Stefano Villanueva Bianchini (Nokia)

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.

"Las velocidades dependen del ancho de banda que el operador licencie. Si licencian, por ejemplo, solamente 5MHz la velocidad máxima será menor a lo especificado.

Tenemos nuestras dudas respecto de definir este parámetro. No obstante ello, entendemos lo siguiente:

- 700MHz: se necesita un ancho de banda mínimo de 10MHz para alcanzar la velocidad propuesta.

- AWS: se requiere un ancho de banda de 15MHz para alcanzar la velocidad propuesta.

- 3.5GHz: En este caso se especifica el ancho de banda y está bien dimensionado. Sin embargo, no tiene sentido asignar menos de 50 MHz continuos pues sería un bloque menor al que los operadores cuentan hoy para 4G, por lo que recomendamos como mínimo 80 MHz a 100 MHz. Es muy importante que se hagan los esfuerzos necesarios para identificar la cantidad necesaria de espectro que permita a cada operador tener entre 80 y 100 MHz continuos.

Aprovechamos en este apartado para hacer algunos comentarios sobre la Situación de la banda de frecuencia de 3.4-3.65 GHz a que se hace referencia en el documento de consulta.

Nokia sugiere una ampliación de la banda abarcando desde 3.3 GHz hasta 3.8 GHz para los servicios de 5G. De esta forma se estarían identificando 500 MHz para servicios móviles que permitirían asignar bloques más grandes acordes a los máximos permitidos por la norma 3GPP (100 MHz). De esta forma, Chile podría contar con una red 5G de alta velocidad y no restringida por el espectro asignado. Esta decisión es muy importante y recomendamos comenzar a la brevedad con la limpieza del espectro que aún no está identificado, de forma tal de ponerlo a disposición de 5G. Para un buen uso, los operadores necesitan espectro continuo en TDD y la recomendación sería que tengan 80 MHz como mínimo hasta 100 MHz.

Respecto de la cobertura especificada, es muy difícil opinar dado que resulta muy subjetivo."

Consulta 1: 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?

"Respecto de la banda de 28 GHz, consideramos que es una muy buena oportunidad para sumar la banda de 26 GHz con la de 28 GHz, lo que daría algo más de 3000 MHz para la 5G en las bandas milimétricas posibilitando muy buenos servicios de 5G. En este último caso se podrían dar segmentos de 800 MHz. Asimismo, sugerimos analizar la posibilidad de incluir también la banda de 38 a 40 GHz.

Dicho esto, es importante tener presente que los criterios fundamentales de esta banda están relacionados con las altas velocidades, el troughput, y dependiendo de la aplicación, la mínima

latencia. Si a 28 GHz se le suma 26 GHz, esta mayor disponibilidad de frecuencia nos permitiría ir a segmentos de 800 MHz o más.

En cuanto a cobertura, esta banda no es para despliegues de gran cobertura, sino para áreas densamente urbanas y alto volumen de tráfico, así como para uso industrial en el sentido amplio de la palabra. Desde este punto de vista, 28GHz se utilizará para Hot Spots, por lo que la cobertura debe ser ad-hoc para rellenar gaps, u ofrecer servicios FWA a corta distancia (~200m) o usos industriales."

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.

“Ya nos hemos pronunciado sobre este tema en la pregunta 1.”

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

"Es fundamental la existencia de una política a nivel nacional de seguridad cibernética, así como una estrategia de ciberdefensa que permita proteger, identificar y mitigar amenazas sobre la infraestructura de telecomunicaciones propuesta.

Asimismo, se recomienda que los concesionarios dispongan de un centro de seguridad cibernética, que incluya soluciones completas de gestión de operaciones de ciberseguridad, cifrado, prevención y detección de intrusiones, trafico malicioso y malware, TMS, respuesta a incidentes (CSIRT), de manera que se tenga completa visibilidad y capacidad de reacción ante eventos de ciberseguridad etc.

La protección de datos se vuelve sumamente importante para 5G, ya que la industria crítica como Financiera, Salud, Milicia, tendrán acceso y se conectarán a través de estas redes. Un estudio sobre posible espionaje o fuga de información de interés nacional es importante."

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

"Desde el punto de vista de gestión de operaciones de seguridad es importante considerar los vectores de ataque sobre las plataformas de IoT que buscan alterar el flujo usual de datos o afectar el servicio como tal, y que no se pueden mitigar en los dispositivos por sus limitaciones en hardware y/o software de forma inherente, de manera que las recomendaciones en seguridad se dan desde la perspectiva de red, donde se pueden monitorear y detectar amenazas basadas en patrones y comportamiento.

Por otra parte, cada potencial uso de IoT debe adherirse a estándares y recomendaciones internacionales. Por ejemplo, en el sector eléctrico los estándares de seguridad de NERC-CIP para el sistema eléctrico norteamericano es una referencia muy completa que incluye protección a la seguridad, gestión de seguridad, manejo de incidentes, etc."

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

"Para que la tecnología de la 5G pueda suministrar lo prometido, es necesario y crítico, por un lado, la existencia de reglas equilibradas de neutralidad de la red que permitan una ""calidad de servicio"" diferenciada. Al tiempo que se preservan los principios de la Internet abierta, es importante diferenciar el tráfico de red, ya que los usuarios requieren velocidades, anchos de banda y latencias diferentes que se ajustan a sus usos específicos ('segmentos de red o network slicing'). Asimismo, el libre flujo de datos transfronterizos es esencial para incentivar y escalar los servicios basados en la nube.

Con respecto a la protección de datos y la seguridad, se debe encontrar un equilibrio delicado para proteger de manera efectiva a los usuarios finales mientras se habilitan nuevos servicios digitales.

La confianza es un elemento esencial en la economía digital, y que se traduce en la confianza en la integridad, fortaleza y seguridad de las tecnologías. La confianza se va sustentando en (1) el conocimiento que tiene el usuario sobre la privacidad en línea, (2) el diseño de la tecnología, (3) las prácticas de los proveedores, y (4) las instituciones que gobiernan el sistema. Cada uno de estos componentes debe ser trabajado para lograr ese equilibrio entre la protección de datos y la seguridad que habiliten nuevos servicios digitales."

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?

“Prácticamente en todos los sectores, estos es sector eléctrico, minería, transporte, banca, seguridad pública y defensa, ciudades inteligentes, etc. Todo aquel sector considerado clave para el desarrollo nacional de Chile, cae en este listado. 5G promete conectar todo a largo plazo, por lo que sin seguridad, Chile puede quedar desprotegido a ataques nacionales e internacionales.”

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

"Los gobiernos interesados en la ciberseguridad de las redes de 5G y su mejora, deben llevar adelante las siguientes acciones:

• Fomentar el uso y la configuración adecuada de las funciones de seguridad especificadas por el 3GPP. La arquitectura de seguridad 3GPP exige el uso de muchos mecanismos de seguridad especificados por el IETF, la UIT-T y el ETSI, entre otros, incluyendo los métodos de cifrado recomendados para la interface de radio, así como el cifrado de datos de usuarios desde las radio bases, la red de transporte y hacia los datacenter de forma que la privacidad y la integridad de la información no se vea comprometida hasta Internet.

• Fomentar la implementación de soluciones adicionales disponibles en el mercado que mejoren la seguridad de las redes:

¿ - Seguridad continua y monitoreo de las configuraciones de seguridad / políticas de seguridad,

¿ - Un sistema de múltiples proveedores que proporciona un inicio de sesión único con administración de identidades privilegiada, análisis de comportamiento del usuario y capacidades de registro de cumplimiento,

¿ - Orquestación y administración de seguridad holística automatizada combinada con controles de seguridad inteligentes y automatizados.

- Cumplir con los esquemas de garantía técnica que evalúan el ciclo de vida de la seguridad en una organización determinada. Se recomienda usar GSMA NESAS para ese propósito.”