

Tiago Machado Brocardo (Ericsson)

**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.

"Cada banda tiene propiedades físicas diferentes, por lo que hay un balance y compensaciones entre capacidad, cobertura y latencia, así como confiabilidad y eficiencia espectral. Si la red está optimizada para una métrica, puede haber una degradación de la otra.

El espectro de banda baja se ha utilizado históricamente para redes 2G, 3G y 4G para servicios de voz y banda ancha móvil, así como para televisión abierta, con anchos de banda disponible típicamente de 10-30 MHz. Esto hace que este espectro sea más adecuado para cobertura de área amplia desde estaciones de tipo radio base macro.

El espectro en banda media se usa actualmente para los servicios 2G, 3G y 4G, y se ha añadido una nueva banda en en 3,5 GHz, donde es probable que veamos anchos de banda más grandes (50–100 MHz), lo que permitirá alta capacidad y baja latencia que se pueden usar para nuevos casos de uso como servicios de internet fijo inalámbrico, por lo que tienen un balance óptimo entre cobertura, calidad, velocidad de transmisión, capacidad y latencia, con buena penetración indoor.

Capacidad:

La capacidad de un sitio depende de del producto de la cantidad de espectro en uso y la eficiencia espectral. La eficiencia espectral es el resultado de una combinación de factores que incluyen la relación señal-ruido de cada terminal conectado, las modulaciones utilizadas, las aplicaciones y la naturaleza del tráfico de datos (continuos, esporádicos o en burst, por ejemplo), y otras variables.

Además, cada aplicación que se establecerá sobre las redes 5G del futuro tendrá un requisito de tráfico distinto: sea 10-100Mbps para banda fija, o 1-10Mbps para video en banda ancha móvil o aún menos de 1Mbps para aplicaciones IoT masivas.

Cobertura

La cobertura de redes móviles depende de una cantidad de factores. Evidentemente, como se ha destacado anteriormente, cuanto más alta la frecuencia, más corto es el alcance. Pero en una misma frecuencia, otros factores impactan fuertemente la cobertura, como la altura de instalación, tipo y ganancia de la antena, potencia de transmisión y antena del terminal, figura de ruido (noise figure) del receptor en la radio base, , velocidad de los terminales para aplicaciones móviles, pérdidas de penetración en edificios, clasificación del clutter (rural, suburbano, urbano, urbano denso y otros) y hasta la temperatura y humedad del aire. Con todas esas variables, se definen los parámetros usados en los modelos de propagación como COST 321, Okumura-Hata y otros.

Por eso, no se deben establecer rangos mínimos de cobertura para cada radio base. Un equipo instalado en un poste tendrá un área urbano tendrá una área de cobertura quizá 10x menor que un equipo de alta capacidad en una torre de 50m de altura en un ambiente rural, con la

misma frecuencia. Lógicamente, el equipo en el ambiente urbano tendrá costos quizá más bajos, que permitan que se instalen más sitios para cubrir una zona de la ciudad.

Por los motivos expuestos, se propone que las obligaciones se organicen en tres dimensiones:

1. Inversiones realizadas en expansión y despliegue de nuevas redes
2. Expansión de servicios y prestación de nuevos servicios – incluyendo IoT, internet fijo inalámbrico y otros casos de uso
3. Calidad de servicio (QoS) – latencia, disponibilidad, velocidades, cobertura, cantidad de dispositivos son algunos de los requisitos de los nuevos servicios sobre redes 5G

<https://www.ericsson.com/assets/local/networks/documents/5g-deployment-considerations.pdf>"

**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 decisiones que enfrentan los reguladores en torno al espectro de 5G son complejas y tendrán un gran impacto en la calidad de los servicios y los casos de uso que se pueden desplegar. En relación a las bandas milimétricas, dada la naturaleza del espectro los servicios de 5G en estas bandas serán en aplicaciones específicas y de alta capacidad para tomar ventaja de la baja latencia y capacidad, como también para que los existentes operadores de servicio móvil en donde ayudarían a descongestionar las tecnologías ya existentes en zonas ya congestionadas. Por lo que estas bandas están orientados a áreas densamente urbanas o punto de acceso de alta capacidad (hotspot), cuyos lugares de cobertura se identifican de forma selectiva y de manera más determinística que estadística. Estos sitios pueden identificarse debido a la necesidad de descarga de capacidad de las redes existentes, debido a su importancia como áreas de alto tráfico, como estadios, centros comerciales o centros de transporte, además de ambientes indoor o con línea de vista a terminales fijos (Line of Sight), como en el caso de acceso fijo inalámbrico. Por eso, las bandas altas no son adecuadas para que se aplique obligaciones de cobertura, por lo que el enfoque desde el punto de vista regulatorio debe de ser en la calidad de servicio (QoS).

El espectro de banda alta proporciona el salto importante en las velocidades para 5G y nuevos servicios. Estas nuevas bandas de espectro están típicamente en el rango de 24-40 GHz, con anchos de banda en bloques de mínimo 100, hasta, 800MHz (o más). Sin embargo, estas frecuencias vienen con una limitación de cobertura en comparación con las bandas más bajas, por lo que altas tasas de velocidad de transmisión como también alta capacidad son el principal foco para el uso de estas bandas, pero no cobertura.

Las velocidades de las bandas milimétricas se determinarán por la cantidad de espectro a ser utilizado y otros factores técnicos de 5G como las asignaciones de la estructura TDD (DL, UL y período de guarda) y la numerología, que pueden variar según la aplicación y necesidades del servicio.

Otro aspecto importante son los anchos de banda. Cuando más alto el ancho, más alta es la eficiencia espectral, reduciéndose las pérdidas de eficiencia con bandas de guardia dentro de los canales. Además, anchos de banda de 800MHz o más permiten que se viabilicen las aplicaciones avanzadas del 5G, por lo que se recomienda que, para las bandas milimétricas como 28GHz, pero también 26GHz y 37-43GHz por ejemplo, se adopten anchos de banda de mínimo de 800MHz, idealmente 1000MHz o más por operador.

Para asegurar la disponibilidad de espectro suficiente para que cada operador tenga acceso a 800MHz, la alternativa es hacer disponible no solo la banda de 28GHz, pero también 26GHz, agregándose otros 3.25GHz de ancho de banda total (de 24.25GHz a 27.50GHz). Además, en la misma banda de 28GHz se puede utilizar el rango de 27.5 a 295.GHz, en un total de 2GHz. Hasta el momento, 17 países del mundo han están considerando de manera formal la banda de 28GHz, cubriendo una población de 2,5MM de personas, lo que garantizará el ecosistema de terminales necesario para economías de escala y una rápida adopción de la banda a nivel global."

**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. "De la misma manera que se ha expuesto anteriormente, se recomienda que la evaluación sea de los siguientes factores: (1) inversiones, (2) servicios y (3) calidad, y no de velocidad o cobertura totales.

Del punto de vista de estrategia a nivel de país para la introducción de una nueva tecnología, se debe evaluar el beneficio a la población y al país, que viene de la oferta de nuevos servicios con calidad, lo que será posible con inversiones en nuevas redes y expansión de las redes existentes. Medir la velocidad total de una estación radio base 5G en futuro no servirá para medir la calidad del servicio, su impacto en el aumento de la productividad de otros sectores y el avance de la digitalización del país."

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

"Hay tres consideraciones importantes en materia de ciberseguridad:

- Capacidades de seguridad (Security Capabilities): Las capacidades de hardware y de software sobre las cuales los proveedores de tecnología desarrollan y fabrican sus productos y soluciones, incluidos la integridad de la toda la cadena de suministro de dichos proveedores de tecnología
- Despliegues de red (Network Deployment): Además de la capacidad de seguridad de los proveedores productos, otros ingredientes importantes incluyen la seguridad de configuración, la aplicación de seguridad lógica y física adecuadas según cómo el producto o solución se utiliza, y conciencia de los riesgos inherentes en el entorno específico en el cual se implementa el hardware y el software.
- Operación de las redes (Network Operation): La seguridad operacional es significativa, ya que ambas, fallas humanas y organizativas, están presentes en causas comunes de incidentes de seguridad. "

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

"Hay tres aspectos centrales con respecto a la protección de IoT:

- Dispositivos IoT muchas veces no tienen interfaz humana. De esta manera, no hay interferencia del operador ni medida de seguridad que se pueda adoptar en su utilización.
- IoT es más que tecnología, son nuevos modelos de negocio, de operación y de transformación digital de todos los sectores. Por eso, la importancia de la ciberseguridad para una gran cantidad de aplicaciones de IoT que serán realidad a corto plazo es aún más alta, porque ya no serán solamente informaciones, sino también serán la operación de sistemas críticos, como salud, transportes y electricidad que podrán ser vulnerables sin las medidas adecuadas de seguridad.
- Multitud de tipos de terminales, de los más sencillos a los más complejos serán una realidad en las redes del futuro. Hoy, los smartphones, aunque sean de alta o de baja gama, son dispositivos parecidos, tienen la misma arquitectura y por lo tanto hay menos variaciones de modelos de uso de los recursos de red. En el futuro, tendremos desde máquinas complejas y robos industriales hasta sensores y otros elementos baratos y sencillos en las mismas redes. Así, el reto es garantizar la seguridad en toda la cadena tecnológica, para todo el amplio rango de tipos de terminales y aplicaciones."

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

"Con respecto al tema de protección de datos personales, se debe considerar:

- Protección de los derechos básicos de los ciudadanos y usuarios (User right protection): la protección de los derechos de los usuarios debe ser una de las bases para cualquier política pública de protección de datos y privacidad.
- Innovación inducida por datos (Data driven innovation): Un nuevo proceso de 'datafication' está emergiendo en todo el mundo. En contraste con la digitalización, que permitió mejoras en la productividad y ganancias de eficiencia en procesos ya existentes, la 'datafication' promete redefinir completamente casi todos los aspectos de nuestra existencia. Mientras tanto, el concepto de 'datafication' codificación de datos se relaciona con el uso de las tecnologías digitales para utilizar el conocimiento asociado con los objetos físicos y los datos asociados con ellos. La ficticia de datos se manifiesta en la sociedad en una variedad de formas y, a menudo, pero no siempre, se asocia con sensores y actuadores, así como con la Internet de las cosas (IoT).
- Flujos de datos libres (Open data flows): la restricción a flujos internacionales de datos se puede convertir en un obstáculo grande a la innovación, a la integración internacional y al desarrollo de nuevas aplicaciones basadas en nube."

**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?

“Se recomienda convertir las preocupaciones con respecto a riesgos de Ciberseguridad en acciones claras y políticas eficaces para garantizar la misma ciberseguridad, creando la confianza necesaria en el proceso de digitalización, sobre todo en las aplicaciones críticas como salud, transportes, energía, agua, servicios públicos como seguridad pública y otras verticales. De esta manera, se puede establecer las condiciones para que avance la digitalización de todos los sectores de la economía y sociedad.”

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

"Cuando se habla de seguridad, el cifrado, y con frecuencia la criptografía extremo a extremo es el primer tema que surge. Si bien es ciertamente una herramienta importante, es sólo una de las muchas herramientas necesarias para garantizar la seguridad de un sistema 5G.

Para construir sistemas seguros es importante tener una visión holística y no solo enfocarse en partes individuales de forma aislada. Por ejemplo, las interacciones entre la autenticación del usuario, la criptografía del tráfico, la movilidad, las situaciones de sobrecarga y los aspectos de resiliencia de la red deben considerarse conjuntamente. También es importante comprender los riesgos relevantes y cómo tratarlos adecuadamente. Esto es lo que hace 3GPP al desarrollar las especificaciones que constituyen la base para la seguridad de los sistemas 5G.

La mentalidad holística también se manifiesta en las muchas organizaciones que están desarrollando el sistema 5G, cada una de las cuales cubre diferentes aspectos y / o se centra en partes específicas. Las especificaciones relevantes y los estudios y funciones de soporte son producidos por organizaciones tales como el IETF, la GSMA, el ETSI NFV y la ONAP, por mencionar algunos.

La seguridad y la resiliencia del sistema 5G se basan en el análisis continuo de amenazas y riesgos, así como en esfuerzos más dedicados. El propósito de esto es introducir un conjunto equilibrado de contramedidas que coincida adecuadamente con las amenazas y los riesgos identificados.

En un nivel más alto, un sistema 5G comprende un dispositivo conectado a una red de acceso 5G, que a su vez está conectado al resto del sistema llamado red central 5G. La red de acceso 5G puede incluir estaciones base de radio 3GPP y / o una red de acceso que no sea 3GPP. La arquitectura de la red central 5G es significativamente más inteligente que la 4G en términos de poder soportar la implementación en la nube y la IoT, con mejoras importantes en la segmentación de la red y la arquitectura basada en servicios (SBA), en particular.

El sistema 5G también se expande en 4G al agregar nuevas capacidades de radio (NR), al hacerlo de manera que LTE y NR puedan evolucionar conjuntamente de manera complementaria. Este desarrollo hace posible que el sistema 5G aproveche los nuevos e importantes conceptos del sistema 4G, que incluyen radio IoT (NB-IoT) de bajo consumo de energía, transmisión de datos pequeña y segura de baja latencia para dispositivos de baja potencia y dispositivos que utilizan estados inactivos de conservación de energía. En este documento, sin embargo, nos centramos en la seguridad de la radio NR y la red central 5G.

Además de la criptografía de vanguardia que se incluye en 5G, la confiabilidad del sistema 5G es el resultado de las cinco propiedades ilustradas en la figura abajo, a saber: resiliencia, seguridad de comunicación, gestión de identidad, privacidad y garantía de seguridad. Estas propiedades hacen del sistema 5G una plataforma confiable que permite la creación de muchos servicios nuevos.

Figura: <https://www.ericsson.com/assets/global/qbank/2018/03/28/five-properties-that-contribute-to-the-trustworthiness-of-the-5g-system-90158resize964844crop00964844autoorientquality90stripbackground23ffffffextensionjpg.jpg>

Más en: <https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system>

<http://www.3gpp.org/DynaReport/33899.htm>

<http://www.5gensure.eu/>