Mario Raul Dominguez Rojas (GTD Larga Distancia S.A.)

Consulta 1: Atendidas las velocidades y coberturas expuestas en las tablas N°s 1 y 2, se le solicita opinar sobre este punto, en lo relativo a las bandas 700 MHz, AWS y 3.5 GHz.

"Respecto de los parámetros que permitan evaluar y comparar las distintas ofertas, considerando entre estos parámetros el cálculo de cobertura por etapas, se estima conveniente, en especial para las bandas más altas incluida la de 28GHz, que se adopte las recomendaciones de la UIT (Organismo de Naciones Unidas que reúne a más países que las NU y concurren Administraciones, Operadores, Fabricantes de Equipos y Universidades) y que nuestro país, Chile, es signatario.

En efecto, las Recomendaciones UIT-R son esenciales para asegurar el funcionamiento adecuado y espectralmente protegido eficientemente de los equipos de radiocomunicaciones, en un entorno donde todo el mundo está utilizando recursos del espectro.

Algunas naciones como EEUU, Japón y Corea del Sur están habilitando servicios 5G con versión pre-estándar, usando espectro en las bandas de 25 y 28 GHz, anticipándose a las recomendaciones y sugerencias de la reunión CMR 2019 de UIT. Sobre el particular, se estima oportuno que en nuestro país se consideren esas bandas de espectro para el despliegue inicial de futuros servicios 5G, según las recomendaciones de la UIT y de los adelantos alcanzados por los países más avanzados.

La UIT y 3GPP señalan que las distintas bandas de frecuencias estarían destinadas en 5G a usos y aplicaciones diversas en función de las características de propagación (cobertura) y de las capacidades (anchos de banda) disponibles en cada una de ellas. En este sentido, se plantea para las bandas de frecuencias que se indican a continuación, lo siguiente:

- Las bandas de 400 MHz y 900 MHz se utilizarían principalmente para IoT; es decir, con canalización de anchos de banda reducidos, con amplias coberturas y capacidad de penetración. Estas bandas se deberían asignar territorialmente teniendo esto en consideración.

- Las bandas medias entre 1,5 GHz y 6 GHz se destinarían a la conectividad de dispositivos móviles y portables con conectividad de amplios anchos de banda (altas velocidades de datos).

- Las ondas milimétricas (28 GHz y superiores) se utilizarían principalmente - pero no exclusivamente - para servicio fijo inalámbrico, dadas las características de muy reducida cobertura de las radio-bases que operan en estas frecuencias, con alta capacidad de datos (del orden de 10 Gbps o más) que estas dispondrían.

En consideración con lo señalado precedentemente, se estima no conveniente definir mediante regulaciones o normas locales las velocidades de bajada y de subida, sino dejarlo a las recomendaciones de la UIT y a los adelantos tecnológicos que se alcancen a nivel mundial.

Se considera más relevante e importante definir los objetivos nacionales de desarrollo digital en la asignación y uso del espectro radioeléctrico, para contar con acciones para incentivar la

participación de operadores de telecomunicaciones que provean servicios de excelencia. Lo dicho a fin de actualizar y adecuar el actual marco normativo que rige en el país, debido a que se cuenta mayormente con regulaciones del servicio de voz, cuyas normas no se condicen con los nuevos adelantos tecnológicos alcanzados a nivel mundial. Sobre el particular se cita entre otros lo siguiente:

Continua a continuación de nuestra respuesta 4”

Consulta 2: En consideración a la baja cobertura de bandas milimétricas, ¿qué criterio(s) considera adecuado(s) para evaluar los aspectos de velocidad y cobertura en la banda de 28 GHz?

"En relación con las materias que se indican en la pregunta, nuevamente sugerimos atenerse a las recomendaciones de la UIT, en especial con las conclusiones que se darán a conocer en el IMT 2020.

Los sistemas 5G en la banda de 28 GHz se utilizarán mayormente en entornos muy localizados y densos, motivo por el cual la cobertura de esta banda se deberá analizar inicialmente para determinadas áreas urbanas y según los avances que se vayan logrando a nivel internacional.

Entre los distintos factores a tener en consideración en la banda de 28 GHz, cabe señalar las particularidades derivadas de la propagación y las características diferentes que se presentan por la diferencia de longitud de onda entre distintas bandas de frecuencias, las que se indican a continuación:

Pérdidas de trayecto en espacio libre: La ley de transmisión de Friis afirma que la pérdida de trayecto en espacio libre crece con el cuadrado de la frecuencia. La longitud de onda menor de las señales de ondas milimétricas significa que pueden colocarse más antenas en la misma superficie y/o torre, lo que luego posibilita mayor ganancia de antena para la misma superficie física. Así, la propagación de las ondas milimétricas no está sujeta a mayor pérdida en el espacio libre cuando se utiliza en mismo trayecto para múltiples antenas.

Difracción: La pérdida por difracción aumenta en forma proporcional a la frecuencia y por lo tanto no será un mecanismo de propagación dominante para las frecuencias de ondas milimétricas.

Reflexión y dispersión: Los mecanismos de reflexión se caracterizan por la reflexión especular (por ejemplo, reflexiones de objetos como agua, muros, vehículos, suelos e incluso personas) y la reflexión difusa (la dispersión de la energía de la señal al encontrar un objeto). Por ende hay que tener cuidado en instalaciones en sectores donde se encuentra presente este tipo de elementos.

La penetración de materiales es la cantidad de energía capaz de ser transmitida a través de un objeto. Típicamente, la pérdida se incrementará a medida que aumenta la frecuencia y, por ello, puede ser posible algún grado de penetración en construcciones en la parte inferior de la banda de ondas.

Pérdidas por lluvia, nieve, neblina aumentan con la frecuencia y ocasionan un perjuicio en las comunicaciones en las bandas milimétricas de aproximadamente 6 dB en condiciones más adversas.

Consideramos que la adjudicación del espectro en las bandas milimétricas debería realizarse exclusivamente a nivel de zonas geográficas limitadas, es decir, las empresas interesadas deberían postular a determinadas zonas geográficas, más o menos densas (demográficamente), con una cantidad de radio-bases suficientes para cubrir la demanda en dichas áreas. Para que esto opere adecuadamente para dispositivos portables es imperativo que se habilite y regule por parte de la Autoridad el roaming obligatorio de los OMR, tal como se señala en el punto anterior.

Las velocidades que se deberían exigir en estas bandas de frecuencias deberían estar expresadas en función de las tecnologías de NR (Release 15 3GPP) que se apliquen; en particular, de las mayores eficiencias espectrales que se obtengan mediante el uso de Massive MIMO. Con esto se deberían definir las velocidades en términos de los anchos de banda de cada bloque asignado y de la eficiencia espectral en [bit/Hz] que le sea aplicable."

Consulta 3: Atendido que la cobertura de los proyectos técnicos se encuentra cautelada con la exigencia de un mínimo de velocidad de subida y de bajada, en cada banda, se le solicita opinar sobre este punto. "En general la cobertura de los proyectos técnicos depende de variados factores, entre los cuales se indican los siguientes:

- Densidad de población en el área geográfica a cubrir con estaciones bases.
- Concentración diaria de la población en una determinada área geográfica.
- Densidad de conexión.
- Conectividad eficiente para una gran cantidad de dispositivos.
- Demanda de servicios de acceso a Internet.

Respecto a los mecanismos de cálculo de cobertura de conformidad con lo señalado precedentemente es necesario que se adopten las recomendaciones de la UIT.

Para propiciar que las personas que viven en zonas rurales y/o de baja densidad poblacional y poseen bajos ingresos puedan acceder a los servicios de acceso a Internet y de telecomunicaciones de voz, datos e imágenes, se propone a la Subsecretaría de Telecomunicaciones que establezca el subsidio a la demanda.

En cuanto a las velocidades mínimas de subida y bajada señaladas en la Tabla 1, nos parece que los valores indicados no contemplarían las mayores eficiencias espectrales que se lograrían con las tecnologías de NR (Release 15 3GPP) que se aplicarán en 5G, ya que las velocidades señaladas no difieren significativamente de las correspondientes a 4G/LTE. Por otra parte, con las velocidades definidas para las distintas bandas de frecuencias, no se lograrían tampoco los incrementos de velocidad que se publicitan en diversos medios para redes 5G."

Consulta 4: ¿Qué aspecto(s) considera relevante(s) para ser tratado(s) en materia de ciberseguridad?

"La ciberseguridad tiene un amplio campo de aplicación que abarca muchas industrias y diversos sectores y el nivel de desarrollo o compromiso de cada país en esta materia, debiéndose considerar en nuestra opinión los tópicos siguientes:

¿ Legales.

¿ Técnicas.

¿ Organizativas.

¿ Creación de capacidad, y

¿ Cooperación.

La Agenda de Ciberseguridad Global de la UIT (GCA) proporciona la base y el marco general para la iniciativa.

La seguridad cibernética es una parte importante dada la gran interconexión de redes que a la fecha ya existe y que continuará aumentando, lo que contribuye a que las redes queden más expuestas y comprometidas.

Actualmente se propone a los Estados definir políticas que apoyen el acceso y la seguridad de la tecnología, definiendo inicialmente una estrategia nacional de ciberseguridad. Sobre esta materia, el Comité Técnico de Normalización CTN 320 de la Asociación Española de Normalización, UNE, y otros organismos de distintos países participarán en foros internacionales y europeos de normalización en los que se elaborarán nuevos estándares sobre ciberseguridad y protección de datos personales.

En consideración con lo anterior, se estima de toda conveniencia que la Subsecretaría de Telecomunicaciones proponga que la definición de política nacional sobre seguridad cibernética sea basada en la experiencia de la UIT y de otros países que se encuentran más avanzados en esta materia, como se señaló en el párrafo anterior.

Continua respuesta 1

- El marco regulatorio nacional debería adecuarse para adoptar el principio de neutralidad tecnológica del uso del espectro (reglamentaciones de ""generación neutral"") para la introducción de la tecnología 5G mediante la disponibilidad y mejoramiento de los actuales servicios, introducción de nuevas prestaciones y el uso de nuevas bandas de frecuencias. Además, dar a los OTT´s un idéntico tratamiento que a los operadores de telecomunicaciones, eliminando la discriminación que existe en el uso de las redes de telecomunicaciones.

- Establecer la obligatoriedad de Roaming Nacional de los OMR para incentivar la competencia, mejorar la utilización del espectro radioeléctrico y propiciar la participación sin discriminación de OMV.

- Revisar, adecuar y coordinar con el Ministerio de Obras Públicas, Ministerio de Bienes Nacionales y las Municipalidades, un procedimiento ágil, transparente y común para que los operadores de telecomunicaciones puedan instalar sus redes de fibra óptica de conformidad con lo dispuesto en la Ley General de Telecomunicaciones, para proveer banda ancha fija considerando que para 5G se requerirán una cantidad importante de más infraestructura de soporte de antenas.

- Revisar y modificar la denominada ley de torres, facilitando la compartición de infraestructura activa y pasiva.

- Propiciar la introducción de innovaciones mediante la flexibilización de las regulaciones que rigen actualmente las comunicaciones de voz, datos y videos.

- Mantener el uso de espectro en bandas 700 MHz, 800 MHz, 1.9 GHz y 2.5 GHz.

- Establecer prioridad de tramitación del proyecto de ley Creación de Mercado Secundario de Frecuencias.

- Para evitar judicializar en exceso, las eventuales discrepancias entre los numerosos actores que participarán, constituir un Panel de Expertos, y

- Para dar margen a no excluir por precio a personas de bajos ingresos y de áreas rurales, considerar un sistema de subsidio a la demanda."

Consulta 5:¿Qué condiciones específicas considera relevantes para la protección de IoT?

"Para la protección de IoT estimamos relevante en primer lugar que se incentive y facilite la incorporación de los adelantos tecnológicos alcanzados a nivel mundial, incluyendo entre éstos el estándar ISO/IEC 30141 que propicia el diseño y desarrollo de aplicaciones de IoT.

La Organización Internacional de Normalización (ISO) publicó el primer estándar que proporciona una arquitectura de referencia de IoT utilizada internacionalmente, optimizando diseños actualmente en uso y las mejores prácticas del sector. El estándar denominado ISO/IEC 30141 Internet de las Cosas (IoT) - Arquitectura de Referencia -, proporciona un marco común para los diseñadores y desarrolladores de aplicaciones de IoT, que permite desarrollar sistemas fiables, seguros, protegidos, respetuosos con la privacidad y capaces de afrontar interrupciones debidas a catástrofes naturales y en particular ciberataques.

Dados los distintos tipos de plataformas IoT que existen en el mercado, se estima de toda conveniencia contar con el pronunciamiento de Subtel en el sentido que la arquitectura de IoT estará sujeta al libre interés de los proveedores del servicio IoT, respetando las normas de convivencia, sin perjuicio de los acuerdos que podrán convenirse entre los proveedores y los usuarios.

Un aspecto importante para la protección de las comunicaciones de IoT es lo relativo a la seguridad de la información entregada por dispositivos, especialmente por la ausencia de sistemas de encriptación adecuados o por lo vulnerables que son actualmente estos sistemas."

Consulta 6: ¿Qué puntos considera importantes en materia de protección de datos personales, en relación con la tecnología 5G?

"La protección de datos personales se debiera atener a un marco legal de aplicación general, común y transparente para todos los sectores de la economía, descartándose el establecimiento de regulaciones para una determinada tecnología de telecomunicaciones.

Estimamos conveniente que las medidas de protección de datos personales no limiten la introducción y habilitación de interfaces abiertas que propician más innovación en las redes de tecnología 5G en vez de favorecer sistemas "cerrados" con el fin de proteger los datos personales de sus usuarios. En efecto, los operadores muestran su preferencia por redes abiertas debido a la mayor flexibilidad para ofrecer servicios, sus menores costos y adaptación a nuevas alternativas que origine el mercado y la tecnología.

Actualmente, se encuentra tramitándose en su primer trámite constitucional el proyecto de ley que regula la Protección de los Datos Personales y crea la Agencia de Protección de Datos Personales (Boletines Nos 11.144-07 y 11.092-07, refundidos). Se estima conveniente que el gobierno asigne prioridad en su tramitación.

Concordante con lo anterior, consideramos una buena referencia la ley implementada en la Unión Europea, en mayo del año 2018. Además, estimamos que en el proyecto de ley se debería incluir lo referente a: Acceso, Rectificación, Cancelación y Oposición, permitiendo robustecer los procesos de Seguridad de la Información y Ciberseguridad. Análogamente, para fortalecer la infraestructura crítica (data centers) se deberá regular lo relacionado con la protección de los datos personales.

Además de la encriptación de la información personal (datos personales) por parte de los equipos y dispositivos asociados a servicios del usuario, es importante que se garantice la seguridad de la comunicación extremo a extremo en la red de telecomunicación que transporta datos; esto es, que no haya alteración de la información como tampoco que los datos se "filtren" a otros destinos."

Consulta 7: ¿En qué sectores o actividades cree que los riesgos sobre la seguridad de la información pueden suponer un mayor freno para el proceso de transformación digital?

"El Consejo Europeo ha señalado en el mes de marzo pasado que es necesario actuar conjuntamente para la seguridad de las redes 5G, sugiriendo acciones para evaluar los riesgos de seguridad cibernética de redes 5G y reforzar las medidas de prevención.

Por su parte GSMA propone a los operadores de telecomunicaciones asumir que la seguridad de sus redes es primordial en esta fase de introducción de la tecnología 5G y para el futuro próximo.

En este contexto, nuestro país tiene la posibilidad de aprovechar las experiencias internacionales, de modo de no partir de cero, incorporando los resultados obtenidos en la ejecución de auditorías y pruebas que se realizan por empresas internacionales para detectar vulnerabilidades y riesgos que enfrentan las redes de última tecnología. Para ello es relevante

que se realice un seguimiento del acontecer en los distintos mercados de Norteamérica, Europa, Japón, China y otros.

La convergencia de los estándares más avanzados a la fecha como son: NIST (USA) y ENISA (UE) con ISO 27001, 27005, 27017, 27018, 27103, 27032, y otros, han sido parte de las acciones en el caso de que se puedan producir brechas de seguridad de la información importantes en las actividades industriales (firmware), de IoT e Infraestructura Crítica.

Por otra parte, se deberá tener presente que IoT, con la sensorización de estados asociada a múltiples actividades, contribuirá a mejorar las condiciones de seguridad y calidad de vida de las personas."

Consulta 8: ¿De qué manera debería implementarse la ciberseguridad a nivel de interfaz de radio e infraestructura de red?

"En la realidad de un mundo cada vez más conectado - en el que Internet, los servicios, dispositivos y tecnologías digitales emergentes se están integrando en las economías de todo el mundo - la ciberseguridad efectiva desempeña un rol esencial.

A medida que aumentan el uso y la dependencia respecto de las TIC, aumentan los riesgos. Para responder a los desafíos presentes y futuros en permanente evolución, se requiere en primer lugar ser conscientes del riesgo que se enfrenta y, consecuente con ello, se adopten las acciones en todos los ámbitos de la ciberseguridad, ya que potenciar sólo el ámbito técnico en desmedro de los otros cuatro: legal, organizativas, creación de capacidad y cooperación, no se lograría hacer frente en forma eficiente y segura a los riesgos.

El Gobierno en conjunto con las empresas, para garantizar un ámbito digital seguro, resistente y protegido -del que puedan beneficiarse todos los ciudadanos- debe promover e incentivar en este ámbito se actúe coordinadamente en todas las áreas: legales, técnicas, organizativas, creación de capacidad, y cooperación, así como la colaboración multisectorial e internacional.

Para lograr lo anterior, el Estado a través de la Subsecretaría de Telecomunicaciones debiera encabezar y dirigir en las distintas áreas las acciones conducentes teniendo presente las iniciativas que se llevan a cabo en Norteamérica, Europa, China, Japón y otros países.

Un proyecto de gobierno, próximo a enviarse al congreso para su trámite legislativo, contiene una Agencia de Ciberseguridad y los CSIRT (Equipos de respuesta a incidentes de seguridad informática) por sectores, donde el CSIRT de Telecomunicaciones debería ser el eje sobre el cual se articula la política de ciberseguridad, ya que son las redes de telecomunicaciones las que transportan y permiten a los agentes maliciosos, poner en riesgo no solo la seguridad de la información de las personas, sino la de la red de infraestructura crítica de un país; tales como hospitales, defensa, hacienda (bancos), energía y otras áreas. Consideramos importante que este organismo cuente con total autonomía técnica y política, de manera de evitar futuros detrimentos operativos y organizacionales, por no tener la independencia requerida para gestionar de manera autónoma y oportuna los eventuales ataques a la seguridad de la información y al ciberespacio nacional. Es evidente que el país está inserto en el mundo y este tema de la ciberseguridad es un tema nacional, pero en un contexto global. "