WOM S.A.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Respecto del diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, debe precisarse que el marco regulatorio objeto de esta norma técnica aplica para el futuro despliegue y actualización de las redes y sistemas; y por lo tanto, no tiene necesariamente un carácter retroactivo mientras el proveedor de servicios o titular de concesión dé cumplimiento a las medidas de protección en materia de ciberseguridad.
Artículo 2.	letra b). Para la definición de ciberincidencia, se recomienda referirse a aquellas ya definidas en la UIT. Además, dentro del concepto de ciberincidencia debe también precisarse qué se entenderá por "normal funcionamiento de los mismos" cuando se refiere a los sistemas de telecomunicaciones, toda vez que una acción que comprometa la disponibilidad de los servicios de telecomunicaciones no necesariamente es una ciberincidencia. Tampoco se identifica claramente los métodos de medición exigibles para poder categorizar un hecho aislado como ciberincidencia.
Artículo 3.	Sin comentarios
Artículo 4.	Respecto de los criterios que menciona que la Subsecretaría tendrá en consideración para declarar si un titular es o no relevante, se debe precisar qué se entenderá por "atención a sectores estratégicos"
Artículo 5.	letra a) Respecto de los sistemas e instalaciones a que se refiere en el literal a), debe precisarse que éstos son aquellos involucrados en la prestación de los servicios objeto de esta normativa. letra f) No queda clarificado a qué sistemas se refiere cuando menciona "monitoreo permanente de los sistemas". ¿A qué tipo de monitoreo se refiere,

	ejemplifique, de disponibilidad, de seguridad, de desempeño? letra g) Sobre las actividades de supervisión, auditoría y prueba. ¿Qué se entiende por actividades de supervisión? Es necesario que se detalle el entendimiento y obligaciones a objeto de diseñar y dimensionar estas actividades. letra h) También es relevante que se haga una presentación de cuáles cuáles normas y estándares internacionales se refiere, por ejemplo de qué organismo, de qué año en adelante, o cuál enfoque de estándar y/o norma. ¿En qué plazo deben cumplirse dichos estándares?, ¿Qué nivel de cumplimiento espera en el plazo señalado?, ¿La autoridad supone la certificación de las normas sugeridas? letra k) Si el operador relevante cumple con estándares internacionales, esta determinación de los equipos o proveedores se entiende incluida; por lo que este numeral es redundante y debiera suprimirse al estar incluido en la letra h). letra j) Respecto de la actualización constante de protocolos y sistemas de seguridad, se debe precisar ¿qué tipo de protocolos, técnicos, procesos refiere este literal?, por favor ejemplificar a qué sistemas de seguridad se refiere deban ser actualizados. ¿A qué tipo de actualización refiere en el caso de sistemas de seguridad, del hardware, de las versiones de software?, ¿Cuáles serán los criterios para considerar un sistema actualizado?.

	Respecto de la frase "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.", Cuando se menciona "en todos los casos" no queda claro a qué casos se refiere, ¿se refiere a los casos de diseño de red?. Tampoco queda del todo claro, nuevamente, a qué estándares internacionales, independientes o nacionales se refiere. Esto último puede dar espacio a una discrecionalidad de la administración y modificar la referencia de un estándar a otro obligando a los proveedores relevantes a adecuarse desde un estándar a otro. Además, cuando se refiere a estándares independientes es demasiado ambiguo e inconsistente con la adopción de un determinado estándar normado por una institución internacional. ¿Será el operador relevante quien elige libremente cuál estándar seguir o éste será dado por la Subsecretaría?. En cuarto inciso, la frase "Esto incluye tanto la selección del fabricante o proveedor como la selección de los equipos y contratistas" está redundante. Por favor referirse al comentario realizado en la letra k) anterior. En el quinto inciso, ¿qué es el Sistema Nacional de Ciberseguridad?, ¿quién lo compone?, ¿de quién depende?, ¿qué rol y atribuciones tiene? Inciso final: Para evitar arbitrariedades, se debe definir claramente qué condiciones se considerarán circunstancias particulares de vulnerabilidad, y además qué estándares podrán ser establecidos por la

	autoridad, a objeto que los operadores relevantes puedan optar por implementar estos estándares al inicio de la vigencia de la normativa.
Artículo 6.	¿Cómo se determina que las competencias del encargado titular sean "suficientes"? Se debe aclarar si este requerimiento se refiere a un símil de la posición conocida como “Oficial de Seguridad” o ciberseguridad o si se trata de una posición diferente.
Artículo 7.	Aclarar si acaso habrán incidencias que se deberán reportar dos veces: ¿Aquellas ciberincidencias también se deberán reportar como Falla Significativa de acuerdo al decreto 60 (25)? Respecto de la publicidad de las ciberincidencias, es importante que Subtel o la autoridad respectiva, se abstengan de publicitar la situación de ciberincidencia para no incitar mayores ataques ni exponer vulnerabilidades de los sistemas a la luz pública. Además, los plazos para reportar la ciberincidencia no se condicen con la obligación de detectar y atender la ciberincidencia. Se debe priorizar comprender el alcance y en controlar la ciberincidencia para que luego se deba reportar. Respecto del inciso cuarto: El operador relevante no tiene control de los canales de recepción de Subtel o el órgano designado para dichos fines. Por lo que la obligación de reportar se entenderá formalmente cumplida luego del envío.

	Inciso final: las consultas formuladas al operador por Subtel deben ser realizada a través de los canales y mecanismos dispuestos para ello. Además, y respecto de la columna "Descripción", la frase "las redes os sistemas están fuera de operación": (i) se debe objetivar la declaración, por ejemplo: las redes o sistema están fuera de operación cuando un porcentaje mayor a 10% de los clientes no tiene servicio; (ii) Describir los criterios con que se aplicará la definición de "Las redes o sistemas están fuera de operación. ¿Es exclusivamente cuando los clientes están sin servicio? Detalle otros criterios si los hubiere. (iv) ¿Estas precisiones objetivas necesarias serán estándar de la industria o serán especificadas para cada compañía por separado de acuerdo a la realidad de sus sistemas?.
Artículo 8.	Respecto de la obligación de envío de "tantos reportes como sean necesarios", en ningún caso la obligación de envío de estos reportes deberá obstaculizar el proceso de resolución de la ciberincidencia, definiendo como obligación prioritaria la resolución de la ciberincidencia por sobre aquella de informar. Lo anterior sin perjuicio del mayor esfuerzo que los operadores relevantes deberán hacer para mantener informada a la autoridad.
Artículo 9.	Ocurrida una ciberincidencia, la prioridad está en superar dicha situación; luego evaluar la situación, impacto y alcances. En paralelo, se está solicitando el envío períodico de información lo cual no debe entorpecer las labores de resolución de la ciberincidencia. En este contexto, parece excesivamente detallada la información a remitir en el contexto de una resolución de ciberincidencia. Esto porque no queda claro el inciso primero que indica que el contenido de las letras a) hasta la m) es el contenido del registro de la ciberincidencia que debe llevarse y almacenarse durante 1 año, y el texto del inciso 3 que indica "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". Por esto, se debe aclarar que las letras a) a m) corresponde al registro y no al reporte del artículo 8. El contenido del reporte del artículo 8 debe ser acorde a los tiempos en los que se está solicitando.
Artículo 10.	Además, debe incluirse la obligación de no divulgar por redes sociales ni ningún medio público cualquier ciberincidencia reportada por un operador relevante.
Artículo 11.	"Respecto de lo descrito en el inciso segundo, la Subsecretaría podrá divulgar la información previa coordinación con el operador o proveedor afectado, para no divulgar información sensible ni estratégica que pueda revelar puntos futuros de ataques o debilidades de los sistemas. Inciso tres: La información es altamente sensible y debe abstenerse de hacerse pública. En caso contrario, deberá realizarse de manera agregada y sin identificar operadores ni sistemas pues es podría incitar a dirigir futuros ataques. "
Artículo 12.	Sin comentarios
Artículo 13.	El tratamiento de datos personales debe realizarse de conformidad a la legislación vigente y de acuerdo a las autorizaciones necesarias y requeridas por el propietario de dichos datos. Sin perjuicio de esto, se debe precisar si por “datos personales” se entienden los datos de clientes, clientes y empleados u otro conjunto o subconjunto.
Artículo 14.	"El título del artículo habla de reportes trimestrales mientras que el contenido del mismo dice que ""el periodo de los reportes será aquel que Subtel indique"". Por favor clarificar.

	Además y considerando el contenidos sensible de dichos reportes, ¿cuáles serán las garantías tecnológicas que aseguren que dichos informes serán de uso exclusivo de los órganos competentes?"
Artículo 15.	Sin comentarios
Artículo 16.	"La información requerida en el párrafo final es altamente sensible, por lo que deberá ser tratada con la más estricta confidencialidad. Además, respecto de la obligación de mantener actualizados los planes de gestión, ¿cómo se controlará que los operadores efectivamente estarán actualizando sus respectivos planes de gestión de riesgos?, ¿se definirán formatos tipo para poder entregar los resultados solicitados por el organismo?"
Artículo 17.	Sin comentarios
Artículo 18.	Comentario general: ¿Hasta qué punto recae la responsabilidad del operador cuando se ha externalizado un servicio que fue objeto de una ciberincidencia?