José Ignacio González Cejas (Claro)

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.

"En el marco de la realización de la consulta pública para el concurso 5G que está llevando a cabo la Subsecretaría de Telecomunicaciones, se presentan los siguientes comentarios por parte del grupo Claro:

Coincidimos con la autoridad en que el óptimo técnico y económico es que las concesiones propuestas deben ser nacionales en un modelo dividido en una fase técnica y una segunda económica con estricta sujeción a lo establecido en la Ley 18.168 de 1982 General de Telecomunicaciones. Por su parte cualquier proceso de concurso supone que se permita y vele por la participación de variados actores actuales y potenciales, resguardando la existencia de múltiples posibles participantes por cada banda evitando la existencia de un único posible participante o adjudicatario o la obligación de participar por "paquetes de espectro" por lo que a nuestro juicio los concursos deben ser divididos por bloques y banda.

Sin perjuicio de lo expuesto, se debe tener en consideración que las velocidades indicadas como exigencias mínimas en las tablas analizadas, solo podrán ser alcanzadas y mantenidas bajo ambientes óptimos.

Se sugiere explorar opciones para aumentar la cantidad de espectro disponible, siguiendo lo realizado en otros países como EE.UU., donde se han llevado a cabo acciones para disponibilizar espectro en la banda 600 MHz que permitiría asignar mayor capacidad espectral.

Para el caso de la banda 3.5 es utilizada como TDD., para ofrecer servicios 5G se sugiere buscar soluciones que apunten a bloques continuos que permitan a los adjudicatarios lograr anchos de banda idealmente de 100 MHz por operador.

Respecto a la banda 28 GHz, para pensar en 5G de alta demanda, baja latencia, alta disponibilidad, se debe pensar en disponer no menos de 400 MHz, por operador, en banda milimétrica para alcanzar los estándares que exigirá la creciente demanda de conectividad, posibilitando ser competitivos con otros mercados. Para lo anterior sugerimos incorporar la banda 26 GHz, logrando así una mayor disponibilidad de espectro en bandas milimétricas, permitiendo obtener mayores anchos de banda para los distintos operadores.

Respecto a los rangos de cobertura:

Parecieran ser adecuados los rangos de cobertura propuestos por comunas, siguiendo esquemas ya probados en procesos concursales anteriores, lo que redunda en esquemas de despliegue que han resultado exitosos en el tiempo. Sin embargo, debe tenerse presente que, a diferencia de concursos anteriores, al analizar la cobertura enlazada a parámetros de velocidad en condiciones outdoor, esta tiene directa incidencia en los valores base para el diseño la arquitectura de la red, entre otros parámetros que definen radios de cobertura.

Este punto igualmente debe someterse a revisión puesto que a medida que los proveedores pongan a disposición del mercado el equipamiento radiante se conocerá con un grado de

certeza mayor los alcances de los equipos y las velocidades que en determinado radio de cobertura se pueda lograr, hoy se habla de prototipos que dan ciertas luces al respecto pero deberá contrastarse lo anterior con el equipamiento que se tenga a disposición en el futuro.

De igual forma las coberturas y velocidades que se alcanzarán en los radios de cada estación base dependerán del ancho de banda adjudicado."

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?

"Las bandas milimétricas requieren tener un gran ancho de banda por la capacidad espectral que prometen. Técnicamente se espera que las bandas milimétricas sean utilizadas preferentemente en ambientes indoor y en pequeñas zonas de alta demanda (hotspots), y no como una solución de cobertura de tipo outdoor standard. Por lo tanto para evaluar las coberturas de esta banda, se debería considerar que el despliegue, en términos de tiempos, debería estar alineado con el crecimiento de la demanda y basado en coberturas tipo Hotspots, y no a cubrir comunas completas o grandes superficies en kilómetros cuadrados. Las velocidades a definir deberán estar alineadas con la porción de espectro a adjudicar por operador y limitadas al rango de cobertura de cada hotspot.

En este sentido, y en consideración a que dicha banda requiere la instalación de un múltiplo importante de antenas adicionales para lograr una mayor cobertura, se hace relevante una nueva normativa para el despliegue de infraestructura que genere facilidades de inversión y desarrollo. Por otra parte esto puede ser a su vez complementado con algoritmos de evaluación que comiencen la contabilización del o los puntajes a partir del segundo periodo o posteriores, a fin de otorgar un tiempo dedicado a la instalación de la infraestructura asociada sin castigo de puntaje.

De igual forma las zonas de cobertura pueden estar delimitadas a polígonos especiales como “zonas industriales” los cuales deben ser claramente definidos."

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.

"Se debe tener presente que la exigencia de cobertura y velocidad deberá ser acorde a los ancho de banda adjudicados a cada operador en condiciones outdoor.

Los mínimos de bajada y subida deben estar alineados con el límite que se requiere para la cobertura de una celda, el que determinará la condición de diseño. La distancia a la cual se cumple esta condición en espacio libre, determinará la cobertura esperada . Sin embargo, también se relaciona directamente con el ancho del canal asignado, es decir a mayor ancho mayor será la velocidad posible. Los valores indicados en la Tabla N° 2, deben además, indicar el ancho de canal asignable para que tengan sentido final.

Finalmente, sugerimos uniformar los criterios de velocidad mínima aplicables a todas las bandas en uno solo, evitando así que exista confusión por parte de los usuarios de los servicios respecto de los estándares de velocidad a exigir a sus proveedores."

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

"Considerar el creciente aumento en la utilización de dispositivos móviles conectados a internet, lo que necesariamente aumenta la preocupación por protegerlos de amenazas. Lo anterior, dado que al estar conectados a la red, son susceptibles de manejarse remotamente, lo que los deja expuestos a riesgos.

Ante la necesidad de los fabricantes de que los dispositivos IoT sean fáciles de configurar e instalar, se da prioridad a la usabilidad más que a la seguridad, por lo mismo es que la Ciberseguridad debe anteponerse a esta realidad y abordar de la mejor forma posible la detección tempranamente de amenazas para poder mitigar eficientemente el riego.

La seguridad de Internet de las Cosas (IoT) debe combinar las capacidades de la compañía en los campos de la Ciberseguridad e IoT, velándose también por la implementación de plataformas que contengan un firewall de excelencia, el cual deberá ser sometido a continua actualización de manera de impedir que la información de los dispositivos inteligentes pueda ser vulnerada.

Es por lo expuesto que resulta recomendable que a nivel de gobierno se defina un estándar técnico en materia de ciberseguridad, en que se contemplen las diversas exigencias en materia de plataformas de equipos interconectados, configuración de las redes y estándares en software de protección de amenazas."

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

"Es primordial, analizar el tráfico IoT en las redes para detectar tempranamente las amenazas y poder actuar de manera eficiente y eficaz.

Para el análisis eficiente del tráfico, será necesario utilizar algoritmos de machine learning, que permitan generar las alertas necesarias en caso de identificar una amenaza que ponga en riesgo la Ciberseguridad de los dispositivos IoT móviles.

Debe hacerse presente que dichas medidas deberán aplicarse tanto a los dispositivos inteligentes como a las app y/o plataforma que los controla.

Dado lo anterior, en la actualidad, cualquier solución de Ciberseguridad orientada a IoT, debe considerar como materia central, las redes y su tráfico. Esto es primordial, dado que las capacidades de la mayoría de los dispositivos IoT son limitadas, lo que no permiten la instalación de software sofisticados para su protección.

Importante es la administración segura de credenciales para los dispositivos IoT y la securitización a nivel de DNS.

Otro tema importante es el cifrado de las comunicaciones y las actualizaciones de seguridad tanto de software como de firmware de los IoT.

Si se trata de dispositivos IoT de empresas y/o corporaciones, además de las medidas tecnológicas a nivel de los proveedores de servicios de comunicaciones, es importante que esto esté apalancado, en cada organización, con políticas de seguridad y/o Ciberseguridad dentro de un plan de Ciberseguridad de la compañía, incentivando a que se adopten buenas prácticas como:

- Adquisición de dispositivos que cuentes con actualizaciones de seguridad.
- Establecimiento de canales de comunicación cifrado.
- Cambio de contraseñas por defecto.
- Configuración de acceso sólo a personal autorizado, entre otras."

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

"En primer lugar, el desarrollo e implementación de la tecnología 5G permitirá no solo la transmisión sino que la recolección de una enorme cantidad de información, sean datos personales o no, asociado a los distintos usos que se le pueda dar a dicha tecnología, así tenemos datos de movilidad de las personas, de hábitos de consumo, de salud etc.

Debido a que se espera que una enorme cantidad de dispositivos estén conectados permanentemente entre sí, transfiriendo una gran cantidad de datos, es necesario establecer el marco regulatorio para el nuevo ecosistema, partiendo de la base de la licitud del tratamiento de los datos, es decir, se debe partir de la base que la recolección, almacenamiento, tratamiento y transferencia de datos, como norma general, es lícito si se cumplen las condiciones que establezca la ley, esto es fundamental para el desarrollo de la economía del siglo XXI que tendrá como uno de sus pilares fundamentales el procesamiento de enormes cantidades de información.

Junto con lo anterior se debe fijar un marco razonable para el tratamiento de los datos personales así como para datos sensibles, como son aquellos relacionados con la salud de las personas. Así, se hace necesaria una actualización de la normativa vigente, en especial de la ley N°19.628, para adecuar nuestras normas a los estándares internacionales actuales.

Esta actualización debe considerar el régimen de responsabilidad para el tratamiento de tales datos, lo cual es fundamental toda vez que gracias a las nuevas tecnologías en un mismo hecho pueden tener algún grado de participación una diversidad de actores, por ejemplo:

- Titular de los datos personales.
- ¿ Empresa de aplicación, software que recoge datos personales.
- ¿ Empresa que almacena datos personales.
- ¿ Empresa de data análisis.

¿ Empresa de telecomunicaciones."

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?

"En los sectores de la minería, banca y de procesos industriales complejos en que parte importante de la producción esta sistematizado e interconectado, produciéndose el riesgo que en caso de una falla o hackeo dichos sistemas queden inservibles, parando la producción por un tiempo bastante importante.

También existe un riesgo en los sectores de prestación de servicios básicos (agua, tratamiento de aguas, gas y eléctrico), que puedan detener su distribución o poner en peligro a la población."

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

“La comunicación en interface de aire (radioeléctrica) en general posee niveles de encriptación robustos y, cada proveedor de tecnología realiza su diseño y oferta con distintos niveles y tipos de encriptación. A nivel de transporte se debe analizar con sistemas. Sin perjuicio de lo expuesto, consideraos que a nivel de ciberseguridad no debiera imponerse restricciones a nivel tecnológico, sino más bien a nivel de cumplimiento dentro de los aspectos normativos que resguardan la confidencialidad, disponibilidad e integridad de la información.”