Telefónica Móviles Chile S.A.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Sin perjuicio de los comentarios de detalle que, con el ánimo colaborativo que caracteriza a Telefonica Chile, se harán a la propuesta normativa en consulta pública, es fundamental señalar que ningún precepto legal le otorga a Subtel competencia en materia de ciberseguridad. En consecuencia, carece de atribuciones para dictar una Norma Técnica o Reglamento de esta naturaleza. Asimismo, la materia que regula la Norma Técnica ("fundamentos generales de ciberseguridad y envío de información sobre ciberincidencias") corresponde que sea tratada en una norma de jerarquía legal, conforme a lo dispuesto en art. 63 N° 20 de la Constitución Política del Estado (CPE). A mayor abundamiento, la Norma Técnica establece una serie de obligaciones que regulan y restringen la garantía constitucional de desarrollar la actividad económica y el derecho de propiedad, materias que, de conformidad con la CPE, sólo pueden ser reguladas por ley. En este sentido, el Tribunal Constitucional ha sostenido lo siguiente: "Que, si bien es efectivo que el legislador haciendo uso de su facultad de "regular" puede establecer limitaciones y restricciones al derecho a desarrollar cualquier actividad económica, esta facultad no le corresponde al administrador, pues de acuerdo al texto constitucional, por el artículo 60, N° 2°, que establece 'Sólo son materias de ley: las que la Constitución exija que sean reguladas por una ley', estas atribuciones

	están entregadas expresamente al legislador, al disponer el constituyente que el derecho a desarrollar una actividad económica se asegura 'respetando las normas legales que la regulen'. En otras palabras, el constituyente entrega al legislador y no al administrador la facultad de disponer como deben realizarse las actividades económicas y a qué reglas deben someterse." (Sentencia Rol N°167/2003). En particular, se debe precisar que el alcance de la frase que define el objeto de la normativa "…las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones" se refiere exclusivamente a los sistemas utilizados para la operación de las redes necesarias para la prestación del servicio (los llamadas sistemas de O&M) y no incluyen los sistemas destinados a la parte administrativa de la empresa (como sería el sistema SAP por ejemplo) ya que no son utilizados para la prestación del servicio de telecomunicaciones.
Artículo 2.	Una normativa técnica que se dicte sobre la materia debe establecer, dentro de sus definiciones, que se considerará como "Reporte de Ciberincidencia" un correo o una alerta que contiene al menos los siguientes campos de información: • Breve Descripción del evento • Fecha de ocurrencia • Tipo de incidencia • Origen • Evidencias • Plan de acción/Recomendaciones a ejecutar

	Consideramos, además que cualquier definición sobre la materia debe quedar contenida en la normativa técnica que se dicte y no puede quedar referenciada, en forma genérica, a otra normativa sectorial, existente o futura, que deja un espacio de incertidumbre y de arbitrariedad a la hora de su aplicación. Respecto a la definición de la letra b), se debe precisar que para efectos de esta normativa sólo incluyen las acciones que comprometan las infraestructuras tecnológicas definidas en la letra a), y de ninguna manera abarcan los sistemas administrativos, como el SAP o sistemas de soporte a la operación, utilizados por las empresas. Por lo mismo, la definición de la letra f) y letra i) se debe precisar que abarca solo las infraestructuras tecnológicas definidas en la letra a)
Artículo 3.	Sin perjuicio de nuestro comentario de fondo, consideramos que cualquier normativa técnica que se dicte sobre la materia debe considerar, dentro de su ámbito de aplicación, a todos los proveedores de servicios digitales, incluyendo a los operadores Over The Top (OTT) que ofrecen sus servicios a través de las redes de los operadores tradicionales de telecomunicaciones. Asimismo, la normativa debe precisar que los operadores de telecomunicaciones son sólo responsables en relación con sus propios servicios y no a servicios que ofrecen terceros operadores que, por el hecho de no poseer red propia, como los operadores móviles virtuales o los OTT, por ejemplo, deben hacerse cargo directamente de las obligaciones que surjan de una normativa de esta naturaleza. Para este efecto, se propone agregar en la tercera línea, después de la frase “utilizados para la prestación de servicios de

	telecomunicaciones", "del propio operador". Por último, debe precisarse que las disposiciones contenidas en una norma técnica de este tipo solamente se aplican sólo sobre las infraestructuras tecnológicas definidas en la letra a) del Art.1, y no debe considerar sistemas administrativos de apoyo o secundarios, tales como SAP, "asistencia de empleados" "Ticketing" "Correo electrónico" y otros que son apoyo para la gestión, pero no para la operación de redes de comunicaciones.
Artículo 4.	Se propone agregar como criterio adicional, el siguiente: f) Cantidad de usuarios atendidos
Artículo 5.	Para la letra a) del presente artículo, se solicita precisar su alcance en los siguientes términos: a) seguridad física y ciberseguridad de los sistemas e instalaciones "utilizados para prestar servicios de telecomunicaciones directos a público y no sistemas de apoyo a la gestión o secundarios" Para la letra h) del presente artículo, debido a la existencia de múltiples estándares internacionales se solicita precisar cuáles serían aquellas normativas o estándares internacionales a los que adherirá el estado de Chile y que los operadores nacionales estarían obligados a cumplir. No puede quedar en la indefinición y sujeto a cambios discrecionales de la autoridad de turno. La misma precisión anterior se debe realizar en el inciso

	tercero de este artículo. El Estado chileno ha adherido a la UIT (Unión Internacional de Telecomunicaciones), organismo dependiente de la ONU como el organismo normativo internacional y no corresponde que se pretenda adherir a otros estándares internacionales indefinidos. En la misma línea anterior, se solicita que se aclare y especifique qué recomendaciones de ciberseguridad en materia de diseño de redes y sistemas son las que la normativa obligaría a cumplir, según lo indica el inciso sexto de este artículo. En relación a la letra l) se debe precisar que entenderá la regulación por "Integridad de la cadena de suministro" y por "verificar el cumplimiento eficaz de dichos criterios", establecido en el inciso cuarto, por cuanto es inviable e impracticable que operadores de un país tomador de tecnología como es Chile, impongan a proveedores mundiales estándares de ciberseguridad locales, so pena de quedar marginados de optar a dichos proveedores y tecnologías, encareciendo el despliegue de tecnologías de punta. Consideramos que no es racional que se impongan estándares locales a empresas que ya aplican normas de seguridad acorde a estándares internacionales, más aún si existen proveedores que por Normas Corporativas Vinculantes se han adaptado a niveles de exigencia de ciberseguridad acordes a la normativa y regulación específica de la Unión Europea. Adicionalmente, es imposible que un proveedor pueda garantizar al 100% "la integridad de la cadena de suministro", debido a que siempre existirán situaciones de fuerza mayor, tal como ha sido demostrado por el COVID y las catástrofes naturales. Los operadores

	debemos estar preparados para reaccionar con prontitud (“resiliencia”) ante problemas de un proveedor, pero la exigencia mencionada es de carácter imposible y excede el ámbito de una normativa sobre ciberseguridad. Finalmente, se solicita eliminar el inciso final del presente artículo por cuanto, a través de actuaciones arbitrarias y discriminatorias, dirigido sólo a una o algunas empresas, de la autoridad de turno, se puede llegar a imponer exigencias u obligaciones de alcance y de impactos en costos desconocidos y, por ende, de factibilidad incierta de cumplimiento por parte de los afectados. Adicionalmente, el entregar facultades discrecionales a la Subsecretaría en esta materia, ámbito que no es propio de su competencia de conformidad a la ley orgánica que la regula, implica un menoscabo a la garantía constitucional del art. 19 N°21 de la CPE, ya que nuestra representada tiene el derecho, y por sobre todo la libertad de desarrollar cualquier actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que la regulen.
Artículo 6.	
Artículo 7.	Una normativa de este tipo debiera contener algunos lineamientos estratégicos generales como los establecidos en Directivas Europeas (Directiva UE 2016/1148) sobre la materia en las cuales se señala que los proveedores de servicios digitales deberán notificar, sin retrasos indebidos, aquellas incidencias que tengan “impacto significativo” en la prestación de sus servicios y que dicha obligación de notificación únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente, en función de los parámetros que se definan para ello. Al acoger principios de esta naturaleza se entregarían las señales correctas para que una normativa de este tipo asegure, como primera

	prioridad, que los esfuerzos se dediquen a minimizar y resolver los impactos de una ciberincidencia y no distraer recursos críticos, en una primera instancia, en tareas administrativas de información y reportería a organismos reguladores. No estamos de acuerdo en que se establezca una obligación de reportar "todas" las ciberincidencias independiente de la evaluación de su relevancia o impacto. Se solicita excluir de esta obligación a las ciberincidencias calificadas como de Alcance BAJA y MEDIA, que importan fallas de impacto parcial, reducido o limitado. La obligación de reportar debe recaer en incidencias de impacto masivo, para lo cual se debiera fijar un estándar único que fije el umbral para el cual regirá dicha obligación. Para focalizar los esfuerzos y recursos en minimizar impactos de una ciberincidencia, se propone definir el "Reporte de Ciberincidencia" con un formato y un procedimiento de notificación simple y ejecutivo como el que ya se planteó en el Artículo 2 de la presente normativa. En todo caso, se propone también contar con canales alternativos de notificación, para el caso que el canal definido como "principal" no se encuentre disponible. Asimismo, el tiempo que se asigne para cumplir con la obligación de reportería debe estar en consonancia con el principio general de la Directiva Europea, antes explicitado, en cuanto a que la obligación de notificación del "Reporte de Ciberincidencia" se aplicará únicamente desde que el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente. Previo a contar con toda la información, se puede definir una "Pre – Alerta"

	de evento de alto riesgo en curso, el que puede ser notificado previamente al Reporte de Ciberincidencia, y eventualmente cancelarse la pre-alerta si era una falsa alarma. Se considera razonable que esta Pre-Alerta informativa deba ser evacuada dentro de las primeras 24 horas, a contar desde la hora en que se detecte el ciber incidente, por parte del Operador. En cuanto al Reporte de Ciberincidencia, se propone que este sea evacuado por el Operador una vez superado el ciber incidente. Por último, en cuanto al asunto de que 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, Telefónica discrepa de este criterio por cuanto deja al completo arbitrio de la capacidad técnica y humana de dicha Subsecretaría la certificación del acto de notificación, independiente de que el proveedor de servicios digitales haya ejecutado en forma oportuna y eficiente esa tarea
Artículo 8.	Esta obligación de reportería sucesiva y en plazos indefinidos en la norma atenta gravemente al esfuerzo de los equipos técnicos especializados que estarán dedicados a solucionar el problema y no debieran ser distraídos en elaborar reportes administrativos recurrentemente. Por eso, la norma debe definir claramente la periodicidad de esta recurrencia, la que debiera ser cada vez mayor a medida que pasan las horas o días desde la ocurrencia. Por ejemplo, en las primeras24 horas de ocurrencia, reportes cada 8 horas; hasta las48 horas, cada 12 horas; después de las 48 horas, una vez al día

Artículo 9.	Se solicita complementar si el "dato de contacto" que señala el literal c) del presente artículo, se refiere a la información del Responsable de Ciberseguridad, del autor del reporte, o del oficial de protección de datos de la compañía (DPO). Adicionalmente, en el párrafo final del Artículo 9° se alude a que el operador deberá conservar todos los "logs y registros" de información. Consideramos que, por razones de claridad y certeza, es necesario incluir dentro de las definiciones contenidas en el artículo 2° el concepto de "log" que se ha de utilizar para efectos de esta normativa, de manera de dejar en claro que no se refiere a los logs de navegación de los usuarios, que son data personal extremadamente sensible, y que estando protegidas por la garantía constitucional de la inviolabilidad de las comunicaciones que consagra el Artículo 19 numeral 5 de la CPE, cualquier entrega de tal información a la autoridad debe ser previamente autorizada y ordenada por tribunal competente
Artículo 10.	Atendido que la información que pueden contener los reportes de incidencia puede incluir datos personales de usuarios, así como información de carácter estratégico sobre él o los negocios del proveedor de servicios digitales que reporta, se debe tener absoluta claridad respecto de las medidas y resguardos que adoptará la autoridad para con dicha información. En específico, qué medidas se adoptarán para resguardar dicha información, cómo se hará su tratamiento, qué plataformas se utilizarán, sólo se utilizará correo electrónico para notificación, entre otros aspectos relevantes
Artículo 11.	Sin perjuicio de nuestro comentario de fondo expuesto en el Artículo N° 1 de esta propuesta normativa, debemos señalar que Telefónica en calidad de responsable del tratamiento de los datos personales de los usuarios de sus servicios de telecomunicaciones, no se encuentra autorizada para entregar los datos de

	contacto de nuestros clientes. De conformidad a la legislación de datos personales, estos solo pueden ser tratados con las finalidades previamente autorizados, por ley o por el titular de los datos personales (los usuarios). La Subsecretaría de Telecomunicaciones no se encuentra autorizada por la ley para hacer tratamiento de los datos personales de los usuarios con las finalidades que señala el Artículo 11. Cualquier otra acción de de Subtel para difundir ciberincidencias debe ser previo conocimiento y acuerdo de la operadora involucrada, por constituir información estratégica para la seguridad y la operación de las redes de telecomunicaciones del país. Por ello, en el tercer párrafo de este artículo, Telefónica solicita hacer la siguiente adecuación de texto marcada en negrilla y cursiva: "En caso de que esta Subsecretaría decida informar, previo acuerdo con la operadora, directamente al público o terceros…" Respecto del párrafo final de este artículo, la legislación vigente no entrega atribuciones a Subtel en esta materia
Artículo 12.	Respecto a la obligación de subsanar establecida en el inciso final, se debe especificar que se debe subsanar "en la medida que sea técnicamente factible", ya que puede haber situaciones de infactibilidad dada las redes o sistemas específicos con que opere la empresa
Artículo 13.	Telefónica en calidad de responsable del tratamiento de los datos personales de los usuarios de sus servicios de telecomunicaciones, no se encuentra autorizada para

	entregar los datos personales de nuestros clientes; salvo en lo que diga relación con el ejercicio de las facultades de fiscalización que detenta la Subsecretaría en el ámbito de sus competencias legales, lo que no es el caso actual. De conformidad a la legislación de datos personales, estos solo pueden ser tratados con las finalidades previamente autorizados, por ley o por el titular de los datos personales (los usuarios). Más aún, si los datos personales revisten el carácter de sensibles, implicaría un tremendo riesgo por la responsabilidad legal que le empece a Telefónica en calidad de responsable de tratamiento, lo que nos sujetaría eventualmente a resarcir e indemnizar los perjuicios que se generen a los usuarios por tratamiento no autorizado de datos y desviación de la finalidad para el cual se nos autorizó a tratar dichos datos. En relación con el párrafo final del Artículo 13, Telefónica al ser una persona jurídica de derecho privado, solo se sujeta a la autoridad al control de los tribunales ordinarios de justicia ante la eventual infracción de las disposiciones vigentes de la Ley 19.628
Artículo 16.	Se debe precisar cuáles son las pruebas de seguridad a que se refiere en el inciso 2 de este artículo, así como precisar también con qué periodicidad se busca obligar a la realización de dichas pruebas. Además, tal como ya se planteó en nuestros comentarios al artículo 9°, se solicita incluir dentro de las definiciones del artículo 2°, el concepto de "log"
Artículo 17.	Ningún precepto legal le otorga a Subtel competencia en materia de ciberseguridad. De este modo, mientras no se dicte la Ley Marco de Ciberseguridad contemplada en la Política Nacional de Ciberseguridad, carece de atribuciones para fiscalizar cualquier asunto relacionado a dicha materia
Artículo 17.	Ningún precepto legal le otorga a Subtel competencia en materia de ciberseguridad. De este modo, mientras

	no se dicte la Ley Marco de Ciberseguridad contemplada en la Política Nacional de Ciberseguridad, carece de atribuciones para fiscalizar cualquier asunto relacionado a dicha materia
Artículo 18.	Mientras no se dicte la Ley Marco de Ciberseguridad contemplada en la Política Nacional de Ciberseguridad, ni se establezcan expresas atribuciones a Subtel en esta materia, será inaplicable el título VII de la Ley General de Telecomunicaciones
Comentarios Generales.	Dentro de las justificaciones para dictar esta Norma Técnica se alude a la Política Nacional de Ciberseguridad y se plantea como objetivo constituir un marco para proteger a usuarios mediante mejoras a los estándares con que son diseñadas, implementadas y operadas las redes. Al respecto, debe precisarse: 1) no existe ninguna ley que regule la materia de ciberseguridad en Chile, tanto es así que la propia Política Nacional de Seguridad fijó como uno de sus objetivos dictar una Ley Marco de Ciberseguridad; 2) el Decreto 533/2015, del Ministerio del Interior, creó el comité interministerial cuya misión es "proponer una política nacional de ciberseguridad y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales en la materia"; 3) el Instructivo Presidencial 1/2017 instruye la implementación de una Política Nacional de Ciberseguridad y el Instructivo Presidencial 8/2018 imparte instrucciones vigentes en materia de seguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado. Ni la Ley General de Telecomunicaciones ni el Decreto 1762/1977 contemplan, la función y/o atribución que Subtel se auto-atribuye en materia de ciberseguridad. En la actualidad, lo único que existe en la materia es la Política Nacional de Ciberseguridad y no se ha dictado la norma de carácter general y obligatoria que regule dicha materia. A mayor abundamiento, Subtel como

	órgano público, debe someterse de forma estricta a principios de legalidad y competencia, so pena que sus actuaciones sean nulas y sin ningún valor. Como lo ha establecido el artículo 6° de la Constitución, los órganos del Estado deben someter su acción a la Constitución y a las normas dictadas conforme a ella. Además, el artículo 7° de la Constitución dispone que "los órganos del Estado actúan válidamente, previa investidura regular de sus integrantes, dentro de su competencia y en la forma que prescriba la ley". Más aún, ninguna magistratura, ninguna persona ni grupo de personas pueden atribuirse, ni aún a pretexto de circunstancias extraordinarias otra autoridad o derechos que los que expresamente le confieran la Constitución y las leyes (inciso 2°), bajo la sanción de que tales actuaciones sean nulas y de ningún valor (inciso 3°). Lo anterior se encuentra ratificado por el artículo 2° de la LOC N° 18.575, que expresamente dispone que "los órganos de la Administración del Estado someterán su acción a la Constitución y a las leyes. Deberán actuar dentro de su competencia y no tendrán más atribuciones que las que expresamente les haya conferido el ordenamiento jurídico". De esta manera, al no existir una expresa habilitación legal que entregue a Subtel competencia en materia de ciberseguridad, consecuencialmente, no podría dictar una normativa asociada a dicha materia sin vulnerar el principio de legalidad, en cuya virtud la regulación de los aspectos sustantivos de determinadas materias –como sucede con Ciberseguridad- sólo puede ser efectuada por ley, máxime, además, si dicha normativa restringe garantías constitucionales. Las normas administrativas pueden complementar los preceptos legales, pero en ningún caso pueden ir en contra de la ley, ni menos establecer condiciones o prohibiciones al margen de la misma, ni menos regular una materia que la constitución reserva a una normativa de jerarquía legal