ISSA Chile

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 2.	Artículo 2°. Definiciones: Las definiciones entregadas en el documento emitido por la SUBTEL debieran ser revisadas en algunos aspectos que son de particular interés: a. ciberincidencia: Las normativas, frameworks y estándares internacionales hablan y se refieren a los incidentes cibernéticos solamente como "incidentes" es importante homologar las definiciones[5] para contextualizar un alcance más exacto respecto del espíritu de la norma propuesta. Debe señalar además que una incidencia "Es toda acción que comprometa o pueda comprometer la disponibilidad..." de tal manera que, si se detectan amenazas que son de real importancia y aún no han materializado su impacto real sean tratadas con la celeridad e importancia adecuada. b. Ciberseguridad: Tal definición debe estar alineada con la definición de ciberseguridad indicada en la política nacional de ciberseguridad pagina 16, punto 6. c. Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante "CSIRT": Debe estar alineada con la Política Nacional de Ciberseguridad y no debe restringir las atribuciones dadas en ella. Punto 4 página 17. Respecto de las atribuciones que tendrá el CSIRT se debe señalar que "es el órgano encargado de recibir y analizar reportes de ciberincidencias, con el fin de analizarlos, monitorear el desarrollo de éstas, emitir alertas y proponer medidas tanto de mitigación como de prevención, y tendrá la autoridad necesaria para coordinar la respuesta técnica frente a incidentes que comprometan la seguridad del país" d. Gestión de incidentes: Además de señalar que son los procedimientos para la detección, análisis, contención, erradicación y recuperación de una incidencia de ciberseguridad, debe considerar la preparación toda vez

	que el proceso debe entenderse como una acción planificada y proactiva y no puramente reactiva, considerando además las lecciones aprendidas (pos incidente) para la mejora continua. e. Incidente: el alcance debe ser establecido en "seguridad de las redes y sistemas de información" sin agregar el término "de telecomunicaciones" debido a que pueden existir incidentes que no están relacionados con los sistemas de información de telecomunicaciones pero que igualmente pueden afectar gravemente la infraestructura crítica. f. Infraestructura crítica de telecomunicaciones: Tal definición debe considerar la integridad como un elemento de interés para la normativa: "…generaría un serio impacto en la seguridad, privacidad, integridad o disponibilidad de servicio de la población afectada". g. Riesgo: No es necesario describir ejemplos en el párrafo de definiciones, de lo contrario se debe ejemplificar en todas las definiciones dadas en el documento. Por otra parte, la matriz riesgo x impacto no es la única manera de medir el riesgo existiendo otras metodologías que podrían quedar inmediatamente descartadas si es que se ejemplifica en la norma técnica. Adicionalmente, Se debe definir "impacto en la ciberseguridad" para ser consistentes con el contenido de la norma en general.
Artículo 3.	2. Artículo 3°. Ámbito de aplicación: Se debe considerar los equipos adyacentes a los activos de información del alcance pues, en un ataque cibernético existe la posibilidad de realizar movimientos laterales que podrían afectar las redes y sistemas críticos para la compañía. Por lo tanto, proponemos: "…y todos los activos de información que pudieran afectar a la seguridad de las redes y sistemas del alcance de esta normativa."
Artículo 4.	3. Artículo 4°. Criterios de relevancia: SUBTEL debe definir una periodicidad de revisión de los actores

	relevantes para mantener la idoneidad de tal categoría asignada a cada empresa.
Artículo 5.	4. Artículo 5°. Obligaciones generales de seguridad: La lista propuesta no considera otros aspectos importantes de la ciberseguridad tales como: Gobierno de seguridad, seguridad operaciones, administración de seguridad, seguridad de personal y entrenamiento, ciberinteligencia, gestión de inteligencia de amenazas, gestión de identidades y acceso, gestión de configuraciones de seguridad, aspectos de desarrollo seguro etc. Además, la norma habla de "de las redes, sistemas e instalaciones" términos que no fueron definidos en el alcance, el documento debe ser consistente con el alcance determinado. Por otra parte, en el mismo artículo se establece 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" sin embargo, continua indicando que "en todos los casos, deberá tener en consideración, a lo menos, las recomendaciones de esta Subsecretaría", a tal afirmación se hace necesario señalar que deben considerar las recomendaciones y "mandatos" de esta manera la labor de la SUBTEL no termina solo en las recomendaciones sino que ejerce disposiciones que deben cumplirse. Debe agregar además que "La documentación y demás antecedentes que den cuenta del detalle de los planes de gestión de riesgo, gestión de seguridad y repuesta a incidentes deberá estar permanentemente disponible en caso de inspecciones a realizar por Subtel" y que "los operadores relevantes deberán considerar en sus planes el estado de la técnica, tácticas y procedimientos y la tecnología disponible en los ámbitos de seguridad de sistemas" para finalizar con que "determinados operadores relevantes deban adoptar los estándares y acciones que la autoridad le indique"
Artículo 6.	5. Artículo 6°. Encargados de ciberseguridad: Debe señalar 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, habilidades, conocimiento y experiencia suficientes para identificar los riesgos de afectación de los servicios de telecomunicaciones por causa de ciberincidencias".
Artículo 7.	6. Artículo 7°. Obligación de reportar ciberincidencias: Si se establece claramente lo señalado en el Punto 4. Artículo 5 se debe indicar que los operadores relevantes deberán reportar "las ciberincidencias que detecte en sus redes, sistemas e instalaciones y que alcance los umbrales de gravedad establecidos en las instrucciones pertinentes emitidas por Subtel". Por otra parte, La matriz de Acuerdo de Niveles de Servicio (SLA) debe preferentemente utilizar la misma tabla de impacto de incidentes que utilice el CSIRT Chile dependiente del ministerio del interior de esta manera homologar la respuesta entre los distintos actores; donde dice "Alcance ciberincidencia" debe decir "impacto" y se propone que los SLA impacto Alto: 15 minutos, Media: 24 horas, baja: 5 días. Además, el plazo de reportar una incidencia no puede depender de un acuse de recibo de la SUBTEL, por lo tanto, se debiera mejorar la redacción del párrafo en cuestión para reflejar el correcto espíritu de la letra.
Artículo 8.	7. Artículo 8°. Desarrollo de los reportes: De acuerdo a la definición de ciberincidencia indicada en esta propuesta este artículo debe comenzar con: "En caso de ciberincidencias con un inminente impacto alto, o bien, ciberincidentes ya materializados de alto impacto que se extiendan por un período de tiempo que exceda de treinta minutos,…".
Artículo 9.	8. Artículo 9°. Contenido de los reportes: Respecto de lo dispuesto en el Punto d), se debe avanzar en proporcionar información de infraestructura crítica potencialmente impactada más allá de la infraestructura crítica de la compañía de telecomunicaciones afectada. Principalmente porque muchas otras infraestructuras críticas dependen de Internet y los servicios de telecomunicaciones. Es importante además agregar puntos como Responsable

	del sistema y Persona que detectó el incidente de esta manera se agilizan los procesos de comunicación y se registra la responsabilidad al momento de resguardar información que no debe ser divulgada. Respecto del registro de la evolución de la incidencia, el registro debe extenderse hasta la completa resolución de la causa raíz del incidente. En el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas el operador afectado deberá conservar por, a lo menos, Un año desde el cierre de la ciberincidencia.
Artículo 10.	9. Artículo 10°. Tratamiento de los reportes: Es importante mantener un registro de los informantes y receptores de la información de tal modo que, si hay información o incidentes que deban mantenerse de forma confidencial, tal registro actúe de forma disuasiva en la revelación de información, se debe considerar además la obligatoriedad de comunicación de información por canales seguros o con sistemas de cifrado de extremo a extremo para mantener la confidencialidad de los datos considerando para esto los planes de instrucción adecuados.
Artículo 11.	10. Artículo 11. Información a terceros e intercambio de información: Se debe mantener concordancia en la norma técnica, ajustando la narrativa a seguridad física o seguridad de instalaciones según corresponda.
Artículo 12.	11. Artículo 12. Obligación de resolución de ciberincidencias: La última disposición del artículo doce debe especificar la resolución de vulnerabilidades y fallos, debido a que podrían existir amenazas de ciberseguridad que deriven de fallos operación, diseño o arquitecturas y no sean una vulnerabilidad propiamente tal.
Artículo 13.	12. Artículo 13. Tratamiento de datos personales: Para el tratamiento de información de carácter personal, se propone que la norma técnica indique que: “En caso de que se deban incorporar datos personales de carácter sensible en un informe de ciberincidencia en razón de ser indispensables para la adecuada comprensión del mismo, se debe privilegiar el uso de enmascaramiento

	de datos en la entrega de estos informes,…”
Artículo 14.	13. Artículo 14. Reportes trimestrales: Tal disposición finaliza indicando que “El período de los reportes será aquel que Subtel indique en las instrucciones pertinentes”, sin embargo, en el título del Artículo ya se señala que los reportes son trimestrales.
Artículo 16.	14. Artículo 16. Supervisión de seguridad: Esta norma técnica de tener a fortalecer en el mayor grado posible la ciberseguridad de las empresas reguladas, por tal motivo, en el según párrafo del artículo debe indicar que “los operadores relevantes deberán someter a pruebas de seguridad a lo menos semestralmente sus redes y sistemas de telecomunicaciones identificados como críticas en el análisis de riesgos”. Asimismo, al finalizar el artículo se señala que SUBTEL podría requerir “los resultados de las pruebas de seguridad y, en general, todo otro tipo de antecedentes relacionados con políticas de seguridad de sus redes y sistemas”, creemos importante retirar la referencia a las políticas e indicar que se podría requerir “los resultados de las pruebas de seguridad y, en general, todo otro tipo de antecedentes relacionados con la seguridad de sus redes y sistemas”.
Artículo 17.	15. Artículo 17. Fiscalización: Esta normativa señala que la “Subsecretaría podrá fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta normativa”, sin embargo, la normativa debiera establecer que la Subsecretaría “Deberá” fiscalizar a lo menos anualmente y en cualquier momento el cumplimiento de esta normativa.
Comentarios Generales.	16. Artículo 19: Es importante considerar un artículo extra en la presente normativa en el que se señale que esta norma técnica deberá ser revisada a lo menos anualmente por SUBTEL, en forma directa o a través del órgano que ésta designe para dicho fin. El objetivo de esta cláusula es asegurar la actualización permanente de la normativa y sus particularidades.

	Articulo completo: ISSA CHILE WORKING PAPER 1 Una Contribución de ISSA Chile a la Nueva Normativa de Ciberseguridad de la Subsecretaría de Telecomunicaciones https://www.researchgate.net/publication/342159180_ISSA_CHILE_WORKING_PAPER_1_Una_Contribucion_de_ISSA_Chile_a_la_Nueva_Normativa_de_Ciberseguridad_de_la_Subsecretaria_de_Telecomunicaciones?channel=doi&linkId=5ee5ca73299bf1faac55bae7&showFulltext=true