Michael Heavey 2 samsing

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 2.	Un glosario de terminos y definiciones facilitan la implementación y fiscalizacion de la norma. es necesario homologar las practicas y usos de ciberseguridad, telecomunicaciones e informatica con terminos internacionales y propios de la industria de manera de tener referencias comunes, Mientras mas definciones mejor, y tambien incluir el alcance de las mismas Se sugiere incluir las siguientes definiciones, entre otras.: j) SISTEMAS DE COMUNICACIONES: Según lo define la ley general de telecomunicaciones (Nota y 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 critico 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) Competencia del personal: es preciso determinar la calidad y preparación del personal interveniente en la ciberseguridad. Cualquier otro término no definido en esta norma técnica tendrá el significado que se le atribuya en la respectiva normativa sectorial de telecomunicaciones, o internacional de telecomunicaciones que Chile hubiera suscrito. (Nota: Los cambios tecnológicos podrían generar un rezago en las definiciones, sugeriría que se considere otra manera de actualizar definiciones reconocidas internacionalmente…)
Artículo 5.	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. 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, no obstante que, en todos los casos, deberá tener en

	consideración, a lo menos, las recomendaciones de esta Subsecretaría, del CSIRT de referencia (creo que falta mayor detalle, a cual CSIRT se refiere en especifico)y de todas las entidades que participen del Sistema Nacional de Ciberseguridad., según lo defina las leyes aplicables (esta frase la pondría más arriba) La documentación y demás antecedentes que den cuenta del detalle de los planes de gestión de riesgos deberán entregarse y actualizarse al menos anualmente a SUBTEL, en la forma que esta determine, quien llevará registro de estos. 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 competente en materia de ciberseguridad. Asimismo, los operadores relevantes deberán considerar en sus planes el estado de la técnica y la tecnología disponible en los ámbitos de seguridad de sistemas, seguridad de instalaciones, resiliencia, continuidad de la operación, gestión de ciberincidencias y monitoreo de redes; los lineamientos y recomendaciones de organismos internacionales de estandarización y aquellos sugeridos por la autoridad (NOTA P.ej:referidos por la autoridad) ; los servicios de capacitación en ciberseguridad disponibles en el mercado; y cualesquiera otras consideraciones que contribuyan a una gestión más segura de las redes y sistemas.

	No obstante lo expuesto, la Subsecretaría de Telecomunicaciones podrá establecer que, en consideración a circunstancias particulares de vulnerabilidad, determinados operadores relevantes deban adoptar los estándares que la autoridad le indique.
Comentarios Generales.	Creo que para ser una norma que apunte a la ciberseguridad, falta mucho trabajo para que pueda ser eficaz, y debe conversar con otras legislaciones de manera de tener un conjunto armonico y no se transforme en una camisa de fuerzas.