San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

Señora
Paula Bogantes Zamora
Ministra del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
despacho.ministerial@micitt.go.cr

Estimada señora:

El viernes cuatro de agosto de 2023, recibimos el oficio MICITT-DM-OF-651-2023, mediante el cual nos dan audiencia escrita por un plazo de 10 días, con carácter confidencial, para referirnos al texto propuesto para el decreto ejecutivo *"REGLAMENTO SOBRE MEDIDAS DE CIBERSEGURIDAD APLICABLES A LOS SERVICIOS DE TELECOMUNICACIONES BASADOS EN LA TECNOLOGÍA DE QUINTA GENERACIÓN MÓVIL (5G)".*

La propuesta de reglamento plantea como objeto "(…) *establecer medidas de ciberseguridad para garantizar el uso y la explotación, segura y con resguardo de la privacidad de las personas, de las redes y los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G)"* (artículo 1), estando sometidos a este reglamento: la habilitación de redes y servicios basados en 5G, actividades de contratación pública con objeto de uso y explotación del espectro radioeléctrico basado en 5G, oferentes en procesos de contratación pública con objeto de uso y explotación del espectro radioeléctrico basado en 5G y personas físicas o jurídicas, públicas o privadas, nacionales o extranjeras que operen redes o presten servicios basados en 5G y permisarios de 5G (artículo 2).

I. CONSIDERACIÓN GENERAL SOBRE LAS DISPOSICIONES REGLAMENTARIAS

La Guía para la elaboración de Reglamentos Técnicos Nacionales[1], de la Dirección de Mejora Regulatoria y Reglamentación Técnica del Ministerio de Economía, Industria y Comercio (MEIC), señala dentro de las características de una buena reglamentación técnica, conceptos tales como: **apego jurídico** (principio de legalidad), **aplicabilidad** (objetiva y aplicable en la práctica, de fácil cumplimiento), **claridad** (fácil de comprender para todos los ciudadanos), **eficaz** (que alcance o cumpla el objetivo propuesto), **equilibrada** (no se debe ser omisa ni excesiva en cuanto a los requerimientos legales), **funcionalidad** (debe ser operativa y coordinada con el fin de lograr lo que esta se propone), **transparente** (debe estar expresa y claramente establecida), y finalmente, **uniformidad** (debe evitar la duplicidad de trámites en las instituciones relacionadas).

A partir de lo señalado en la Guía de cita, es recomendable que el reglamento propuesto, considere lo establecido por la autoridad competente en la materia, siendo que dichas disposiciones se constituyen en un índice de aplicación en la elaboración de instrumentos normativos como el que se traslada a consulta de esta Superintendencia.

[1] Disponible en https://www.reglatec.go.cr/reglatec/DescargaAdjunto?name=Guia_.pdf

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

En términos generales, sin demérito del análisis que se realizará en los siguientes puntos, no se tiene claridad en cuál es la entidad responsable de realizar ciertas funciones contempladas en la propuesta de reglamento, lo que dista de las características de la buena regulación que debe considerar dicho instrumento. A guisa de ejemplo, en el Capítulo III, artículos 5 al 11, se hace referencia a la información que se recaba en el proceso de gestión y mitigación de riesgos nacionales de ciberseguridad 5G, sin que exista precisión y claridad de cómo se van a gestionar estos, y la entidad que se encargará de su seguimiento y fiscalización.

II. DE LA EXISTENCIA DE NORMATIVA EN RELACIÓN CON EL TEMA CONSULTADO

Es importante señalar que en materia de protección y tutela de los derechos de los usuarios finales en temas de telecomunicaciones, es competencia de la Sutel lo desarrollado en el Capítulo II, de la Ley N°8642. Por su parte, en lo que se refiere a la protección de *"los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos",* es competencia de la Agencia de Protección de Datos de los Habitantes (Prodhab), según se establece en la Ley N°8968, denominada Ley de Protección de la Persona frente al tratamiento de sus datos personales y la propuesta de reglamento no hace relación alguna a dicha ley.

III. DE LOS PROCESOS CONCURSALES DE ESPECTRO

De la lectura del proyecto de reglamento se desprende que en el apartado antecedentes, punto XLVII y XLVIII, se referencia la instrucción a la Sutel para el inicio del concurso público de bandas de espectro radioeléctrico para el desarrollo de sistemas IMT, incluyendo 5G, así como el lineamiento "K" del documento denominado *"Lineamientos técnicos adicionales de la Ministra Rectora en cumplimiento de lo dispuesto en el artículo 2 del Acuerdo Ejecutivo N° 031-2023-TEL-MICITT",* relativo a *"Seguridad de las redes IMT-2020 y la privacidad de los usuarios de los servicios de telecomunicaciones."*

En cumplimiento de lo dispuesto por el ente rector, es de conocimiento del MICITT que en el borrador de pliego de condiciones del concurso IMT 5G, se incorporaron en el apartado ***"21.3.17. Requisitos mínimos de seguridad",*** donde entre otras cosas *"El Concesionario debe cumplir con los protocolos de seguridad 3GPP"*, que es la regulación de referencia para este tipo de redes.

En virtud de lo anterior, se somete a valoración del MICITT, considerar las condiciones de seguridad propuestas en el citado apartado en aplicación de normas como las de la 3GPP (conocido por sus siglas en inglés *"The 3rd Generation Partnership Project"*).

Asimismo, en el borrador del pliego de condiciones, se estableció en ese mismo apartado, que el *"Concesionario debe cumplir con la normativa y disposiciones que se emitan en la materia",* en consecuencia, se desprende de las reglas pre cartelarias que los posibles adjudicatarios estarán sometidos a las nuevas disposiciones normativas que al efecto se emitan.

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

IV. DEL PRINCIPIO NEUTRALIDAD TECNOLÓGICA

El artículo 3 inciso h) de la Ley General de Telecomunicaciones, establece lo siguiente:

> ***"h) Neutralidad tecnológica:*** *posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados, cumplan los requerimientos necesarios para satisfacer las metas y los objetivos de política sectorial y se garanticen, en forma adecuada, las condiciones de calidad y precio a que se refiere esta Ley."*

Según se observa en el numeral citado, el principio de neutralidad tecnológica evoca la facultad de los operadores de redes y proveedores de servicios de telecomunicaciones para elegir las tecnologías por utilizar siempre que estas sean acordes a los estándares debidamente establecidos. En este sentido, el Reglamento se direcciona a regular la materia de ciberseguridad únicamente para la tecnología 5G, dejando de lado las otras tecnologías (2G, 3G, 4G, entre otras) actualmente en funcionamiento, sobre las cuales igualmente pueden darse riesgos de seguridad.

Así las cosas, la propuesta reglamentaria no cumple con el principio citado, siendo que está direccionada únicamente a un tipo de tecnología, incluso dejando de lado que las redes 5G pueden operar de forma interconectada con otras tecnologías como lo es el modo *"non-standalone"*[2], dada la facultad que ostentan los operadores de desarrollar y diseñar sus propias redes.

Finalmente, el reglamento propuesto debería apegarse al principio de neutralidad tecnológica, siendo que debe contemplar las tecnologías en uso y las que se vayan a desarrollar e implementar.

V. DE LAS COMPETENCIAS DE SUTEL EN LA MATERIA

El artículo 60 inciso 1) de la Ley General de la Administración Pública (LGAP), establece que la competencia de los entes y órganos públicos *"se limitará por razón del territorio, del tiempo, de la materia y del grado",* implicando que la competencia por la materia se refiere a los fines que se deben perseguir y las tareas y actividades o actuaciones sustanciales que legítimamente puede desempeñar el ente u órgano para alcanzarlos, rigiendo para estos efectos el criterio de especialidad, en aras del cumplimiento de los fines para los cuales fue creada para el caso particular la Sutel.

En su artículo 129, la LGAP dispone que: "*El acto deberá dictarse por el órgano competente y por el servidor regularmente designado al momento de dictarlo, previo cumplimiento de todos los trámites sustanciales previstos al efecto y de los requisitos indispensables para el ejercicio de la competencia."* Por definición legal entonces, la competencia se instituye en un elemento sustantivo necesario para la validez de los actos administrativos.

[2] Las redes *"non-standalone"* utilizan la interfaz de radio de 5G (NRAN o new radio) y el núcleo o core de redes 4G.

Seguidamente el artículo 60 inciso a) de la Ley de la Aresep (Ley N°7593), determina como una obligación fundamental de la Sutel aplicar *"el ordenamiento jurídico de las telecomunicaciones, para lo cual actuará en concordancia con las políticas del Sector (…)".*

De la lectura de la Ley de la Autoridad Reguladora de los Servicios Públicos y de la Ley General de Telecomunicaciones y su reglamento, no se observan competencias específicas de la Sutel en relación con temas de ciberseguridad tal y como se contempla en el reglamento en consulta. Así las cosas, las obligaciones y funciones de la Sutel y el Consejo están establecidas en los artículos 59, 60 y 73 de la Ley de la Autoridad Reguladora de los Servicios Públicos (Ley N°7593), y de su lectura no se desprenden competencias puntuales de la Superintendencia en temas de ciberseguridad y su fiscalización y mucho menos en lo relativo a la cadena de suministros.

La protección de datos en los servicios de telecomunicaciones se encuentra normada a través de un conjunto de estipulaciones legales e infra legales, dentro de las cuales podemos referir la Ley General de Telecomunicaciones, Ley N° 8642, su Reglamento Ejecutivo aprobado mediante Decreto Ejecutivo N° 34765, el Decreto Ejecutivo N° 35205 que define el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones, así como el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones dictado por la Junta Directiva de la Autoridad Reguladora de los Servicios Públicos.

De manera particular la LGT en su artículo 2 inciso d) dispone dentro de sus objetivos *"garantizar la privacidad y confidencialidad en las comunicaciones, de acuerdo con nuestra Constitución Política."* Y en su artículo 3 inciso j) remite de manera expresa al artículo 24 de nuestra Carta Magna que garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.

Del mismo modo, la LGT en su Título II de Garantías Fundamentales, Capítulo II Régimen de protección a la intimidad y derechos del usuario final, establece un conjunto especial de normas legales que protegen la privacidad de las comunicaciones y la confidencialidad de los datos de los usuarios finales (ver artículos 41-43).

Y en un ámbito infra legal, el Poder Ejecutivo mediante Decreto Ejecutivo Nº 35205-MINAE, dictó el referido Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones, mismo que en su artículo 5 inciso o) define el tratamiento de datos como las "*Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la selección, grabación, conservación, elaboración, modificación, bloqueo y cancelación de información relacionada con las comunicaciones hechas a través de redes de telecomunicaciones, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

En el mismo sentido, el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, define en su artículo 3 el concepto de comunicación como "*cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de telecomunicaciones electrónicas disponible para el público (…)"*

Con fundamento en estas disposiciones, podemos identificar en el ordenamiento jurídico de las telecomunicaciones, una protección especial a favor del derecho fundamental a la intimidad del usuario final, el cual se enfoca en la privacidad y el secreto de sus comunicaciones, con inclusión de sus datos personales relacionados con el proceso de comunicación, localización y tasación de servicios.

A la Sutel le corresponde entonces, en su rol de regulador del sector telecomunicaciones, asegurar que las comunicaciones (v.gr. llamadas o sesiones de datos), no sean intervenidas, escuchadas o inspeccionadas por terceros no autorizados por el usuario, con las excepciones normativas antes referidas.

Y en relación con los datos personales vinculados con la localización y cobro, la protección que brinda la Sutel comprende por imperativo legal, el intercambio de registros de tasación de los servicios e interconexión (v.gr. CDRs de llamadas o de datos) de forma que no opere un posible *"rastreo"* de comunicaciones, sin la autorización del titular de la información o por orden judicial o del Ministerio Público, según corresponda. Debiendo reiterarse en este sentido que, dentro de las competencias otorgadas a este Órgano regulador, no destaca el registro y administración de las bases de datos gestionadas por las empresas reguladas dentro de su giro comercial.

De conformidad con lo anterior, es claro que la normativa legal e infra legal de telecomunicaciones, en lo que respecta a las competencias de la Sutel, regula expresamente el régimen de protección de los derechos de los usuarios finales, y no contempla dentro de su amplio ámbito de regulación lo relativo a las medidas de ciberseguridad y cadena de valor aplicables a los servicios de telecomunicaciones, tal como se propone en el Reglamento sobre Medidas de Ciberseguridad.

En lo que respecta al reglamento propuesto, en los artículos 9 (Análisis y gestión del riesgo en la cadena de suministros) y 11 (Medidas aplicables ante la identificación de riesgo alto)**,** se cita a esta Superintendencia y se le otorgan competencias puntuales, sin que las mismas provengan de la normativa legal que regula la materia de telecomunicaciones y que le resulta aplicable (Ley N°7593 y Ley N° 8642 y su reglamento), razón por la cual se debe valorar excluir a la Sutel de las funciones que en los citados numerales se pretenden endilgar a esta Superintendencia.

Finalmente, no debe confundirse lo que es la regulación de la tutela de los derechos de los usuarios finales, con las redes de comunicación de los operadores de los servicios de telecomunicaciones. Los objetivos de la Ley N°8642, sobre la protección de los derechos de los usuarios (Capítulo II, Ley N°8642) no están relacionados con temas de ciberseguridad en las redes, sino con el régimen de protección a la intimidad y derechos de éstos, por lo que es conveniente realizar la distinción entre uno y otro régimen, con el fin de delimitar la materia regulatoria y las entidades a cargo de su fiscalización y cumplimiento.

VI. DEL EXCESO DE LA POTESTAD REGLAMENTARIA

La normativa que se pretende implementar roza con aspectos de legalidad y competencia, puesto que el artículo 2 de la propuesta reglamentaria impone obligaciones a sujetos que no califican como operadores de redes o prestadores de servicios de telecomunicaciones a pesar de que el artículo 1 de la Ley 8642 define dentro de su ámbito de aplicación que están sometidas a la misma *"las personas físicas o jurídicas, públicas o*

privadas, nacionales o extrajeras que operen redes o presten servicio de telecomunicaciones que se originen, terminen o transiten por el territorio nacional."

Además de que, el artículo 42 de la Ley 8462 es enfático en señalar que los sujetos obligados a garantizar el secreto de las comunicaciones, el derecho a la intimidad y a la protección de datos de carácter personal de los abonados y usuarios finales, son los operadores y proveedores de servicios de telecomunicaciones, por lo que dicha obligación no puede hacerse extensiva a terceros no previstos por dicha ley, como lo sería los oferentes en procesos de contratación pública, los permisionarios o aquellos que habiliten redes y servicios o sean proveedores de equipos tecnológicos.

En relación con el mismo tema, la Procuraduría General de la República en el Criterio C-200-2002 del 12 de agosto del 2002 cita a la Sala Constitucional la cual ha expresado que:

> *"La potestad reglamentaria es la atribución constitucional otorgada a la Administración, que constituye el poder de contribuir a la formación del ordenamiento jurídico, mediante la creación de normas escritas (artículo 140 incisos 3 y 18 de la Constitución Política). *La particularidad del reglamento es precisamente el ser una norma secundaria y complementaria, a la vez, de la ley* cuya esencia es su carácter soberano (sólo limitada por la propia Constitución), en la creación del Derecho. Como bien lo resalta la más calificada doctrina del Derecho Administrativo, *la sumisión del reglamento a la ley es absoluta, en varios sentidos*: no se produce más que en los ámbitos que la ley le deja, *no puede intentar dejar sin efecto los preceptos legales o contradecirlos, no puede suplir a la ley produciendo un determinado efecto no querido por el legislador* **o regular un cierto contenido no contemplado en la norma que se reglamenta** (...)* (Resaltado corresponde al original)
>
> *Dentro de los reglamentos que puede dictar la administración, se encuentra el que se denomina* ***"Reglamento Ejecutivo", mediante el cual ese Poder en ejercicio de sus atribuciones constitucionales propias, el cual se utiliza para hacer posible la aplicación o ejecución de las leyes, llenando o previendo detalles indispensables para asegurar no sólo su cumplimiento, sino también los fines que se propuso el legislador, fines que nunca pueden ser alterados por esa vía. *Ejecutar una ley no es dictar otra ley, sino desarrollarla, sin alterar su espíritu por medio de excepciones, pues si así no fuere el Ejecutivo se convierte en legislador*** *(…)".* (Destacado intencional)

En dicho criterio, también se desarrolla las consecuencias de un exceso en la potestad reglamentaria, al violarse los límites que este tipo de normativa tiene con respecto al texto legal:

> *"A. Sobre los Reglamentos Ejecutivos*
>
> *(…) En cuanto a su definición señala Eduardo Ortiz: "(…) es una norma que tiene por objeto el hacer posible la aplicación práctica y precisa de la ley, dentro de las condiciones que ella misma prevé"*[3]

[3] Tesis de Derecho Administrativo. Departamento de Publicaciones, U.C.R., 1976, tesis VII, p.12.

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

Sobre el particular, Rubén Hernández Valle define el reglamento de la siguiente forma:

> *"(…) es el producto del ejercicio de la potestad reglamentaria, la cual puede definirse como el poder que dimana directamente de la Constitución, en virtud del cual las Administraciones Públicas pueden dictar normas con eficacia jurídica inferior a la ley".*[4]

En relación con su objeto continúa argumentando el autor: *"consiste en aclarar, precisar o complementar la ley (…). Dado que el Reglamento Ejecutivo desarrolla los términos de la ley, de allí derivan límites precisos al ámbito de su regulación. (…). Por mayoría de razón,* ***tampoco puede esta clase de Reglamento innovar el ordenamiento jurídico, reformando o derogando normas de rango superior, o interpretar auténticamente normas legales. Tampoco puede violar lo que la ley dispone o permitir lo que ella prohíbe. Dentro de este orden de ideas, el Reglamento Ejecutivo no puede crear nuevas obligaciones ni suprimir derechos contenidos en la ley que regula****"*[5]

Es así como, partiendo de las anteriores consideraciones doctrinales y jurisprudenciales, y toda vez que se presente en la especie una incompatibilidad de contenidos entre una norma de rango legal y otra de carácter reglamentario, es que nos encontraríamos ante un **exceso en el ejercicio de la potestad reglamentaria**, por lo que procedería desaplicar toda aquella normativa reglamentaria que modifique y contradiga los contenidos de la norma de rango legal, derivado de la jerarquía normativa.

En este sentido se ha pronunciado la Procuraduría en los dictámenes N° C-129-96 del 6 de agosto de 1996 y C-111-2000 de 17 de mayo del 2000, indicando en esa oportunidad lo siguiente: *"Es preciso indicar que ante el supuesto de contradicción o exceso de la potestad reglamentaria, es claro que la ley debe privar como consecuencia del principio de jerarquía normativa, con lo cual debe desaplicarse la norma reglamentaria que exceda los límites que se le imponen*."[6]

Así las cosas, la referencia al artículo 42 de la LGT y la asignación de competencias o funciones a la Sutel en la propuesta de Reglamento de Ciberseguridad, podría constituir un exceso en la potestad reglamentaria por parte del Poder Ejecutivo, siendo lo regulado en el reglamento, carece de base legal que le ampare.

VII. DEL PROYECTO DE LEY SOBRE CIBERSEGURIDAD

Por otra parte, resulta relevante destacar que la presente propuesta reglamentaria no se encuentra amparada a una ley que regule específicamente dicha materia como se pretende con el proyecto tramitado en la Asamblea Legislativa con el expediente N° 23292 denominado ***"LEY DE CIBERSEGURIDAD DE COSTA RICA"*** en el cual se propone en su artículo 4 la creación de la Agencia Nacional de Ciberseguridad que formará parte del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), la Agencia estará bajo la Dirección de Gobernanza Digital del (MICITT) como encargada de la gestión preventiva, reactiva y proactiva

[4] El Derecho de la Constitución. Volumen I, Editorial Juricentro, San José, 1993, p.611.
[5] Hernández. Op. Cit. p. 623
[6] Artículo 6 de la Ley General de la Administración Pública, en relación con el artículo 2 del Código Civil.

de las amenazas e incidentes cibernéticos que, a través del uso de datos, puedan generar un riesgo para la población costarricense.

Inclusive, nótese que este proyecto define en su artículo 3 inciso t) como servicios esenciales objeto de la regulación: *"Todo servicio, prestado por el Estado **o por empresas privadas**, respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción, no disponibilidad o destrucción de su infraestructura de la información pueda afectar gravemente: la vida o integridad física de las personas; la provisión de servicios sean estos: sanitarios, de seguridad, energéticos, de suministro de agua, educativos **o de telecomunicaciones**; y al normal funcionamiento de infraestructura vial y medios de transporte; a la generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; o de modo general, el normal desarrollo y bienestar de la población."* (Destacado intencional)

Además, que, en el artículo 33 de dicha propuesta de ley también se prevén obligaciones específicas para la protección de datos personales sensibles dentro de los cuales se encuentran:

"(…)

a) *Identificar, resguardar los datos personales sensibles y de misión crítica almacenados por la institución, de acuerdo con el inventario requerido en el artículo anterior y en cumplimiento de la normativa aplicable en el país.*
b) *Evaluar los controles de acceso a los datos descritos en el apartado anterior, la necesidad de un almacenamiento fácilmente accesible de los datos y la necesidad de los individuos de acceder a los datos.*
c) *Cifrar o hacer indescifrables para los usuarios no autorizados los datos descritos en el apartado a), que se almacenan en los sistemas de información de la institución o que transitan por ellos (…)"*

Finalmente, en el Transitorio III se propone que el Poder Ejecutivo deberá reglamentar la propuesta de Ley en un plazo de seis meses posterior a su publicación.

Así las cosas, la emisión de reglamentos que correspondan a temas de ciberseguridad deben necesariamente correlacionarse con las disposiciones legales particulares que se aprueben sobre esta materia, y en el caso del Reglamento de Ciberseguridad consulta, se observa la ausencia de respaldo normativo que permita su desarrollo de una forma clara, precisa y uniforme, según lo establece la Guía para el establecimiento de reglamentos técnicos de la Dirección de Mejora Regulatoria del MEIC.

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

VIII. ANÁLISIS DE LOS ARTÍCULOS DE LA PROPUESTA DE REGLAMENTO

A continuación se realizará un breve análisis de los artículos 2 y 8 al 11 del Reglamento de Ciberseguridad propuesto:

- **Artículo 2. Ámbito de aplicación**

De conformidad con lo establecido en el punto 1 de este informe, el ámbito de aplicación no está claramente delimitado, lo que podría resultar en su inaplicabilidad, por cuanto, se establece como parte de los elementos sometidos al reglamento "*equipamiento tecnológico activo*" (inciso a), no resultando claro ni preciso el por qué se somete al reglamento a una empresa que se dedica a la manufactura de equipo tecnológico, no regulada en materia de telecomunicaciones.

La actividad de contratación pública que tenga por objeto la habilitación del uso y la explotación del espectro radioeléctrico tiene como fin la implementación de redes y servicios de telecomunicaciones, por lo que aplicación de un reglamento de este tipo, tiene que estar dirigido a las redes y servicios de telecomunicaciones, y no a la actividad de contratación pública (inciso b).

En el inciso c) de la propuesta reglamentaria, se hace referencia a los *"oferentes"* en los procesos de contratación pública, siendo que un oferente no podría estar sujeto a la reglamentación propuesta dado que éste asumiría los derechos y obligaciones de un proceso de contratación hasta que se constituya en contratista.

En este artículo, debe considerarse lo relativo al concepto de neutralidad tecnológica, siendo que se enfoca en la tecnología de quinta generación 5G.

Asimismo, a lo largo del reglamento, se hace referencia al *"ámbito de aplicación del artículo 2 de este reglamento",* (véase el artículo 7, 6, 8, entre otros), por lo que su claridad y precisión permitirá su debido cumplimiento.

Finalmente, debe considerarse el artículo 6 inciso 20)[7], 9 y 26 de la LGT, por cuanto existe una incongruencia o contradicción con lo señalado en el inciso e) del reglamento propuesto y su último párrafo *("Exceptúese de su aplicación la operación de redes privadas de telecomunicaciones"*). En este inciso, es importante señalar que un permisionario de frecuencias únicamente puede operar redes privadas, así sean *"los permisionario 5G",* siendo que independientemente de la tecnología en la cual implementen sus redes (principio neutralidad tecnológica), su operación estará limitada a una red privada de telecomunicaciones de uso no comercial.

[7] **20) Red privada de telecomunicaciones:** red de telecomunicaciones destinada a satisfacer necesidades propias de su titular, lo que excluye la prestación y explotación de estos servicios a terceros.

- **Artículos 8 y 9 (Gestión del Riesgo de las Redes 5G y Análisis y Gestión del Riesgo en la cadena de suministro):**

Estos artículos se relacionan entre sí, y refieren a la gestión de riesgos en las redes 5G y al análisis y gestión del riesgo en la cadena de suministro, respectivamente.

Como un primer aspecto a considerar, es que en ambos artículos se hace referencia a que dichas disposiciones de análisis y gestión de riesgos, resultan de aplicación a *"Quienes se encuentren comprendidos"* y a *"Los sujetos comprendidos"*, sin embargo, como ya señaló el artículo 2 tiene múltiples imprecisiones que debe ser ajustadas, y además, los 2 primeros incisos no están referidos a personas, sino a redes y servicios, equipos y actividad de contratación pública.

No se tiene claridad de cuál o cuáles son las entidades responsables de velar por el cumplimiento y fiscalización de la normativa propuesta, considerando lo señalado en el punto 3 de este informe sobre las competencias de esta Superintendencia.

En este sentido, el artículo *"9. Análisis y Gestion del Riesgo en la Cadena de Suministro",* no señala el procedimiento a seguir con la información que se recabe en el proceso de análisis y gestión del riesgo en la cadena de suministro, no indica qué pasa si dicha información no se presenta, no es clara sobre las funciones de las autoridades competentes para recabar y procesar esa información, y en específico, tampoco es clara en determinar quién es el competente de velar por la cadena de suministro, en el entendido de que se trata de un tema más de índole comercial que regulatorio de las telecomunicaciones, por lo que tal y como se indicó no se puede considerar la cadena de suministro como un elemento en el ámbito de regulación de la Sutel.

- **Artículos 10 y 11 (Parámetros de riesgo alto y medidas aplicables ante la identificación de riesgo alto)**

Por su parte, en lo atinente a los *"Parámetros de riesgo alto",* establecidos en el artículo 10, en su mayoría se enfocan a aspectos de software y hardware de proveedores de equipos y diversas presiones sobre éstos, así como sus ubicaciones geográficas, y la relación con los respectivos gobiernos, sobre lo cual esta Superintendencia no ostenta ninguna competencia. Al respecto, en dicho artículo se regulan parámetros no vinculados a aspectos técnicos, como por ejemplo, la tutela sobre los datos trasegados en las redes de telecomunicaciones, autenticación de usuarios y redes, encriptado y cifrado de las comunicaciones, entre otros. Se observa referencia temas de índole político (presiones de gobiernos) y demográficos, sin que estos elementos puedan ser considerados parámetros técnicos objetivos relacionados con el alto riesgo en materia de ciberseguridad y sin que exista precisión respecto a dichas consideraciones políticas que determinan los riesgos esbozados.

De la lectura del numeral 10 propuesto, se colige que los parámetros de riesgo alto están direccionados a la cadena de suministros, siendo que se hace referencia en sus diversos incisos a los proveedores de hardware y software, sea se encuentra dirigido a fabricantes o comerciantes de equipos y de software, los cuales no se encuentran comprendidos como sujetos de regulación en la LGT.

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

En adición a lo anterior, los parámetros de alto riesgo establecidos, y según la referencia errónea (en criterio de esta Superintendencia) al artículo 42 de la LGT, que se realiza en el artículo 11 de la propuesta de reglamento *"…de parámetros de riesgo alto deberá informarlo a la Superintendencia de Telecomunicaciones de conformidad con las disposiciones del artículo 42 de la Ley General de Telecomunicaciones, N°8642,dentro de los 3 días naturales siguientes a su identificación y adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de sus redes y sus servicios.",* no se corresponden con la materia regulada en la normativa de Telecomunicaciones, dado que esos parámetros de alto riesgo no guardan relación con la regulación de los derechos de los usuarios en el trasiego de sus datos a través de las redes de telecomunicaciones, sino como ya se indicó, refieren a consideraciones de índole político y demográfico de los proveedores de hardware y software.

Tal y como se desprende, los alcances del artículo 42 de la Ley 8642 están delimitados para garantizar la privacidad de las comunicaciones que se tramitan por medio de las redes de telecomunicaciones, siendo los operadores y proveedores de dichos servicios los únicos obligados a velar por el cumplimiento de dicha obligación.

Del mismo modo, se establece que la presencia de parámetros de alto riesgo debe ser informada a la Sutel, sin que se especifique el tratamiento o procedimiento que se debería seguir una vez comunicada la incidencia de alto riesgo o las consecuencias de su no presentación, amén de lo ya señalado, con respecto a la ausencia de norma expresa que habilite a la Sutel para atender situaciones como las descritas en dicho numeral, por lo que es importante que dicha información sea canalizada por medio del ente competente.

En el párrafo in fine del artículo 11, se hace referencia a *"autoridades correspondientes"* de manera genérica, sin que se concrete quién es el competente de la función ahí señalada, lo cual refuerza las imprecisiones de la propuesta reglamentaria y su distanciamiento de las mejores prácticas reglamentarias establecidas en la citada Guía para la elaboración de reglamentos técnicos. Además, debe considerarse que los procesos concursales de espectro radioeléctrico no deben regular o reglamentar lo relativo a la cadena de suministros propiamente, sino que únicamente se limitan a establecer parámetros técnicos concernientes con el resguardo de la seguridad de la información que se trasiega en las redes y la tutela de los derechos de los usuarios finales de los servicios de telecomunicaciones.

Finalmente, se establece en la propuesta de reglamento que *"contar con parámetros de riesgo alto se establece como uso incorrecto del espectro radioeléctrico",* no obstante, debe considerarse que dentro de las causales del régimen sancionatorio de la LGT, no se encuentra una disposición en ese sentido, por lo que podría resultar vacío de contenido una declaratoria de uso incorrecto del espectro, siendo que no podría aplicarse una sanción de conformidad con la normativa vigente de Telecomunicaciones. De igual forma, debe recordarse que el régimen sancionatorio debe derivar de una norma legal que le ampare, ergo, está vedado a la Administración Pública crear causales y sanciones, sin una norma de base legal que le ampare expresamente.

San José, 17 de agosto del 2023
06900-SUTEL-CS-2023

IX. ANÁLISIS DE LA PROPUESTA DE REGLAMENTO DE CARA A LA NORMATIVA DE COMPETENCIA EN LA OPERACIÓN DE REDES Y SERVICIOS DE TELECOMUNICACIONES

Dentro de ese marco de rango legal de la SUTEL, se estableció un régimen sectorial de competencia a su cargo, que se rige según lo dispuesto en el Título III, Capítulo II, de la Ley 8642 y supletoriamente por los criterios establecidos en el Capítulo III de la Ley 7472; régimen sectorial sobre el que la Procuraduría General de la República en el dictamen 015 del 19 de enero de 2010 refirió en lo que interesa:

> *"Cabe señalar, además, que cuando el artículo 52 de la Ley de Telecomunicaciones define la competencia de la Superintendencia de Telecomunicaciones como regulador en materia de competencia efectiva, le atribuye la promoción de los principios de competencia, analizar el grado de competencia efectiva en los mercados, determinar los actos que pueden afectar la competencia, garantizar el acceso al mercado y el acceso a las instalaciones equitativas; evitar abusos y prácticas monopólicas, así como conocer, corregir y sancionar las prácticas monopolísticas cometidas por operadores o proveedores que tengan por objeto o efecto limitar, disminuir o eliminar la competencia en el mercado de las telecomunicaciones".*

La Ley General de Telecomunicaciones, Ley 8642 y la Ley de la Autoridad Reguladora de los Servicios Públicos, Ley 7593, facultan a la SUTEL, como autoridad sectorial de competencia, a velar porque la regulación impulsada e implementada no genere restricciones anticompetitivas, que afecten el desempeño eficiente del mercado de telecomunicaciones.

De conformidad con lo anterior, la operación de redes, incluyendo aquellas que soportan los servicios de radiodifusión sonora y televisiva de acceso libre, y la prestación de servicios de telecomunicaciones, están sujetos al régimen sectorial de competencia en telecomunicaciones y su aplicación corresponde exclusivamente a la SUTEL (artículo 2 de la Ley de Fortalecimiento de las Autoridades de Competencia de Costa Rica, Ley 9736); régimen que se aplica en igualdad de condiciones a todos los operadores de redes y proveedores de servicios de telecomunicaciones, sean estos públicos o privados.

En este sentido, el artículo 20 de la Ley 9736 establece que la SUTEL realizará actividades de promoción y abogacía de la competencia con el objetivo de fomentar e impulsar mejoras en el proceso de competencia y libre concurrencia en el mercado; eliminar y evitar las distorsiones o barreras de entrada, así como aumentar el conocimiento y la conciencia pública sobre los beneficios de la competencia.

Legalmente la normativa establece las diversas herramientas no coercitivas que posee la SUTEL en materia de promoción y abogacía de la competencia, tales como emisión de opiniones y recomendaciones, emisión de guías, realización de estudios de mercado, actividades de asesoramiento, capacitación y difusión, acuerdos de cooperación, programas de cumplimiento voluntario, además de la difusión y publicación de su labor.

En particular, según los artículos 21 de la Ley 9736, 24 del Reglamento a esa misma Ley y 30 del Reglamento del régimen de competencia en telecomunicaciones de la Superintendencia de Telecomunicaciones, la SUTEL tiene la potestad de emitir opiniones y recomendaciones en materia de competencia y libre concurrencia, de

oficio o a solicitud del Poder Ejecutivo, de la Asamblea Legislativa, demás entidades públicas o de cualquier administrado, sobre la promulgación, modificación o derogación de leyes, reglamentos, acuerdos, circulares y demás actos y resoluciones administrativas, vigentes o en proceso de adopción.

La propuesta de reglamento establece medidas de ciberseguridad con la finalidad de garantizar el uso y explotación de manera segura y con el resguardo de la privacidad de las personas, de redes y servicios de telecomunicaciones basados en la tecnología 5G; por ende, se considera que lo dispuesto en la propuesta de reglamento tiene incidencia en el mercado de las telecomunicaciones y en el actuar de la SUTEL.

1. DEL MARCO PARA EL ANÁLISIS DE LA REGULACIÓN QUE SE PRETENDE PROMULGAR

La promulgación, modificación o derogación de leyes, reglamentos, acuerdos, circulares y demás actos y resoluciones administrativas (en adelante regulaciones), vigentes o en proceso de adopción, son una herramienta legítima que posee el Estado para lograr metas específicas a nivel de política pública, por lo que es vital valorar su impacto sobre el nivel de competencia.

La mayor parte de regulaciones no tienen el potencial de dañar indebidamente los niveles de competencia, pero en algunos casos, si dichas regulaciones se diseñan sin garantizar principios básicos de libre concurrencia, pudiera generar una distorsión que afecte la innovación y el crecimiento a largo plazo del sector de las telecomunicaciones, perjudicando en última instancia al consumidor. Por el contrario, si se diseñan regulaciones haciendo hincapié en los principios de competencia, el mercado saldrá beneficiado como un todo, tanto por parte de las empresas, como de los consumidores.

En este sentido, una de las principales actividades de Abogacía de la Competencia que realizan las diversas autoridades a nivel mundial consiste en el análisis de las restricciones públicas a la competencia. Dicho análisis permite proporcionar insumos para fortalecer a las legislaciones, regulaciones o políticas, ya sean en proceso de elaboración o existentes, para prevenir que estas resulten en restricciones que afecten a la competencia, generen resultados adversos en el precio, la calidad, la innovación, limiten las opciones de decisión del consumidor, entre otras consecuencias.

Es así como dentro del proceso de implementación de la Ley 9736, la SUTEL ha desarrollado la “Guía para la Evaluación de la Regulación desde la Perspectiva de la Competencia” (en adelante, Guía), aprobada mediante acuerdo 037-061-2022 del 5 de setiembre del 2022, por lo que lo pertinente es realizar el análisis de la propuesta de reglamento en estricto apego a su metodología.

Esta Guía desarrolla un método práctico para la identificación de restricciones a la competencia, en la que se parte del principio de que el Estado tiene la potestad, cuando lo considere necesario, de emitir reglas que norman las actividades económicas y sociales de los particulares para alcanzar objetivos de política pública concretos. Sin embargo, existen casos donde estas regulaciones, lejos de alcanzar tales objetivos, restringen el funcionamiento de los mercados.

De tal forma, el objetivo de la Guía es contar con un instrumento que permita identificar las políticas públicas existentes o propuestas que restrinjan indebidamente la competencia, desarrollando los criterios, específicos

y transparentes que toma en cuenta la SUTEL para realizar la evaluación de la competencia, así como para la evaluación de alternativas adecuadas que resulten más favorables al proceso competitivo de los mercados de telecomunicaciones y logren, a su vez, cumplir con los objetivos de interés público perseguidos, teniendo en cuenta los beneficios y costos de implementación.

De tal manera, la Dirección General de Competencia (DGCO) de la SUTEL ha valorado el posible impacto en la competencia en el sector telecomunicaciones de la propuesta de reglamento, utilizando como base dicha Guía.

A. PRIMERA FASE DE ANÁLISIS: ¿LA REGULACIÓN ANALIZADA RESTRINGE LA COMPETENCIA?

En lo que interesa para los efectos de esta Autoridad, la propuesta de reglamento contiene disposiciones que podrían tener el potencial de afectar la competencia, por lo cual el análisis de la DGCO se centra en los artículos 6, 7, 8, 9, 10 y 11 de la propuesta de reglamento.

A partir de esto, se procede a realizar el análisis puntual de los posibles efectos de los artículos referidos de la propuesta de reglamento en consulta para analizar su impacto sobre la competencia en el mercado de telecomunicaciones, lo anterior a partir de las preguntas contenidas en la Guía de la siguiente manera:

a. Regulaciones que limitan la cantidad o variedad de participantes del mercado

1. *¿Otorga a un proveedor o grupo de ellos el derecho exclusivo para explotar algún recurso, suministrar un bien o prestar algún servicio?*

La propuesta de reglamento **no** concede derechos exclusivos o especiales para explotar algún recurso, suministrar un bien o prestar algún servicio.

2. *¿Establece un sistema de licencias, permisos o autorizaciones para operar en el mercado?*

La propuesta de reglamento no fija procedimientos para la obtención de licencias, permisos o autorizaciones como requisito para iniciar operaciones, sin embrago, en el **artículo 11 condiciona** a los operadores que participen en **la asignación de concesiones** para el uso y explotación del espectro radioeléctrico para redes y servicios de telecomunicaciones 5G, indicando que no podrán tener parámetros de riesgo alto; el nivel de riesgo es tipificado por la misma propuesta de reglamento.

3. *¿Limita la posibilidad de ciertos tipos de operadores o proveedores para ofrecer un bien o prestar un servicio?*

La propuesta de reglamento en el **artículo 6** establece estándares de seguridad que deben aplicar todos los agentes sujetos al cumplimiento de la normativa, así mismo en el **artículo 8** se introduce el tema de auditorías en ciberseguridad, las cuales deberán ser realizadas por entidades acreditadas según los estándares establecidos; si bien, en este último artículo no se establece de forma tácita para los regulados con la normativa

la obligatoriedad de contar con las certificaciones mencionadas en el artículo 6, se podría interpretar que el no contar con dichas certificaciones podría resultar en un aspecto relevante para limitar la posibilidad de algún operador o proveedor de servicio de ofrecer sus servicios en tecnología 5G.

4. *¿Eleva de forma significativa el costo de entrada o de salida del mercado para un operador?*

La propuesta de reglamento **no** impone requisitos a la entrada o salida de un mercado que se considere que eleven de forma significativa los costos y que deban cumplir los operadores y/o proveedores que participan en el mercado de telecomunicaciones.

5. *¿Crea barreras geográficas para ofrecer bienes o prestar servicios?*

La propuesta de reglamento **no** contiene elementos relacionados con la capacidad de crear barreras de naturaleza geográfica para los operadores o proveedores de servicios basados en tecnología 5G.

6. *¿Limita la transferencia o cesión de licencias y autorizaciones?*

La propuesta de reglamento **no** fija procedimientos para la transferencia o cesión de licencias, permisos o autorizaciones como requisito.

7. *¿Crea preferencias en las compras de gobierno a efecto de promover o beneficiar a una categoría o grupo de proveedores?*

En su **artículo 10** la propuesta de reglamento impone una serie de características sobre los denominados suministradores de hardware y software de los sujetos comprendidos en el ámbito de acción de la normativa, que si bien son de aplicación igualitaria para todos los operadores y proveedores de servicios de telecomunicaciones en el país, al momento de dotarse de sus productos o servicios para 5G los operadores y proveedores de servicios de telecomunicaciones, tanto privados como estatales, deberán optar solo por aquellos suministradores de hardware y software que cumplan con los estándares definidos en el **artículo 6** y que a su vez no impliquen un riesgo alto como los mencionados en los incisos a), b), c), d), e) y f) del **artículo 10**, lo anterior, estimula las preferencias de las compras de los operadores y proveedores de telecomunicaciones estatales hacia los suministradores de hardware y software que cumplan con lo establecido en la normativa.

En suma, a partir del análisis de los primeros siete parámetros que contiene la Guía, es posible concluir que la propuesta de reglamento analizado tiene el potencial de limitar la posibilidad de ciertos tipos de operadores o proveedores de telecomunicaciones para prestar sus servicios al condicionar la asignación de concesiones para uso y explotación del espectro radioeléctrico para redes y servicios de telecomunicaciones 5G, así como al establecer características específicas, no estrictamente de índole comercial, que deberán adoptar los operadores y proveedores de telecomunicaciones al dotarse de bienes y servicios requeridos en la implementación de sus redes 5G.

b. Limitaciones a la capacidad de competir

1. *¿Limita las condiciones de la oferta de determinados bienes o servicios, incluyendo la posibilidad de determinar el precio o las condiciones de intercambio?*

La propuesta de reglamento **no** contiene elementos que limiten las condiciones de la oferta de servicios de telecomunicaciones.

2. *¿Limita la capacidad de promocionar o hacer publicidad de bienes o servicios?*

La propuesta de reglamento **no** contiene elementos relacionados con la publicidad de los servicios de telecomunicaciones o sus redes.

3. *¿Establece estándares técnicos o de calidad de los productos o servicios que proporcionan ventajas discriminatorias o exigencias que van más allá de lo razonable?*

La propuesta de reglamento en su **artículo 6** establece estándares de seguridad dirigidos a los operadores y proveedores de servicios basados en tecnología 5G y a los suministradores de hardware y software para sus redes, pero no se desprende que el cumplimiento de los estándares pueda generar ventajas discriminatorias al resultar de aplicación general para todos los agentes por igual.

Cabe señalar, que este tipo de normativa si bien tiene la capacidad de generar costos adicionales para los agentes relacionados a la tecnología 5G, la relación costo-beneficio de dicha implementación normativa pudiera ser positiva, en el tanto que los beneficios alcanzados en el colectivo en términos de ciberseguridad pudieran superar los costos incurridos.

4. *¿Eleva los costos de algunos operadores o proveedores respecto a otros?*

Si bien la aplicación de los estándares descritos en el **artículo 6,** así como la eventual sustitución de equipos, productos y servicios que demanda el **artículo 11**, tienen la capacidad de generar costos adicionales para los operadores y proveedores de servicios de telecomunicaciones basados en la tecnología 5G, la normativa no lo hace de manera discriminatoria si no que plantea una eventual elevación de costos de forma igualitaria, en virtud que aplica para todos los agentes involucrados.

5. ¿Exige el uso de algún estándar, modelo, plataforma o tecnología en particular, o de algún *producto o servicio protegido por derechos de propiedad intelectual o que resulte costoso?*

La propuesta de reglamento en su **artículo 6** establece estándares de seguridad que deberán ser cumplidos por todos los agentes sujetos al ámbito de aplicación de la normativa, así como la aplicación de auditorías (**inciso f), artículo 8**) derivadas de estos y si bien como se señaló en el punto 3 de esta subsección, son de aplicación general y no parecen tener el potencial de generar ventajas discriminatorias, lo cierto es que pueden elevar los costos para operar los servicios de telecomunicaciones bajo la tecnología 5G.

Así las cosas, con base en el análisis de los parámetros anteriores es posible concluir que la propuesta de reglamento analizado tiene el potencial de elevar los costos de todos operadores o proveedores basados en la tecnología 5G, producto de la aplicación de estándares establecidos en la normativa, así como de eventuales sustituciones de equipos, productos y servicios.

c. Reduce incentivos para competir vigorosamente

1. *¿Genera un régimen de autorregulación o co-regulación?*

La propuesta de reglamento **no** establece o fomenta un régimen de autorregulación o co-regulación por parte de los operadores de redes y/o proveedores. Así que no se observa afectación a nivel de competencia existente en el mercado.

2. *¿Exige o fomenta la publicación de información sobre volúmenes de producción, precios, ventas o los costos de los agentes económicos?*

La propuesta de reglamento **no** promueve un esquema que implique intercambios o publicidad de cierto tipo de información entre agentes económicos competidores entre sí, tales como, precios, costos de producción, volúmenes de producción, mercados atendidos o estrategias comerciales.

3. *¿Exime un sector, actividad o agentes económicos de la aplicación de las leyes de competencia?*

La propuesta de reglamento que se analiza **no** contempla ni incentivos, ni exenciones en favor de operadores de redes y/o proveedores de los servicios de telecomunicaciones, de la aplicación de la normativa de competencia vigente; de manera que no genera beneficios en favor de alguna empresa o actividad en particular.

4. *¿Promueve o permite acuerdos anticompetitivos?*

La propuesta de reglamento que se analiza **no** promueve o facilita la creación de acuerdos anticompetitivos entre de operadores de redes y/o proveedores de los servicios de telecomunicaciones.

5. *¿Genera incertidumbre regulatoria, permite la aplicación discrecional de las regulaciones?*

En el **artículo 7** de la propuesta de reglamento se señala que los sujetos comprendidos en el ámbito de aplicación de la norma deberán analizar los riesgos de seguridad de diferentes elementos de sus redes detectando vulnerabilidades y amenazas, los resultados de estos análisis deberán ser presentados por cada una de las actividades establecidas en el artículo 2; sin embargo, dentro de la normativa no se establece el procedimiento a seguir para la presentación de la información obtenida por medio de los análisis, es decir, no resulta claro aspectos referentes a la rendición tales como: a quién, cada cuánto y como se debe entregar.

Esa misma situación se replica en el **artículo 9**, en relación al análisis de riesgo, prácticas y medidas de seguridad requeridas a los suministradores de hardware y software, dado que el artículo 9 indica que esa información deberá presentarse atendiendo las particularidades de los procesos dispuestos por el Poder Ejecutivo y la Sutel para la habilitación de redes y servicios basados en la tecnología de quinta generación móvil (5G) de acuerdo con su ámbito de competencia, esto sin llegar a especificar los procesos a seguir para llevar a cabo dicha entrega.

El **artículo 8**, plantea incertidumbre regulatoria al señalar en el inciso f) el sometimiento a auditorías en ciberseguridad (asumiendo el costo el auditado) por parte de los sujetos comprendidos en el ámbito de aplicación de la norma, esto sin definir un procedimiento dejando con ello en el limbo aspectos como: a qué autoridad se debe presentar o en qué condiciones.

Por otra parte, el **artículo 10** establece los parámetros para la determinación de un riesgo alto, dentro de los que se destacan las normativas o políticas de gobiernos extranjeros sobre suministradores de hardware y software, la ubicación de la sede de estos en países no adheridos a la Convención de Budapest y el no cumplimiento de los estándares de ciberseguridad dispuestos en el artículo 6. Sin embargo, no todos los parámetros cuentan con el mismo nivel de facilidad de comprobación por parte de los operadores y proveedores de servicios de telecomunicaciones.

6. ¿Exige el uso de algún estándar, modelo, plataforma o tecnología en particular, o de algún *producto o servicio protegido por derechos de propiedad intelectual o que resulte costoso?*

La propuesta de reglamento en su **artículo 6** establece estándares de seguridad que deberán ser cumplidos por todos los agentes sujetos al ámbito de aplicación de la normativa, así como la aplicación de auditorías (**inciso f), artículo 8**) derivadas de estos y si bien como se señaló en el punto 3 de esta subsección, son de aplicación general y no parecen tener el potencial de generar ventajas discriminatorias, lo cierto es que pueden elevar los costos para operar los servicios de telecomunicaciones bajo la tecnología 5G.

Así las cosas, con base en el análisis de los parámetros anteriores es posible concluir que la propuesta de reglamento analizado tiene el potencial de elevar los costos de todos operadores o proveedores basados en la tecnología 5G, producto de la aplicación de estándares establecidos en la normativa, así como de eventuales sustituciones de equipos, productos y servicios.

d. Reduce incentivos para competir vigorosamente

1. *¿Genera un régimen de autorregulación o co-regulación?*

La propuesta de reglamento **no** establece o fomenta un régimen de autorregulación o co-regulación por parte de los operadores de redes y/o proveedores. Así que no se observa afectación a nivel de competencia existente en el mercado.

2. *¿Exige o fomenta la publicación de información sobre volúmenes de producción, precios, ventas o los costos de los agentes económicos?*

La propuesta de reglamento **no** promueve un esquema que implique intercambios o publicidad de cierto tipo de información entre agentes económicos competidores entre sí, tales como, precios, costos de producción, volúmenes de producción, mercados atendidos o estrategias comerciales.

3. *¿Exime un sector, actividad o agentes económicos de la aplicación de las leyes de competencia?*

La propuesta de reglamento que se analiza **no** contempla ni incentivos, ni exenciones en favor de operadores de redes y/o proveedores de los servicios de telecomunicaciones, de la aplicación de la normativa de competencia vigente; de manera que no genera beneficios en favor de alguna empresa o actividad en particular.

4. *¿Promueve o permite acuerdos anticompetitivos?*

La propuesta de reglamento que se analiza **no** promueve o facilita la creación de acuerdos anticompetitivos entre de operadores de redes y/o proveedores de los servicios de telecomunicaciones.

5. *¿Genera incertidumbre regulatoria, permite la aplicación discrecional de las regulaciones?*

En el **artículo 7** de la propuesta de reglamento se señala que los sujetos comprendidos en el ámbito de aplicación de la norma deberán analizar los riesgos de seguridad de diferentes elementos de sus redes detectando vulnerabilidades y amenazas, los resultados de estos análisis deberán ser presentados por cada una de las actividades establecidas en el artículo 2; sin embargo, dentro de la normativa no se establece el procedimiento a seguir para la presentación de la información obtenida por medio de los análisis, es decir, no resulta claro aspectos referentes a la rendición tales como: a quién, cada cuánto y como se debe entregar.

Esa misma situación se replica en el **artículo 9**, en relación al análisis de riesgo, prácticas y medidas de seguridad requeridas a los suministradores de hardware y software, dado que el artículo 9 indica que esa información deberá presentarse atendiendo las particularidades de los procesos dispuestos por el Poder Ejecutivo y la Sutel para la habilitación de redes y servicios basados en la tecnología de quinta generación móvil (5G) de acuerdo con su ámbito de competencia, esto sin llegar a especificar los procesos a seguir para llevar a cabo dicha entrega.

El **artículo 8**, plantea incertidumbre regulatoria al señalar en el inciso f) el sometimiento a auditorías en ciberseguridad (asumiendo el costo el auditado) por parte de los sujetos comprendidos en el ámbito de aplicación de la norma, esto sin definir un procedimiento dejando con ello en el limbo aspectos como: a qué autoridad se debe presentar o bajo qué condiciones.

Por otra parte, el **artículo 10** establece los parámetros para la determinación de un riesgo alto, dentro de los que se destacan las normativas o políticas de gobiernos extranjeros sobre suministradores de hardware y software, la ubicación de la sede de estos en países no adheridos a la Convención de Budapest y el no cumplimiento de los estándares de ciberseguridad dispuestos en el artículo 6. Sin embargo, no todos los parámetros cuentan con el mismo nivel de facilidad de comprobación por parte de los operadores y proveedores de servicios de telecomunicaciones.

Aunado a lo anterior existe ambigüedad sobre la forma en que se pueden valorar las disposiciones extranjeras y sobre quién es el encargado de hacerlo, por ejemplo, no se determina si existirá un listado emitido y actualizado, y quién sería el responsable de emitir dicho listado.

Además, el inciso e) del artículo 10 es incierto en cómo se debe catalogar la participación de suministradores con múltiples sedes, tanto en países adheridos al Convenio de Budapest como los que no. Por ejemplo, no se define si una filial domiciliada en Costa Rica es el suministrador de un operador, pero otra sede de la que es organizativamente dependiente está ubicada en un país que no forma parte de dicho convenio, esta situación se debe considerar de riesgo alto o no.

De esta forma, es posible concluir que la propuesta de reglamento analizado tiene el potencial de propiciar la reducción de los incentivos de las empresas para competir, al no establecer criterios claros y libres de ambigüedades conducentes a la presentación de los resultados de los análisis de riesgos y la clasificación de estos como altos, además de no detallar el procedimiento y cualquier otro elemento con el fin de ordenar la ejecución de auditorías de ciberseguridad con cargo al auditado.

e. Limita las opciones e información disponible para los consumidores

1. *¿Limita la información disponible y la posibilidad de los consumidores de elegir a quién compran los servicios de telecomunicaciones?*

La propuesta de reglamento **no** limita la capacidad de los consumidores para elegir entre los operadores de redes y/o proveedores de servicios de telecomunicaciones en el territorio nacional.

2. *¿Incrementa los costos explícitos o implícitos de cambiar de proveedor, reduciendo la posible movilidad de los clientes?*

La propuesta de reglamento **no** limita la capacidad de los consumidores para cambiar de operador de red y/o proveedor de servicios de telecomunicaciones en el territorio nacional.

En resumen, es posible concluir que la propuesta de reglamento no limita la información disponible para que los consumidores elijan a sus operadores de redes y/o proveedores de servicios, ni tampoco incrementa los costos para cambiar entre estos.

B. SEGUNDA FASE DE ANÁLISIS: ¿SE JUSTIFICAN LAS RESTRICCIONES?

En esta sección se analiza si las restricciones están justificadas. Esta necesidad de justificar y valorar las restricciones contenidas en las regulaciones no solo se deriva de los principios de competencia y de la búsqueda de la eficiencia en el mercado y el bienestar del consumidor, sino que también está alineada con el principio de razonabilidad y proporcionalidad, que es de resorte constitucional. Al respecto, la Sala Constitucional de la Corte Suprema de Justicia ha señalado que todo acto limitativo de derechos, para ser válido, debe ser razonable, necesario, idóneo y proporcional (Sala Constitucional, 1998).

La Segunda Etapa del análisis consta de dos pasos:

a) Identificar los objetivos de la regulación y de las restricciones a la competencia que contiene.

b) Analizar una a una las restricciones identificadas para determinar si son razonables y proporcionales.

El objetivo del *"Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G)"* es *"[…] establecer medidas de ciberseguridad para garantizar el uso y la explotación, segura y con resguardo de la privacidad de las personas, de las redes y los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G)".*

En ese sentido es claro que el objetivo es válido y pretende desarrollar un instrumento para complementar el marco regulatorio sectorial de telecomunicaciones en Costa Rica, en materia de ciberseguridad orientado de forma específica a redes de tecnología 5G dada la alta relevancia que conlleva el desarrollo de esta tecnología en el quehacer económico y social del país. En cuanto al análisis de la razonabilidad y proporcionalidad de las restricciones identificadas se procede a continuación a realizar una valoración de cada una de ellas:

06900-SUTEL-CS-2023

17 de agosto de 2023

Criterio	Artículo 6	Artículo 7	Artículo 8	Artículo 9	Artículo 10	Artículo 11
¿Es necesaria?: Debe existir una relación causal entre el fin de interés público que persigue la regulación y el medio elegido para alcanzarlo.	Sí. Enlista los estándares en ciberseguridad que el Poder Ejecutivo considera que se deben seguir en materia de redes 5G	Sí. Caracteriza los elementos que componen el análisis de riesgo solicitado.	Sí. Incluye las acciones que solicita adoptar para la gestión de riesgos identificados.	Sí. Al ser los suministradore s el eslabón inicial de la cadena de suministros de productos y servicios de los operadores y proveedores de servicios, estos se incluyen en la propuesta.	Sí. Parametriza las consideracio n es para catalogar un "riesgo alto", concepto que se utiliza para la toma de decisiones dentro de la propuesta.	Sí. Define las medidas aplicables ante la identificación de un riesgo catalogado como alto.
¿Es proporcional?: El costo de las restricciones contenidas en la regulación no supera el beneficio que con ella se pretende para la colectividad.	Sí. Los estándares mencionados abarcan temas relacionados con el objetivo de la propuesta y son de aplicació n general.	Sí. El análisis de riesgos de los propios operadores y proveedores de servicios sobre sus propias redes es una medida adecuada en el contexto de la propuesta.	No, dado que no es posible determinarlo en tanto el sometimiento a auditorías en ciberseguridad es un punto no suficientement e desarrollado como para valorar la proporcionalid ad.	Sí. El análisis de riesgos de los propios operadores y proveedores de servicios sobre los suministradore s es una medida adecuada en el contexto de la propuesta.	Sí. Se alinea con el objetivo de la propuesta.	Sí. Pese a contener medidas como no uso de elementos, sustitución de equipos y software y decretar el contar con parámetros de riesgo alto como un uso incorrecto del espectro, se alinea con el objetivo de la propuesta.
¿Es eficaz?: La norma o regulación debe ser capaz de alcanzar los objetivos o efectos deseados, actuando directamente sobre las causas del problema que busca solucionar,	Sí. La inclusión de estos estándares se enfoca en la gestión de las medidas de seguridad que se buscan en el objetivo de la propuesta.	Sí. Al incluir una disposición tendiente a la ejecución de análisis de riesgos sobre las redes 5G y desarrollar los elementos	Sí, al imponer medidas específicas para la gestión del riesgo en redes 5G.	Sí. Al incluir una disposición tendiente a la ejecución de análisis de riesgos sobre los suministradore s.	No. Pues no es clara sobre como valorar la definición que se hace del concepto "presión de gobiernos extranjeros" o como aplicar el	Sí, está alineada con el objetivo de la norma al establecer medidas correctivas ante la identificación de riesgos altos.

para promover los cambios de comportamiento necesarios para resolverlos.		y factores a tomar en cuenta.			criterio de locación de la sede de los suministradores.	
¿Es transparente?: Debe existir transparencia y claridad en el proceso de adopción de las normas, regulaciones y demás actos administrativos, así como en su redacción	Sí es transparente al contener un listado claro con el indicativo de la norma y el título, dejando indudable la	Sí, es clara en los elementos que demanda evaluar.	No. Demanda el sometimiento a auditorías en ciberseguridad especificando únicamente que el costo debe ser	No, dado que no llega a especificar los procesos a seguir para llevar a cabo la entrega de los resultados de los análisis y	No, dado que no es clara en el proceso de comprobación de los incisos c), d) y e) del artículo.	Sí, es clara en su intención.
Criterio	**Artículo 6**	**Artículo 7**	**Artículo 8**	**Artículo 9**	**Artículo 10**	**Artículo 11**
final y en la forma en que se implementa y ejecuta.	temática del estándar.		cubierto por el auditado, dejando abierto el rol de auditor y no especificando qué condición detona la ejecución de esta auditoría, en qué plazo o mediante que procedimiento.	gestión del riesgo en la cadena de suministro.		
¿Es predecible?: La regulación debe ofrecer a los agentes económicos un marco estable y sólido, que genere seguridad jurídica.	Sí, al establecer estándares específicos no crea dudas sobre cuáles deben aplicarse.	No. No existe claridad en específico sobre el procedimiento a seguir para la presentación de los resultados de los análisis.	No. Existe ambigüedad en la ejecución de auditorías externas en ciberseguridad.	No, por cuanto no es expresa en cuanto a los elementos y factores a evaluar.	No. No es expresa en cuanto a los criterios de localidad de la sede de los suministradores o de valoración de la "presión" de	No. En particular no desarrolla el "uso incorrecto del espectro" en relación con el Título V Régimen Sancionatorio de la Ley General de Telecomunicaciones.

					gobiernos extranjeros.	
¿Es indispensable?: Entre las distintas alternativas disponibles para alcanzar un objetivo, debe elegirse aquella que implique el menor impacto posible a la competencia en el mercado.	Sí. Normalmente podría considerarse que es más conveniente definir parámetros y características antes que estándares particulares, sin embargo, al tratarse de una materia de tanta trascendencia como la seguridad de las comunicaciones en redes 5G, se considera que si es adecuado e indispensable presentar estándares concretos.	Sí, se encuentra fundamento en su inclusión y el objetivo de la propuesta.	Sí, al corresponder con las medidas preventivas para la gestión de riesgos.	Sí, porque los suministradore s forman parte de la cadena mediante la cual los operadores y proveedores de servicios se dotan de equipos y software para el ofrecimiento de sus servicios y por ende se debe velar por su seguridad.	Sí, porque busca establecer parámetros de clasificación .	Sí, al corresponder con las medidas correctivas ante la identificación de riesgos altos.

C. TERCERA ETAPA DE ANÁLISIS: ¿HAY ALTERNATIVAS MENOS RESTRICTIVAS PARA ALCANZAR EL MISMO FIN?

Es posible que algunas de las restricciones a la competencia contenidas en la regulación estén justificadas, pero sus objetivos pueden alcanzarse de forma distinta y menos restrictiva. De ahí que en los casos donde resulte conveniente es importante de valorar alternativas regulatorias que permitan alcanzar los objetivos que persigue la regulación, de forma tal que se elimine o se reduzca lo más posible su impacto negativo sobre la competencia en el mercado.

De esta forma, esta Tercera Etapa de análisis consiste en una aplicación del principio de "indispensabilidad" o de "mínima distorsión" sobre los artículos que se considera que se pueden formular de forma alternativa o incluso eliminarse.

A partir de la valoración realizada, para minimizar el impacto sobre la competencia del sector, se recomienda ajustar los artículos 7, 8, 9, 10 y 11 de la propuesta de reglamento de la siguiente forma:

- Artículo 7: Detallar dentro del mismo artículo sobre el procedimiento que se debe seguir para la presentación de los resultados del análisis de riesgos solicitados, con el fin de

aumentar la predictibilidad de los agentes que realizan este estudio. Siendo indispensable la determinación de procesos para la presentación de análisis de riesgo en vista que esta indefinición puede entorpecer el desarrollo de las actividades mencionadas en el artículo 2.

- Artículo 8: Desarrollar lo asociado al sometimiento a las auditorías de ciberseguridad, en cuanto al procedimiento y causales para demandar su ejecución, las potestades de las autoridades que pueden imponer esta medida y el mecanismo de selección, contratación y aprobación de las entidades auditoras.

- Artículo 9: Desarrollar este artículo de forma análoga al artículo 7, en particular que se detallen elementos a incluir en el análisis, así como los factores, jerarquizaciones y priorización en distintos parámetros relevantes.

- Artículo 10: Valorar la efectividad de la redacción actual en cuanto al uso de la locación de la "sede" como parámetro para detectar un riesgo alto. Así como establecer un mecanismo por medio del cual el Poder Ejecutivo determinará y comunicará al sector aquellos suministradores de hardware y software considerados susceptibles de sufrir presión por parte de gobiernos extranjeros, con la finalidad de que los operadores y proveedores de servicios puedan tener información previa y precisa para la toma de decisiones en materia de dotación de equipos y de software para sus plataformas de tecnología 5G.

- Artículo 11: Vincular la condición de "contar con parámetros de riesgo alto" con el Título V Régimen Sancionatorio de la Ley General de Telecomunicaciones en términos de lo que el reglamento describe como "uso incorrecto del espectro".

X. OTRAS CONSIDERACIONES

1. En el apartado de definiciones, punto k, en lo relativo al concepto de *"Permisionario 5G"*, se sugiere revisarlo en el entendido que una red no comercial, no habilita prestar servicios de telecomunicaciones (no existe la prestación de servicios de telecomunicaciones no comercial).

2. Se observa que el reglamento de manera general asigna funciones sin determinar de manera específica cuál entidad será la encargada de velar por su efectivo cumplimiento, con frases como *"Dicha información deberá de ser presentada de conformidad con cada una de las actividades comprendidas en el artículo 2 del presente reglamento, atendiendo a las particularidades especiales de cada procedimiento, sin perjuicio de las potestades de control y fiscalización superior por parte de las autoridades sectoriales en su ámbito de competencia"* (artículo 7), *"Dicha información deberá de ser presentada atendiendo a las particularidades de los procesos dispuestos por el Poder Ejecutivo y la Superintendencia de Telecomunicaciones para la habilitación de redes y servicios basados en la tecnología de quinta generación móvil (5G) de acuerdo con su ámbito de competencia; o de conformidad con las disposiciones establecidas por la*

Administración o entidad contratante en los procesos de contratación pública que tengan por objeto la habilitación del uso y la explotación del espectro radioeléctrico para redes y servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G)" (artículo 9), por lo que se hace necesario se precisen las entidades responsables, de conformidad con el ámbito de sus competencias.

3. En relación con el artículo *"13. Sanciones e infracciones",* debe considerarse que vía reglamentaria no es posible establecer un régimen sancionatorio, por cuanto amerita como base, que la sanción e infracción esté previamente tipificada en una norma de rango de ley. En consecuencia, de acuerdo con lo señalado, en caso de incumplimiento del reglamento en consulta, podría resultar inaplicable el régimen sancionatorio que dispone la Ley N°8642. Asimismo, se puede observar que el régimen sancionatorio de la citada ley, deviene del incumplimiento de los derechos de los usuarios finales de los servicios de telecomunicaciones, y no lo relativo a la ciberseguridad en las redes de telecomunicaciones y su debida implementación por parte de los operadores, tal y como se propone.

XI. CONCLUSIONES Y RECOMENDACIONES

1. Los artículos 21 de la Ley 9736 y 24 del Reglamento a esa misma ley, la SUTEL tiene la potestad de emitir de oficio o a solicitud, opiniones y recomendaciones en materia de competencia y libre concurrencia **sobre la promulgación**, modificación o derogación de leyes, **reglamentos**, acuerdos, circulares y demás actos y resoluciones administrativas, vigentes o **en proceso de adopción**.

2. La propuesta de reglamento pretende desarrollar un instrumento para complementar el marco regulatorio sectorial de telecomunicaciones en Costa Rica, en materia de ciberseguridad orientado de forma específica a redes de tecnología 5G dada la alta relevancia que conlleva el desarrollo de esta tecnología en el quehacer económico y social del país.

3. La SUTEL basándose en su *"Guía para la Evaluación de la Regulación desde la Perspectiva de la Competencia"*, realizó el análisis de la propuesta de *"Reglamento a la Ley para incentivar y promover la construcción de infraestructura de telecomunicaciones en Costa Rica, sobre los procedimientos y especificaciones técnicas de la infraestructura de telecomunicaciones"*.

4. De acuerdo con los principios evaluados se encuentra que:

- La normativa propuesta **tiene el potencial** de limitar la posibilidad de ciertos tipos de operadores o proveedores de telecomunicaciones para prestar sus servicios, al condicionar la asignación de concesiones para uso y explotación del espectro radioeléctrico para redes y servicios de telecomunicaciones 5G, así como establecer características específicas, no estrictamente de índole comercial, que deberán adoptar los operadores y proveedores de telecomunicaciones al dotarse de bienes y servicios requeridos en la implementación de sus redes 5G.

- La normativa propuesta **tiene el potencial** de elevar los costos de todos operadores o proveedores basados en la tecnología 5G, producto de la aplicación de estándares establecidos en la normativa, así como de eventuales sustituciones de equipos, productos y servicios.

- La normativa propuesta **tiene el potencial** de propiciar la reducción de los incentivos de las empresas para competir, al no establecer criterios claros y libres de ambigüedades conducentes a la presentación de los resultados de los análisis de riesgos y la clasificación de estos como altos, además de no detallar el procedimiento y cualquier otro elemento con el fin de ordenar la ejecución de auditorías de ciberseguridad con cargo al auditado.

- La normativa propuesta **no limita** la información disponible para que los consumidores elijan a sus operadores de redes y/o proveedores de servicios, ni tampoco incrementa los costos para cambiar entre estos.

5. El objetivo de la propuesta de reglamento es válido y pretende impulsar aspectos de ciberseguridad en las tecnologías basadas en 5G.

6. En cuanto al análisis de la razonabilidad y proporcionalidad de las restricciones encontradas, se determina que el artículo 6 cumple con los criterios evaluados y que, pese a que impone un conjunto de estándares con el potencial de generar costos adicionales sobre la actividad de los operadores de redes y proveedores de servicios en tecnología 5G, este se encuentra justificado en la relación costo beneficio de la norma. El artículo 7 no cumple con el criterio de predictibilidad; el artículo 8 no cumple con los criterios de proporcionalidad, transparencia y predictibilidad; el artículo 9 no cumple con el criterio de transparencia y predictibilidad; el artículo 10 no cumple con los criterios de eficacia, transparencia y predictibilidad y el artículo 11 no cumple con el criterio de predictibilidad.

7. A partir de los resultados de los anteriores parámetros se considera que la propuesta de reglamento **tiene el potencial de generar barreras a la competencia** entre los agentes del mercado, por lo cual se recomienda ajustar los artículos 7, 8, 9, 10 y 11 de la citada propuesta de la siguiente forma:

- Artículo 7: Detallar dentro del mismo artículo sobre el procedimiento que se debe seguir para la presentación de los resultados del análisis de riesgos solicitados con el fin de aumentar la predictibilidad de los agentes que realizan este estudio. Siendo indispensable la determinación de procesos para la presentación de análisis de riesgo en vista que esta indefinición puede entorpecer el desarrollo de las actividades mencionadas en el artículo 2.

- Artículo 8: Desarrollar lo asociado al sometimiento a las auditorías de ciberseguridad, en cuanto al procedimiento y causales para demandar su

ejecución, las potestades de las autoridades que pueden imponer esta medida y el mecanismo de selección, contratación y aprobación de las entidades auditoras.

- Artículo 9: Desarrollar este artículo de forma análoga al artículo 7, en particular que se detallen elementos a incluir en el análisis, así como los factores, jerarquizaciones y priorización en distintos parámetros relevantes.

- Artículo 10: Valorar la efectividad de la redacción actual en cuanto al uso de la locación de la "sede" como parámetro para detectar un riesgo alto. Así como establecer un mecanismo por medio del cual el Poder Ejecutivo determinará y comunicará al sector aquellos suministradores de hardware y software considerados susceptibles de sufrir presión por parte de gobiernos extranjeros, con la finalidad de que los operadores y proveedores de servicios puedan tener información previa y precisa para la toma de decisiones en materia de dotación de equipos y de software para sus plataformas de tecnología 5G.

- Artículo 11: Vincular la condición de "contar con parámetros de riesgo alto" con el Título V Régimen Sancionatorio de la Ley General de Telecomunicaciones en términos de lo que el reglamento describe como "uso incorrecto del espectro".

Atentamente,

SUPERINTENDENCIA DE TELECOMUNICACIONES

FEDERICO CHACON LOAIZA (FIRMA)

Firmado digitalmente por FEDERICO CHACON LOAIZA (FIRMA)
Fecha: 2023.08.18 14:34:05 -06'00'

Federico Chacón Loaiza
Presidente
Consejo de SUTEL

MMA
cc. Junta Directiva Aresep
FOR-SUTEL-CSC-UJU-CGL-00075-2023