Michael Heavey 1 Samsing

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	La presente norma técnica tiene por objeto establecer un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben diseñarse, instalarse, operarse y protegerse las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones por parte de aquellos titulares de concesión o permiso que hayan sido declarados como operadores relevantes por esta Subsecretaría, (El criterio de declaración debe ampararse en alguna legislación, en especial la incidencia de las redes en la relación de los ciudadanos con el estado, y entre de las reparticiones de este dentro el proceso de transformación digital del estado) De igual manera, esta norma técnica busca regular el envío de información sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deban reportar a la Subsecretaría, (se debe especificar la resolución o decreto) con el objeto de coordinar las acciones orientadas a mitigar sus efectos y contribuir a una oportuna restitución de las redes, sistemas y los servicios afectados. Esta norma busca generar confianza en dichas redes, sistemas y servicios aumentando sus grados de ciberseguridad, en concordancia con la Política Nacional de

	Ciberseguridad vigente y las demás normas legales relacionadas. Las que se detallan a continuación:
Artículo 2.	a) Ciberespacio: es el ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones de todo tipo que se verifican en su interior. Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros. Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red. b) Ciberincidencia: es toda hecho acción, de cualquier naturaleza, que comprometa o amenace la disponibilidad, autenticidad, integridad, confidencialidad o seguridad en general de los datos almacenados, transmitidos o tratados,..... funcionamiento de estos. c) Ciberseguridad: conjunto de políticas, técnicas y prácticas destinadas a lograr..... d)...Computer Security Incident Response Team . En este caso particular debe especificarse la dependencia del CSIRT al que se hace referencia, está el CSIRT de gobierno pero empresas de servicios pueden tener los propios e) Gestión de incidentes: procedimientos y protocolos para la detección, análisis, manejo, contención, resolución y registro de una incidencia de ciberseguridad y

	responder ante ésta. g) Infraestructura crítica de telecomunicaciones: 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..... significativas en los sistemas de telecomunicaciones. Hay legislación atingente a la infraestructura crítica que debe ser referida, y debe considerar también las zonas insulares y regiones extremas como infraestructura crítica. h)....(establecidos, designados, reconocidos) como infraestructura crítica por resolución fundada de la Subsecretaría. (debe señalarse los criterios y proptocolos aplicables para esta decisión, pues puede importar condciones economicas no consideradas por el operador.... 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…)

	Sin perjuicio de lo anterior es necesario incluir mas definiciones con apego a los usos de la industria, tanto de las telecomunicaciones, ciberseguridad e informatica entre otras.
Artículo 3.	Las disposiciones contenidas en esta norma técnica solamente se aplican al diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones que .....
Artículo 4.	La declaración de un titular de servicios de telecomunicaciones como operador relevante se efectuará mediante resolución fundada de esta Subsecretaría, en la que se dejará constancia tanto de los criterios de relevancia tenidos en consideración como de la valoración que de ellos se hiciere. Nota: 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. A fin de determinar si un titular de servicio de telecomunicaciones debe ser declarado relevante para los fines de la presente norma técnica, la Subsecretaría tendrá en consideración, a lo menos, 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, y zonas extremas o territorios especiales en los que opere (debidamente priorizados según criterios establecidos) f) Participación de mercado; g) Daño a la imagen del proveedor
Artículo 5.	Los operadores relevantes de servicios de telecomunicaciones tendrán como obligación determinar y adoptar las medidas técnicas y de organización que permitan gestionar adecuadamente los riesgos de las redes y sistemas que utilizan para prestar servicios de telecomunicaciones a terceros en razón de

	sus títulos habilitantes, aún en caso de que tal gestión estuviere externalizada. Dichas medidas deberán garantizar un nivel adecuado de seguridad de las redes y sistemas, tomando en consideración la naturaleza y el contexto de los servicios prestados, los riesgos asociados y la tecnología disponible, así como tener en cuenta, a lo menos, los siguientes conceptos: a) seguridad física y ciberseguridad de los sistemas e instalaciones; b) costos de implementación; c) gestión del riesgo propio de la actividad; d) gestión de incidentes; e) gestión de la continuidad de los servicios; f) monitoreo permanente de los sistemas y patrullaje de instalaciones físicas atingentes g) actividades periódicas de supervisión, auditoría y prueba, incluidos simulacros de ciberincidentes. h) cumplimiento de buenas prácticas, normas y estándares internacionales; i) conocimiento y difusión interna de las alertas de ciberincidencias a nivel nacional e internacional;

	j) actualización constante de protocolos y sistemas de seguridad; k) determinaciones nacionales e internacionales en relación a los riesgos de seguridad asociados al uso de determinados equipos o proveedores; l) integridad de la cadena de suministros de equipos y software; m) disponibilidad de respaldos de equipos y sistemas críticos de rápido reemplazo De igual forma, los operadores relevantes deberán tomar las medidas adecuadas para prevenir y reducir al mínimo los efectos de las ciberincidencias que afecten la seguridad y resiliencia de las redes y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa. En todos los casos, se deberá diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes y sistemas en conformidad con estándares internacionales, independientes o nacionales, de amplia aplicación así como los mínimos que establezca esta Subsecretaria. (nota: Sería apropiado que la autoridad establezca o sugiera algunas referencias específicas, las que pueden ser variables en el tiempo…. Al dejar amplia aplicación deja una ventana para eventuales adopciones de subestándares en atención a los costos; así se asegura una estructura robusta)

	Nota : el uso del adjetivo relevante es innecesario 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 Esto incluye tanto la selección del fabricante o proveedor como la selección de los equipos y contratistas. con las apropiadas credenciales y certificaciones de competencias (nota: Facilita trazabilidad). Asimismo, d... su entrada en servicio , es decir con una trazabilidad robusta necesaria en un sistema de ciberseguridad. Mas en segunda entrega
Artículo 6.	Encargado de la ciberseguridad.....Esto cae en el ámbito de las definiciones y competencias que deben incluirse más arriba que se le va a exigir al operador, utilizando los términos usuales que se usan en la industria (P.EJ: CISO)

	Los operadores relevantes deberán informar al Responsable Subtel, en el plazo que se instruya, las identidades de sus encargados de ciberseguridad, la unidad a la que pertenecen y los medios de contacto pertinentes, informando oportunamente. (NOTA: este concepto, atendida la dinámica de ocurrencia de las ciberincidencias y sus efectos))en caso que exista alguna modificación al respecto. Para lo anterior, la autoridad dispondrá de un registro en línea en la cual conste y se actualice dicha información.
Artículo 7.	Los operadores a través de sus CISOs deberán reportar al Responsable Subtel. y al CSIRT del Ministerio del Interior y Seguridad Pública, directamente o a través del órgano que designe para dichos fines, acerca de todas las ciberincidencias que detecte en sus redes y sistemas y que alcance los umbrales de gravedad establecidos en las instrucciones y protocolos pertinentes emitidas ..... Los reportes deberán ser formulados por los CISO y enviados a través de los.... mecanismos, deben estar mas elaborados, pues da espacio a interpreatcion e improvisación.... informar con que proposito, que hace subtel con ello..... La obligación de reportar se entenderá formalmente cumplida solamente luego de que Subtel, directamente o través del órgano designado para dichos fines, haya acusado recibo a través de los mecanismos dispuestos para ello, excepto si éstos no se encontrasen disponibles; sin perjuicio de lo anterior, la Subtel dispondrá de un sistema telefónico y registro online que dejará registro automático de su recepción, con el

	fin de asegurar trazabilidad y accountability de los incidentes. Toda consulta formulada a un operador, sea directamente por Subtel a través del Responsable de Subtel por el órgano designado para dichos fines, generará para éste una nueva obligación de reportar, que deberá cumplir dentro del plazo señalado en el propio requerimiento. Subtel podrá delegar en otros órganos del estado el manejo de una ciberincidencia, lo que será informado oportunamente por el operador afectado, lo que será debidamente informado por el Responsable Subtel.
Artículo 8.	
Artículo 9.	deberán mantener, durante un plazo no inferior a tres años desde su ocurrencia, registros de ciberincidencias que den cuenta, a lo menos, de los siguientes datos: a. Titular de servicio de telecomunicaciones. b. Jefe de seguridad y encargado de seguridad en funciones. CISO c. Datos de contacto. d. Afectación actual y eventual de infraestructuras críticas.

	e. Hechos indiciarios o reveladores de la ciberincidencia. f. Momento estimado de inicio de los hechos y duración de la ciberincidencia. g. Redes y sistemas actual y eventualmente afectados. h. Estimación de la cantidad de usuarios y clientes actual y/o eventualmente afectados. i. Grado de afectación a usuarios y clientes. j. Alcance geográfico actual, densidad de servicios y eventual de la ciberincidencia. k. Origen posible de la ciberincidencia. l. Detalle de medidas de mitigación y restablecimiento. m. Tiempo estimado para la resolución definitiva de la ciberincidencia. n. Cualquier otra información que se considere relevante (síntomas, encriptación, malware, DDoS, ataque físico, etc) Deberá mantenerse registro de la evolución de la ciberincidencia conforme su desarrollo y, en caso de que puedan afectar o se afecten infraestructuras críticas, el registro debe extenderse hasta que se hubiere cerrado, es decir, su completa resolución.

	Los reportes deberán enviarse en forma oportuna conforme el desarrollo de la ciberincidencia, incorporando toda la información que sea pertinente y reportando cada cambio sustancial a medida que suceda. El encargado de ciberseguridad en funciones deberá reportar en la oportunidad que corresponda según la gravedad aparente de la ciberincidencia, aún en caso de que no cuente con todos los antecedentes necesarios -los que podrá completar en reportes posteriores-, a fin de coordinar las medidas de mitigación y presentar planes de acción, y actualizar aquellos de recuperación posterior al incidente. Adicionalmente, en el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas, el reporte deberá indicar los motivos por los que no contiene toda la información pertinente, la que deberá ser enviada tan pronto como sea obtenida. En caso de que el impedimento persista, se deberá continuar reportando a Subtel, sea directamente o a través del órgano designado para dicho efecto, los motivos del impedimento y las gestiones efectuadas para subsanarlos. Los operadores de infraestructura crítica que resulte afectada deberán informar inmediatamente de la situación a todos quienes puedan verse afectados por depender directamente de sus redes, sistemas o servicios, de acuerdo con los

	protocolos que deberán disponer para estas contingencias. Asimismo, el operador afectado deberá conservar por, a lo menos, doce meses (Nota: hay ciberataques que desde el instante cero toman su tiempo desde el acceso a la vulnerabilidad hasta la concretación de un ataque, por lo que se sugiere extender este plazo) desde el cierre de la ciberincidencia, todos los logs y registros que hubieren podido registrar efectos y actividades relacionadas con el posible ataque así como las medidas de gestión y resolución adoptadas.
Artículo 10.	El contenido de los reportes de ciberincidencias será tratado con especial reserva por los organismos del Estado que tomen conocimiento de éstos. En particular, se tendrá especial cuidado en revelar cualquier parte del reporte a partir del cual pudiera llegar a inferirse la identidad del operador relevante y de los encargados de ciberseguridad que participaron en su formulación., conforme a la legislación vigente
Artículo 11.	En caso de que sea necesario informar a terceros para prevenir, gestionar o resolver una ciberincidencia, el operador relevante podrá solicitar la asistencia del CSIRT (NOTA: debe especificar a cual CSIRT se refiere) de referencia o de Subtel. (Nota definir Quien o que departamento en SUBTEL) Por su parte, 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. “, para lo cual, en todo caso, deberá resguardar la información sensible o datos personales que pudieran estar relacionados al incidente y que no deban difundirse”. (NOTA: se debe tomar especial cuidado puesto que una información de cibervulnerabilidad hecha pública pudiera tener efectos económicos y comerciales severos, que produzcan más daños por imagen a la institución que el ciberevento en si). En caso de que esta Subsecretaría decida informar directamente al público o terceros, la publicación estará orientada a la entrega de información sobre las ciberincidencias, posibles causas, circunstancias, medidas de mitigación, recomendaciones de seguridad, alternativas de acciones a seguir, operadores relevantes, zonas geográficas o sistemas afectados y cualquier otra información de importancia para la correcta y oportuna información del público en general, sin que esto signifique afectaciones a la reputación del operador. Asimismo, conforme las atribuciones que conferidas por la legislación aplicable, Subtel, en conjunto con el CSIRT del Ministerio del Interior y cualquier otra entidad pública competente, adoptará medidas y efectuará gestiones orientadas a promover el intercambio de información entre actores públicos y privados en materias de seguridad física y de

	ciberseguridad de redes y sistemas de telecomunicaciones. (Nota: ¿Es Subtel la instancia de Gobierno para esto?,)
Artículo 12.	Superada una ciberincidencia, los operadores elaborarán un informe de evaluación (assesment) de la contingencia, con un resumen de los acontecimientos y principales medidas tomadas, y que servirá para mejorar sus procedimientos operativos y capacitaciones. . Dicho informe deberá ser remitido a Subtel, la cual guardará registro del mismo dando cuenta de su pertinencia o insuficiencia. En este último caso, ordenando corregir aquellas medidas consideradas insuficientes".
Artículo 13.	operador para que envíe a un tercero particular una copia del reporte, deberá eliminar todos los datos de carácter sensible que pudieran figurar en él, conforme a la legislación vigente en materia de protección de datos personales. En caso de que a partir del análisis de una ciberincidencia se advierta la ocurrencia de una posible vulneración de datos personales, Subtel o el órgano designado para dicho fin deberá remitir los informes pertinentes a la entidad a cargo de la protección de los datos personales competente. Junto con las secciones pertinentes de los reportes, se indicarán los motivos por los que pudo haber existido vulneración de datos personales conforme a la ley Nº 19.628.

Artículo 14.	enviar a Subtel, en forma directa o a través del órgano que esta designe para dicho fin, reportes periódicos trimestrales (Nota: la fijación taxativa obliga a los operadores a informar con una periodicidad establecida y no a una periodicidad relativa, la que deja espacios para incumplir con los necesarios procesos de actualización y difusión que demanda la dinámica de la ciberseguridad) que den cuenta de las modificaciones introducidas en sus redes y sistemas, sean en la capa de software o en elementos de hardware, para dar solución a las vulnerabilidades detectadas en el último período informado.
Artículo 16.	Los operadores relevantes deberán actualizar a lo menos cada 6 meses los planes de gestión de riesgos de las redes y s Asimismo, los operadores relevantes deberán someter al menos trimestralmente regularmente sus redes y sistemas de telecomunicaciones a pruebas de seguridad. ... Deberá dejarse constancia en el registro en línea que para estos efectos dispondrá Subtel de las pruebas efectuadas, los estándares aplicados, los resultados obtenidos y las medidas adoptadas en consecuencia.
Artículo 17.	in perjuicio de lo establecido en el artículo 15° de la presente norma técnica, la Subsecretaría o el CSIRT podrán fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta normativa.
Artículo 18.	infracciones a las disposiciones de la presente norma técnica serán sancionadas

	de acuerdo a lo dispuesto en el Título VII de la Ley. N° xxxx, titulo, y fecha.
Comentarios Generales.	Nota inicial: 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,. Cuando se establezcan comunicaciones, deberían especificarse las direcciones de acceso Web y de correo electrónico, como portales oficiales en virtud de la legislación de modernización del estado.. Se sugiere considerar otras normas internacionales, como por ser la española, francesa, estonia y otras, que permitirían darle robustez a la normativa en consulta. Se aprecia que los objetivos carecen de la profundidad suficiente para contar con un instrumento robusto. Debe partir por homologar terminología tanto nacional como internacional, de los diversos actores e intervinientes así como su ámbito de acción y extender la profundidad de las definiciones, e incluir otros términos más atingentes a los usos en ciberseguridad y en la industria, como los que aplican a los responsables de las redes y de la ciberseguridad, entre otros.