correctiva están incluidas, ya que son diferentes de la de operación. Dichas funciones si no son realizadas o realizadas en forma deficiente, serán causa de fallas o vulnerabilidades. El decreto 18/2004 considera el servicio de acceso a internet y los servicios públicos del mismo tipo que no están descritos en forma explícita en la Ley 18.168.

	¿Podrían o deberían estar ambas? No se considera el factor de riesgo más alto de una empresa, el factor humano, esta es la parte más vulnerable de un sistema, bajo cualquier mirada.
Artículo 4.	En el punto c) Impacto social o económico de eventuales interrupciones. No considera degradación del servicio o infiltración que afecte la seguridad. Cuando se menciona, todo concesionario o permisionario de servicios de telecomunicaciones que opere redes y sistemas hayan sido declarados infraestructura crítica por esta Subsecretaría. Es relevante que la definición de Infraestructura crítica posea una sola definición a nivel país, por lo tanto, debe estar alineada a lo definido en los marcos regulatorios ya existentes, o en una Ley de Protección de Infraestructura Crítica, o a una definición anterior que ya esté siendo manejada por el CSIRT u otra instancia competente que la defina y que sea única para Chile.
Artículo 5.	El uso del concepto “adecuadamente” y “adecuado” en los párrafos iniciales es ambiguo, sería importante considerar la definición de niveles de servicio y/o cumplimiento claros, para la determinación de los riesgos, seguridad, etc. Para lo conceptos descritos en este artículo de a) a l), se hace necesario poseer una única definición con las demás instancias de Gobierno y Ministerios. Para los conceptos, c), d), e), f), g) y h). Estas funciones corresponden a funciones de disponibilidad de servicio,

	aseguramiento de la calidad de servicio, gestión del tráfico, carga y rendimiento en virtud de la definición de ciberincidencia. Globalizarlas bajo el concepto de seguridad implica ampliar su campo a situaciones, por ejemplo, de fuerza mayor qué interrumpen los servicios (accidentes, catástrofes, etc.) Bajo este contexto, si un camión choca un poste y corta cables de fibra óptica, será tratado como una ciberincidencia al igual que un ataque. Esto podría llevar a una sobrecarga de los sistemas y equipos de ciberseguridad para resolver problemas operativos o de contingencia que ya están al menos declarados y calificados en la normativa vigente. Cuando se menciona que, "los operadores relevantes deberán tomar las medidas adecuadas para prevenir y reducir al mínimo los efectos de las ciberincidencias". ¿Cuáles son esos mínimos? Cuando se menciona, "el uso de estándares internacionales, independientes o nacionales, de amplia aplicación". Es necesario que se definan cuáles deben ser considerados como referencia, debido a que estos son diversos y sus definiciones también. En el párrafo 4, cuando se menciona "Los operadores relevantes de servicios de telecomunicaciones deberán aplicar criterios orientados a minimizar los riesgos de ciberincidencias y a facilitar una adecuada gestión de éstos durante su operación…", se identifica: • Es necesario especificar claramente cuáles son los criterios orientados a minimizar los riesgos de ciberincidencias.

	• ¿Cómo se verificará? ¿Cómo se mide?, ¿Cuál es el nivel mínimo de servicio necesario? • Se omite el período de explotación o de funcionamiento que es cuando interesa asegurar la gestión de los riesgos, ya que los servicios se encuentran activos o en operación. Sólo considera el diseño e implementación de redes e infraestructura. En el párrafo 5, se menciona que, "operadores relevantes deberán contar con planes de gestión de riesgos de seguridad formulados con arreglo a principios, estándares y directrices". No se indica a que estándares se refiere, cómo se determinan, o quién los establece. En el párrafo 6, se menciona que, "tanto el diseño de las redes y sistemas como la elaboración de los planes de gestión de riesgos serán de responsabilidad exclusiva del respectivo operador relevante". Esto implicará un aumento de los costos del operador y se supone un aumento en los precios y tarifas de los servicios. Al incluir las funciones de disponibilidad del servicio, calidad, tráfico y de resolución de eventos accidentales o catastróficos, qué en la actualidad ya se están gestionando, en virtud de la normativa vigente, implica derivar los costos de operación a la seguridad en virtud de la definición de ciberincidencia. Fiscalizar que los operadores cumplan con la norma se hace necesario ya que no es suficiente, lo que existe a la fecha. Se debieran crear mecanismos de certificación de los operadores que aseguren la calidad de las medidas de ciberseguridad para los usuarios finales

Artículo 6.	Cuando se menciona que, "Todo operador relevante deberá contar permanentemente con, a lo menos, un encargado titular de ciberseguridad en funciones y un suplente, quienes deberán poseer las competencias suficientes para identificar los riesgos de afectación de los servicios de telecomunicaciones". No se especifica a que "competencias suficientes" se refiere, cómo se determinan, o quién las establece. Encargados de Ciberseguridad. Oficial de Seguridad. Terminología internacional.
Artículo 7.	En el párrafo 1, cuando se menciona, "Los operadores relevantes deberán reportar oportunamente a la Subsecretaría de Telecomunicaciones". El uso de "oportunamente" es subjetivo, se puede hacer mención a los plazos entregados a continuación, en la tabla de alcance de la ciberincidencia v/s tiempo para reportar ciberincidencia. En la tabla, es necesario especificar más claramente cuando las redes o sistemas están "fuera", "parcialmente" o "fallas limitadas", debido a que esto llevará a considerar como ciberincidencia problemas comunes de los servicios. Un ejemplo, en la tabla, en alcance "Alto", para el campo descripción, cuando se menciona "Las redes o sistemas están fuera de operación". Considerar que problemas accidentales en planta externa, aumento excesivo del tráfico, situaciones de corte de energía que por su duración superan las capacidades de los respaldos (por ejemplo y corte de 3,5 horas afecta en 30 minutos los sistemas que cuentan con respaldo de energía por 3 horas), lluvias, inundaciones, sismos, sunamis en región costera, etc. serán tratadas como ciberincidencias.

	En el párrafo siguiente a la tabla, cuando se menciona, “las autoridades competentes impartan en relación a determinadas categorías de ciberincidencias”. No indica a que “categorías de ciberincidencia” se refiere, cómo se determinan, o quién las establece. No se identifican acciones que considere el nivel para los casos críticos.
Artículo 8.	Cuando se menciona, “En caso de ciberincidencias que se extiendan por un período de tiempo que exceda de treinta minutos”. ¿Por qué 30 minutos? Se sugiere debería ser con relación a un índice de gravedad (por definir). Por ejemplo, atentados al sistema de comunicaciones y alarmas (en general a la infraestructura crítica), con el objeto de cometer delitos mayores y que produzcan interrupciones menores de 30 minutos, no serán informados ni gestionados porque la norma así lo permite.
Artículo 9.	En la descripción de los datos d) a m), no menciona los servicios afectados y que son finalmente los que pueden, o no, incidir en las actividades normales de clientes y usuarios. Un operador relevante puede tener concesión y/o permiso para brindar servicios de telefonía y televisión. Si la indisponibilidad es de telefonía o de televisión ¿tendrá la misma categorización y tratamiento? En el último párrafo, cuando se menciona que “el operador afectado deberá conservar por, a lo menos, seis meses desde el cierre de la ciberincidencia, todos los logs y registros que hubieren podido registrar efectos y actividades relacionadas con el posible ataque”, Se observa necesario, que la autoridad considere el desarrollo de una plataforma informática, de recepción automática y almacenamiento de datos, además de reportes de ciberincidencia, que permita

	cautelar que los datos no sean manipulados posteriormente y que permita efectuar investigación y gestión sobre la información relevante. Además, se identifica que 6 meses de observación es poco, internacionalmente las observaciones/investigaciones duran más de un año de trabajo, teniendo en cuenta además el resguardo de la data.
Artículo 10.	Respecto a la reportería, es relevante considerar una plataforma informática para la administración de la información, su seguimiento y análisis posterior. Mantenido un historial que permita efectuar investigaciones posteriores.
Artículo 11.	En el párrafo 2, se menciona que la "la Subsecretaría de Telecomunicaciones podrá difundir aquellas ciberincidencias cuyo conocimiento por parte del público general contribuya a reducir su ocurrencia o mitigar su eventual impacto". ¿Cuál será el mecanismo?
Artículo 12.	Sin Comentarios.
Artículo 13.	Se menciona la manipulación de "datos personales de carácter sensible", sería relevante tener una definición común con otras instancias de Gobierno y Ministerios para evitar la subjetividades y mal uso de información por omisión.
Artículo 14.	Respecto a la reportería, es relevante considerar una plataforma informática para la administración de la información, su seguimiento y análisis posterior. Mantenido un historial que permita efectuar investigaciones posteriores.
Artículo 15.	Hay reportes que, si se debieran considerar, aquellos de causa¿ efecto, a nivel internacional estos son de alta relevancia, ya que al creer que está todo solucionado, quedan vestigios que generan nuevos ataques, en el ámbito de la ciberseguridad se conocen como "ataques

	de rebote".
Artículo 16.	En el párrafo 2, se menciona, "los operadores relevantes deberán someter regularmente sus redes y sistemas de telecomunicaciones a pruebas de seguridad". Se debería definir una periodicidad porque "regularmente" es subjetivo. En el párrafo 2, se menciona, "En todo caso, deberán efectuarse conforme estándares actualizados, sean internacionales, independientes o nacionales, o bien, conforme criterios ampliamente aceptados por la industria de las telecomunicaciones". ¿Estos estándares estarán previamente definidos por la SUBTEL?
Artículo 17.	Sin Comentarios.
Artículo 18.	Sin Comentarios.
Comentarios Generales.	El Área Informática y Telecomunicaciones de INACAP, posee más de 20 años en el desarrollo de los profesionales en carreras, tanto técnicas como profesionales, en Técnico en Telecomunicaciones, Conectividad y Redes e Ingeniería en Telecomunicaciones, Conectividad y Redes; en el Sistema de Educación Superior, posee la mayor presencia nacional en 17 sedes de Arica a Punta Arenas y segunda en cantidad de estudiantes. Además desde el año 2017 ha fortalecido el desarrollo de las capacidades en el ámbito de la Ciberseguridad. Participantes del Análisis. • Jorge Olivares A., Docente Ruta Telecomunicaciones, Conectividad y Redes, Sede Santiago Sur • Armin Brun R., Docente Ruta Informática, Sede Santiago Centro

	• Lidia Herrera M., Directora de Carrera sede Valparaíso • Rodrigo Silva S., Asesor de Programa de Estudios, Área Informática y Telecomunicaciones • Karin Quiroga S., Directora Área Informática y Telecomunicaciones