Constanza Polo Molina

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.

"Los requisitos de velocidad mínima para cada una de las bandas descritos en la consulta podrían ser razonables dependiendo de la interpretación que se dé a “velocidades mínimas”. Si en el área definida, Subtel entiende que, como mínimo, la red 5G debería poder proporcionar las velocidades de carga y descarga especificadas al aire libre en conjunto, entonces los requisitos son muy razonables. Sin embargo, si Subtel interpreta que los requisitos significan que cada dispositivo individual siempre obtendrá al menos estas velocidades, sin importar dónde se encuentren en el área de cobertura definida (interior, exterior, subterráneo, etc.), entonces estos requisitos no son prácticos. Las velocidades mínimas son casi imposibles de mantener a nivel de dispositivo individual, ya que depende en gran medida de la carga de la red fluctuante en cualquier momento y ubicación. De manera similar, el ambiente interior es demasiado complejo, impredecible e imposible de probar para poder mantener un objetivo de forma confiable en cualquier lugar, sin importar dónde se encuentre un dispositivo móvil.

Los requisitos deben encuadrarse como el rendimiento total mínimo alcanzable en el borde de la celda en el exterior en una red completamente descargada. Estos criterios se pueden usar para formular una Pérdida de ruta máxima permitida aceptable (MAPL), que se puede medir con bastante facilidad a través de la prueba de manejo realizada por Subtel. En cualquier caso, le pedimos a Subtel que proporcione muchos más detalles sobre una definición exacta de los requisitos de cobertura y cómo se planea medir y hacer cumplir esos compromisos mínimos.

No entendemos por qué hay un límite máximo en la cantidad de puntos que una propuesta puede recibir según el área cubierta. Actualmente, la forma en que está estructurada la consulta, el encuestado recibirá el número máximo de puntos permitidos para proporcionar los requisitos de rendimiento mínimo a aproximadamente el 5% del área de Chile en cada banda. Seguramente Chile se beneficiaría si se cubriera una mayor parte del país, ¿por qué no mantener un incentivo para que los encuestados aumenten tanto su área como la cobertura de la población?"

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?

“No hay comentarios”

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.

“Ver respuesta a pregunta No.1”

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

"Ciberseguridad debe ser un criterio importante en la evaluación de la oferta y debe calificarse y utilizarse como un diferenciador entre los remitentes. Se debe preguntar a los encuestados y deben abordar la seguridad en todos los vectores del ecosistema, incluidos:

• Operaciones de Seguridad / Gestión

• * Seguridad de dispositivos móviles

• Cifrado

• Datos / * Seguridad de la aplicación

•Seguridad de la red

• Protección avanzada contra amenazas

•Respuesta al incidente

• Inteligencia de amenazas globales

• * ICAM

• Protección de punto final

• Soluciones basadas en estándares industriales ISO / IEC, 3GPP

• Cumplimiento de procesos estándar de la industria, por ejemplo, ITIL

(* Opciones de usuario)

Un programa de ciberseguridad debe garantizar la disponibilidad y protección además de priorizar la seguridad, integridad y confidencialidad de los datos que atraviesan la red. La aplicación de la protección de seguridad perimetral únicamente, el enfoque “castle defense”, es un concepto obsoleto. Se requieren múltiples capacidades de seguridad integradas en todo el entorno para garantizar una protección completa y en capas. Una buena solución debe proporcionar seguridad E2E en: Core, Instalaciones, RAN, Aplicaciones y Equipo de Usuario y usar una estrategia de defensa contra amenazas de “defensa en profundidad” utilizando múltiples componentes y estrategias para conformar la solución de seguridad completa. El enfoque de defensa en profundidad presenta muchos vectores de ataque con muchas capas de protección y detección para frustrar a los adversarios con múltiples obstáculos únicos. Por ejemplo:

• Un ataque pasivo podría ser frustrado primero por el enlace y la encriptación de la capa de red para asegurar los flujos de tráfico. Si los adversarios vencen este obstáculo, se encontrarán con la seguridad habilitada en la capa de aplicación como una línea de defensa adicional.

• Un ataque activo puede encontrarse con cortafuegos y sistemas de detección de intrusos. Si se omiten esos sistemas, los adversarios se enfrentarán a controles de acceso en hosts y servidores dentro del propio entorno informático.

• Los ataques internos deben superar las medidas de seguridad física y personal. Si tienen éxito, estos adversarios serían sometidos a vigilancia técnica.

• Los ataques de denegación de servicio distribuido (DDOS) serán detectados por nuestro Sistema de protección contra intrusiones (IPS) y activarán el bloqueo automático del tráfico malicioso.

El oferente debe proporcionar y ser evaluado en una estrategia para un ciclo de vida de defensa de amenaza global, reconociendo que la ""seguridad de extremo a extremo"" significa que el enfoque tradicional de ""defensa de castillo"" debe adaptarse para convertirse en un marco de gestión de riesgos intercalado completo.

El proveedor de red debe tener y poder demostrar las capacidades para predecir, prevenir, detectar y responder a problemas de seguridad.

Además, se debe esperar que el proveedor de la red brinde acceso abierto y trabaje en colaboración con la agencia gubernamental correspondiente en cuanto a los planes, el estado, los informes de SLA y KPI, el cumplimiento (según las auditorias y las pruebas internas / externas), la alineación con los estándares nacionales y la respuesta a incidentes y revisiones post mortem (trimestrales)."

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

"Los oferentes deben abordar los 4 objetivos de seguridad clave que deben cumplirse para las implementaciones de seguridad IOT / M2M:

• Remitente y receptor autenticados, entre sí

• Disponibilidad y accesibilidad de la red, la falta de comunicación en sí es una falta de seguridad

• La precisión de los datos transmitidos, los datos de misión crítica deben estar libres de errores

• Confidencialidad, solo el destinatario correcto debe tener acceso a los datos transmitidos

Los riesgos de seguridad pueden ser reconocidos y comprendidos. Los oferentes deben abordar la implementación de los métodos de seguridad que se incorporarán en el dispositivo IOT / M2M y el software asociado con la aplicación con nuevas implementaciones y certificación relacionada. Entre otras cuestiones a considerar y gestionar se encuentran:

• Autenticación de presencia en múltiples redes.

• Autorización para servicios múltiples

• Escala para administrar la gran cantidad de dispositivos en soluciones IOT / M2M

• Automatización para la operación y gestión de aplicaciones.

• Largos ciclos de vida para dispositivos y aplicaciones desplegadas.

• Implementación de actualizaciones de seguridad en dispositivos remotos.

Se debe evaluar cómo los oferentes gestionarán o mitigarán el riesgo en un entorno IOT / M2M con procesos de certificación, capacidades y procesos de operaciones, diseño y optimización de la red y controles relacionados en los servicios IOT / M2M."

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

"Las redes 5G son tanto una evolución como una revolución innovadora de las redes móviles 4G. En consecuencia, la seguridad 5G ha sido diseñada para construirse sobre la base de, y mejorar aún más, los controles de seguridad 4G actuales. Las principales mejoras de seguridad en 5G según lo definido por 3GPP incluyen lo siguiente:

• Las comunicaciones seguras y los mecanismos de protección de integridad y cifrado de vanguardia se utilizan en 5G para proteger el plano de usuario, el plano de control y el tráfico de gestión.

• Marco de autenticación unificado para las diversas tecnologías y dispositivos de acceso 5G. Esto permitiría una movilidad sin problemas a través de diferentes tecnologías de acceso y soporte de conexiones concurrentes

• Protección de privacidad del usuario para la información que puede ser utilizada por partes no autorizadas para identificar y rastrear a los suscriptores (por ejemplo, proteger identificadores permanentes como SUPI, IMSI e IMEI) • Arquitectura segura basada en servicios y aislamiento de segmentos que permiten diferentes servicios y aplicaciones para implementar mecanismos de seguridad optimizados y evitar que los ataques se propaguen a otros segmentos

• Técnicas de detección y mitigación de RBS, utilizando mecanismos de detección de RBS asistidos por el UE y análisis de informes de radio

• En los escenarios de itinerancia, las redes domésticas y visitadas están conectadas a través de SEPP para abordar las vulnerabilidades de seguridad que se encontraron en las redes de itinerancia heredadas que utilizan los protocolos vulnerables de SS7 y Diameter. Además, 5G agregó soporte nativo para una dirección segura de roaming (SoR). La solución 5G SoR permite al operador de la red doméstica dirigir a sus clientes en itinerancia a sus redes de socios visitados preferidas para mejorar la experiencia de los clientes en itinerancia, reducir los cargos de itinerancia y prevenir el fraude de itinerancia.

• Varias características caracterizan a 5G como un paso revolucionario en los anales de la evolución de la tecnología móvil. Desde el concepto de segmentación de la red hasta la compatibilidad con dispositivos IoT altamente restringidos, desde NFVI hasta “cloudification”, desde latencias ultra bajas hasta la mejora de las velocidades de datos en órdenes de magnitud, 5G incorpora conceptos y características que marcan una significativa discontinuidad con el pasado."

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?

“No hay comentarios”

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

"Una nueva red o una nueva red 5G tienen ventajas sobre un híbrido existente o incluso una red únicamente 4G.

5G aborda los problemas de seguridad conocidos en los sistemas 4G y la simplicidad de una plataforma no híbrida con Ciberseguridad diseñada desde su inicio con los estándares y prácticas actuales es y debe considerarse una ventaja con una nueva solución de compilación. Los encuestados deben responder a la adhesión a los estándares 5G y describir las operaciones y la gestión de seguridad en entornos nuevos o existentes:

Puntos clave:

• TS 33.401, TS 33.501 (Fase 1) y TS33.501 (Fase 2) son especificaciones de seguridad 3GPP para interfaz de radio 5G e infraestructura de red

• Hay mejoras tanto para redes independientes 5G como con redes 4G / 5G interconectadas (roaming)

• La diferenciación entre seguridad 4G y 5G se aborda con la moneda de lanzamiento, y debe ser necesaria. Las operaciones en un entorno de tecnología mixta envejecida son intrínsecamente más complejas y desafiantes, y deberían considerarse más desafiantes e inferiores a una nueva solución de construcción.

• 5G Security representa mejoras sobre la seguridad 4G y problemas conocidos y vulnerabilidades

• Dado el cumplimiento estándar, las personas, los procesos y los sistemas son áreas de diferenciación entre los posibles operadores. Seguridad debe ser incluido como un elemento clave a considerar y evaluarse como un diferenciador."