Kenneth Pugh Olavarría

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Se sugiere reemplazar "norma técnica" por "norma general", en atención a que la institucionalidad en Ciberseguridad se encuentra en desarrollo, la actual es aún transitoria y se debe esperar a que el Ejecutivo defina el nuevo sistema nacional de ciberseguridad nacional. Agregar en el inciso primero la palabra protegerse para que diga: "diseñarse, instalarse, operarse y protegerse". En el mismo inciso sugiero eliminar la frase "que hayan sido declarados como operadores relevantes por esta Subsecretaría", porque lo que se busca establecer un estándar para todos los operadores titulares de concesión o permiso redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, no solo los que han sido declarados como "relevantes". En el inciso segundo se sugiere cambiar "normar" por el verbo "regular". Se sugiere también especificar el reglamento o cuerpo legal que establece el procedimiento, plazo y departamento de la Subsecretaría encargado de recibir dichos reportes. De esta forma, la frase quedaría "(…) deban reportar a la Subsecretaría, según (el decreto, la resolución, Nº de ……), con el objeto de (…)". Al final del mismo inciso se sugiere ampliar el sentido, para que la norma señale "de las redes, sistemas o servicios afectados". Agregar un nuevo inciso tercero que señale:

	“Esta norma busca generar confianza en dichas redes, sistemas y servicios aumentando sus grados de ciberseguridad, en concordancia con las Política Nacional de Ciberseguridad vigente y las demás normas legales relacionadas.”. Eliminar la palabra "relevantes".
Artículo 2.	Se sugiere cambiar "norma técnica" por "norma". a) Ciberespacio: Reemplazar texto "es el ambiente compuesto por: “se entenderá por tal aquel que comprende (…)” . También reemplazar “sociales” por: “de todo tipo”. b) Ciberincidencia: Reemplazar inicio por: "es toda acción o hecho de cualquier naturaleza que comprometa o amenace”. c) Ciberseguridad: Agregar al final el concepto de "prácticas" para que el texto diga: "políticas, técnicas y prácticas". d) CSIRT: Se debe señalar que existen para cada sector de la industria, al igual que en el Estado y que se coordinan en red. e) gestión de incidentes: Agregar después de la palabra procedimientos: “y protocolos (…)”. Al final donde dice "ésta", eliminar tilde. f) Infraestructura crítica de Telecomunicaciones: Cambiar inicio por: "es el conjunto de redes y sistemas físicos o virtuales de telecomunicaciones, de carácter esencial y/o estratégica, y cuya perturbación, interrupción, destrucción, intervención, corte o fallo generaría un serio impacto en la seguridad, privacidad o disponibilidad de servicio de instituciones y población afectada"

	Se sugiere además incluir las definiciones de los siguientes términos: j) SISTEMAS DE COMUNICACIONES: Según lo define la ley general de telecomunicaciones se sugiere incluir además una definición lo suficientemente amplia que permita considerar en nuevas alternativas y tecnologías como por ser LES: Low Orbit Satellite, MES: Medium Orbit Satellite, enlaces ópticos, enlaces radioeléctricos de cualquier tipo, conexiones virtuales sobre portadoras (p.ej: redes eléctricas), enlaces y conductos subterráneos, y otros , y que pueden ser vulnerados por terceros. Con todas sus componentes, partes y piezas que permitan una comunicación digital o transmisión de datos. k) Seguridad de los sistemas': significa la capacidad de los sistemas de resistir cualquier acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos procesados en los sistemas o de servicios ofrecidos por, o mediante, aquellos sistemas l) Red y sistema de información: significa una red de comunicaciones electrónicas dentro del de lo definido por la ley general de telecomunicaciones, cualquier dispositivo o grupo de dispositivos interconectados o relacionados, uno o más de ellos, conforme a un programa, lleva a cabo procesamiento automático de datos digitales o datos digitales adquiridos, almacenados, procesados, recuperados o transmitidos por elementos mencionados con el propósito de su operación, uso, protección y mantención;

	m) Ciberincidente: significa cualquier evento en el sistema que comprometa o tenga un efecto perjudicial a la seguridad del sistema; n) Proveedor de servicios de comunicaciones o) Servicio esencial o crítico p) Operador de servicio esencial o critico q) Gestión de incidente r) Responsable de la red s) Responsable SUBTEL de la gestión de esta norma (el interlocutor subtel-proveedores) t) Responsable de la operación de la red (p.ej: CISO) u) Vulnerabilidad: según su tipo (física, virtual, canales, intervención, etc). v) Que pasa con los proveedores de servicios de nube, data centers y otras componentes de las redes informáticas, w) Resiliencia x) Trazabilidad y) Competencias de Ciberseguridad: es preciso determinar la calidad y preparación de las personas que intervienen en la ciberseguridad con cursos formales y competencias acreditadas por organismos competentes y reconocidos.

	z) Neutralidad Tecnológica
Artículo 3.	Se sugiere cambiar "norma técnica" por "norma". Se sugiere cambiar donde dice: "al diseño, instalación y operación de redes y sistemas" por: "al diseño, instalación, protección y operación de redes, servicios y sistemas".
Artículo 4.	Es necesario establecer la forma, vigencia y alcance en la aplicación de estos criterios, y eventualmente establecer categorías de afectación según la relevancia. Esta determinación se realizará conforme a los criterios que establezca esta subsecretaria, de acuerdo con los procedimientos que establezca, y serán revaluados periódicamente y comunicados a las partes y tendrán efecto inmediato. La declaración de relevancia será establecido y comunicada al operador por SUBTEL en un plazo determinado, en forma oficial (definir claramente la forma y alcances) estableciendo las zonas y áreas de afectación consideradas. Consideraría los siguientes criterios: a) Extensión territorial del servicio, densidad promedio del mismo, cobertura efectiva b) Sustituibilidad del servicio; c) Impacto social o económico de eventuales interrupciones, en consideración de su duración, población o servicios afectados. d) Impacto geopolítico de la vulnerabilidad

	e) Atención a sectores estratégicos, zonas extremas y territorios especiales en los que opere (debidamente priorizados según criterios establecidos) f) Participación de mercado; g) Daño a la imagen del proveedor
Artículo 5.	Reemplazar el texto: "Los operadores relevantes de servicios de telecomunicaciones deberán determinar" por: "Los operadores de servicios de telecomunicaciones tendrán como obligación determinar"... Eliminar la palabra "relevantes". Agregar despues de "seguridad" la palabra resilencia para que el texto diga: "seguridad y resiliencia de las redes". En punto f) agregar al final: "y patrullaje a las instalaciones físicas" En punto g) cambiarlo para que señale: actividades periódicas de supervisión, auditoría y prueba, incluidos simulacros de ciberincidentes y ejercicios nacionales en el mes de Octubre, de acuerdo a lo señalado en la Ley 21.113. En punto h) Especificar cuáles van a ser esas normas y estándares internacionales. Son muchos y una norma técnica los debe enumerar y señalar si se cumplen en su totalidad o sólo algunos artículos. En punto i) agregarr después de "conocimiento": y difusión interna Sugiero eliminar el punto k) dado

	corresponde a una decisión de otro nivel de competencia el que decidirá que tipo de equipamiento estratégico se empleará el país, el que puede seguir las directrices del "Comercio Estratégico Internacional", definidas por la Cancillería, o decidir la "Neutralidad Tecnológica" para el equipamiento. Sugiero eliminar el punto l), dado no permitiría materializar el objetivo E) de la Política Nacional de Ciberseguridad (PNCS-2017) al no permitir el desarrollo de una Industria Nacional de Ciberseguridad especialmente en el desarrollo de software y criptografía nacional. Los equipos de telecomunicaciones digitales actualmente son del tipo SDR (Software Defined Radios) y se puede mejorar o proteger su desempeño con conocimiento y capacidades nacionales, tal como lo pretende el futuro "Instituto de Telecomunicaciones Inteligentes" que está desarrollando la PUCV y el "Instituto Nacional de Ciberseguridad" - INCIBER - en Valparaíso. Sugiero agregar un nuevo punto: m) disponibilidad de respaldos de equipos y sistemas críticos de rápido reemplazo o redundantes Eliminar en el inciso tercero las palabras "relevantes" y agregar " y resilencia" después de la palabra "seguridad". En el mismo inciso tercero sería apropiado que la autoridad establezca o sugiera algunas referencias específicas. 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, no obstante que, en todos los casos, deberá tener en consideración, a lo menos, las recomendaciones de esta Subsecretaría, del CSIRT de referencia (Aquí falta mayor detalle, a cual CSIRT se refiere en específico) y de todas las entidades que participen del Sistema Nacional de Ciberseguridad., según lo defina las leyes aplicables. En el mismo inciso tercero agregar después e la palabra "Contratistas" el texto: "con las apropiadas credenciales y certificaciones de competencias" En inciso siete, cambiar texto después de las palabras "gestión de riesgos" por el siguiente: "deberán entregarse y actualizarse al menos anualmente a SUBTEL, en la forma que ésta determine, quién llevará registro de ellos. Del mismo modo, deberán encontrarse disponibles, trazables y actualizados cuando se efectúen ejercicios de gestión de incidentes y simulacros de crisis organizados por la autoridad nacional en materia de ciberseguridad".
Artículo 6.	Se debe definir, normalizar y estandarizar los términos los que se usan en la industria, por ejemplo el de CISO (Chief Information security Officer) y recomendar que en los gobiernos corporativos se considere un director con experiencia certificada y acreditada en Ciberseguridad. Los "encargados de ciberseguridad" deben existir en los niveles de la operación de los procesos controlados por el gerente general y también en los procesos estratégicos que conduce el directorio o el gobierno corporativo,

	Eliminar la palabra "relevantes.
Artículo 7.	Eliminar la palabra "relevantes". Los ciberincidentes que comprometen la integridad del sistema de telecomunicaciones, especialmente los ciberataques a la infraestructura, deben ser reportados de forma instantánea, dado se deben tomar acciones a nivel nacional que permitan enfrentar esa amenaza. Esto se puede realizar de forma automática o semiautomática de acuerdo al nivel de madurez en ciberseguridad alcanzado. Las telecomunicaciones son la parte mas importante de la "Infraestructura Crítica de la Información", por lo que es la autoridad nacional, dependiente actualmente del Ministerio encargado de la Seguridad Pública quien debe definirlo. La Ciberseguridad tiene dos partes, el espacio "Ciber" y la "Seguridad" que es responsabilidad de ese ministerio. Este artículo se debe redactar en base a lo que ese ministerio señale. Los reportes deben ser en línea y en red, usando sistemas transaccionales seguros, por la criticidad y sensibilidad de los datos entregados, usando tecnologías del tipo blockchain o de "ledger distribuido". De ser necesario cierta información puede ser anonimizada si así se requiere. En el caso que el Ciberincidente esté además asociado a la pérdida, destrucción o alteración de información de datos personales, esto se deberá ser denunciado y reportado a la Brigada de Cibercrimen de la PDI por constituir un delito informático y a la agencia encargada de la protección de

	datos, una vez ella entre en servicio.
Artículo 8.	La actualización de reportes después de un ciberincidente deberá ser una práctica habitual, ampliando la información ya entregada y señalando las acciones realizadas. Se podrá definir intervalos de tiempo definidos (por ejemplo cada una hora) dependiendo de la gravedad de ellos. Esta política debe ser definida por la autoridad nacional de ciberseguridad y aplicarse de igual forma o diferenciada para otras industrias que dependan de las telecomunicaciones para sus procesos críticos.
Artículo 9.	Eliminar la palabra "relevantes". Cambiar en b) Jefe de seguridad y encargado de seguridad por CISO Aumentar a tres años el tiempo mínimo para mantener registro de los Ciberincidentes, dado hay ciberataques que una vez logrado ingresar a los sistemas pueden estar esperando por mucho tiempo para ver el comportamiento de la organización, realizar movimientos laterales para ocultarse y finalmente cuando así lo quieran, realizar el ataque. Este plazo puede incluso superar un año.Esto se describe en la literatura especializada con el "Kill Chain", término acuñado por Lockheed Martin de USA.
Artículo 10.	Se debe definir con mayor precisión en el concepto de "tratado con reserva" y "tendrá especial cuidado". si esta es información sensible. De ser así debe estar protegida por una clasificación tal que permita perseguir como delito a quien la divulgue, si ella afecta la seguridad del

	país. Eliminar la palabra "relevantes".
Artículo 11.	Eliminar la palabra "relevantes". Se sugiere cambiar el término "podrá" por uno más imperativo, dado en Ciberseguridad por regla general no se compite. SE COLABORA. Al igual que en el fraude, no se compite, se colabora para proteger a toda la industria. Se debe evitar que los operadores manejen a discreción el intercambio de información relevante. Se debe precisar a cual CSIRT se va realizar el reporte.
Artículo 12.	Se debe precisar cual es el "CSIRT de referencia". Una vez superada una ciberincidencia, los operadores deberán elaborar un informe de evaluación (assesment) de la contingencia, con un resumen de los acontecimientos y principales medidas adoptadas, y que servirá para mejorar sus procedimientos operativos y capacitaciones, los que posteriormente deberán ser verificados por la autoridad fiscalizadora. Eliminar la palabra "relevantes".
Artículo 13.	El tratamiento de los datos personales debe hacerse de acuerdo a la nueva ley de protección de datos personales, que sigue la línea del reglamento europeo de datos personales (GDPR). No se podrá hacer uso de esta información de forma discrecional, sin contar con el consentimiento del titular de los datos.

	En el caso que el Ciberincidente esté además asociado a la pérdida, destrucción o alteración de información de datos personales, esto se deberá ser denunciado y reportado a la Brigada de Cibercrimen de la PDI por constituir un delito informático y a la agencia encargada de la protección de datos, una vez ella entre en servicio.
Artículo 14.	Eliminar la palabra "relevantes". Los reportes trimestrales no eximen la emisión de informes cuando se producen ciberincidentes, por lo que se sugiere evaluar la pertinencia de este artículo, que podría sólo ser una medida burocrática administrativa sin sentido. Se ha propuesto en el Artículo 16 el envío del plan de gestión de riesgo actualizado y esta periodicidad de seis meses parece más adecuada, además del informe que se genere cuando ocurran los incidentes.
Artículo 15.	Eliminar la palabra "relevantes". Todos los operadores deben informar los ciberincidentes. No solo los relevantes. Se debe precisar cuales son las "autoridades competentes".
Artículo 16.	Eliminar la palabra "relevantes". Dada la rápida evolución de las "ciberamenazas": "los operadores deberán actualizar a lo menos cada 6 meses los planes de gestión de riesgos" y así precisar un tiempo específico para poder fiscalizar. Se debe registrar la identificación completa de todas las personas que hayan realizado pruebas de seguridad por parte de terceros

	externos especializados.
Artículo 17.	Se debe agregar además que la Infraestructura Crítica de la Información podrá ser también fiscalizada por una entidad dependiente del Ministerio encargado de la Seguridad Pública, especializada en temas de ciberseguridad o ciberdelitos. Este artículo debe referirse al artículo 16°, dado el artículo 15° se refiere a los "Reportes no obligatorios".
Artículo 18.	Se debe especificar de qué ley se trata.
Comentarios Generales.	Se sugiere utilizar un solo término para referirse a la Subsecretaría de Telecomunicaciones, ya que a través del texto este se refiere tanto a "Subsecretaría" como a "Subtel". Toda referencia a legislación específica debe individualizarse explícitamente señalando, a lo menos, número y título. Mas que una "Norma Técnica" se debe señalar que es una "Norma General" en atención a que la institucionalidad en Ciberseguridad se encuentra en desarrollo, la actual es transitoria y se debe esperar a que el Ejecutivo defina el nuevo sistema nacional de ciberseguridad nacional. Esta norma se debe aplicar a TODOS los operadores y no solo a los "relevantes", dado que al no hacerlo así, se deja vulnerable luego a todo el sistema por las brechas que se pueden explotar.