José Felipe Otero Muñoz

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 5.	El énfasis de la industria de telecomunicaciones móviles en la seguridad ha sido un diferenciador muy importante con respecto a otras tecnologías inalámbricas. El uso de espectro bajo licencia y para uso exclusivo provee una capa adicional de protección contra el acceso sin consentimiento al tráfico de voz, video o datos. La seguridad ha sido una de las prioridades de las distintas generaciones de tecnologías de banda ancha móvil. Los grupos técnicos de trabajo del Third Generation Partnership Project (3GPP) han producido mecanismos, especificaciones y características de seguridad para 3G, 4G y ahora 5G. El Grupo de Trabajo SA3 es responsable por los aspectos de seguridad y privacidad para los sistemas 3GPP y el alcance de su trabajo es determinar requisitos de seguridad y privacidad, así como especificación de arquitecturas y protocolos para tales fines. El 3GPP combina siete organismos de normalización y provee para sus miembros un ambiente estable para producir reportes y especificaciones definitorias para sus tecnologías. Por ejemplo, la 3GPP TS V15.1.0 (2018-06) es una especificación reciente publicada por el grupo SA3 para seguridad de las redes 5G. Define arquitectura, características y mecanismos para las redes 5G, incluyendo sus centrales (Core). Adicionalmente, abarca procedimientos de seguridad que se realizan al interior de los sistemas 5G, incluyendo centrales y Nueva Radio (NR).

	5G introduce además el concepto de "Network Slicing" que da a los operadores capacidades de segmentación que no eran posibles en generaciones móviles pasadas. La segmentación es una alternativa común en el mundo de las tecnologías de la información para mitigar riesgos de seguridad informática.
Artículo 12.	El Internet de las Cosas (IoT) es uno de los servicios con más proyección con 5G, pero también involucran riesgos de seguridad digital. Varios "objetos" del IoT pueden tener vulnerabilidades de "día cero", desconocidas incluso para sus fabricantes, que luego puedan ser explotadas por quienes buscan perpetrar ataques informáticos. Además de las medidas de seguridad que ya contempla la industria de telecomunicaciones móviles, una preocupación actual es la falta de estandarización en IoT, aunque hay organizaciones de normalización y estandarización que se encuentran trabajando en ello. Con una mayor distribución de las capacidades de la red con el uso de Cloud y computación en el borde (Edge Computing), surgen otras consideraciones de seguridad para redes 5G que la industria busca atender con estrategias proactivas y reactivas. En la formación de esas estrategias participan los operadores, fabricantes de equipo, organizaciones normalizadoras y otras asociaciones formando un bucle iterativo de aprendizaje continuo sobre nuevas amenazas y opciones de respuesta. En la modernización de las redes móviles, la automatización, orquestación y virtualización de las funciones de la red

	(NFV) son tecnologías clave para responder, contener y prevenir ataques al combinarse elementos de ciberseguridad. Además de esas funciones de la red, la segmentación de sistemas se incluye en 5G con “Network Slicing”, la habilidad de configurar la operación de redes virtuales/lógicas para dar soporte a aplicaciones de negocio o servicios independientes sobre una misma infraestructura física. En la arquitectura de 5G, esta funcionalidad aprovechará atributos de virtualización central de 5G para atender de manera flexible una amplia variedad de requisitos de rendimiento y seguridad para varios servicios. La industria continúa trabajando sobre retos de implementación de seguridad en “Network Slicing”, como el aislamiento de las secciones de la red y el aseguramiento para casos de uso específicos apoyadas en gestión definida por software (SDN). Otro elemento en la respuesta a retos de seguridad para la industria móvil es la Infraestructura Basada en Servicios (Service Based Architecture o SBA), que permite la creación de “secciones” de la red optimizadas para servicios específicos. Este esquema da soporte a requerimientos específicos de seguridad que pueden requerir algunos servicios que no necesariamente se requieren implementar en otras secciones.
Comentarios Generales.	El camino a la seguridad en redes de telecomunicaciones es una evolución de mejores prácticas en común, gente, procesos y herramientas que ya se observan en la industria para asegurar la infraestructura de red. Las redes 5G son simultáneamente una evolución y una

	revolución con respecto a las redes 4G y la seguridad 5G está diseñada para expandir y mejorar los fuertes controles de seguridad de redes 4G. 5G Americas resume algunas las principales mejoras de 5G definidas por el 3GPP en seguridad: • Comunicaciones seguras y encriptación para proteger la gestión de tráfico, y los planos de control y usuario. • Marco de referencia unificado para autenticación (soporte para conexiones concurrentes manteniendo movilidad). • Protección y privacidad de la información. • SBA segura y aislamiento de “secciones” de la red (Network Slicing) para optimizar mecanismos de seguridad y prevenir contacto con otras secciones. • Detección y mitigación de radio bases falsas (“rogue”, o RBS por sus siglas en inglés). • Enlace a través de un Security Edge Protection Proxy para roaming entre las redes doméstica y visitante. La seguridad en 5G seguirá evolucionando y los mecanismos preconfigurados serán complementados progresivamente con Inteligencia Artificial (IA), que apoyará en el despliegue e implementación de mecanismos de defensa, tomando en cuenta que los ataques también evolucionarán. Cuando la detección se logra “inscribir” en elementos de la propia red, los nodos 5G se convierten en una especie de detectores de amenazas, incrementando la efectividad potencial de

	los sistemas de defensa, que a su vez son más fuertes si se logra una segmentación adecuada. Las tecnologías de Network Slicing y su integración con IA son desarrollos futuros que se esperan en grandes rasgos en cuanto a seguridad en 5G. 5G Americas agradece a la SUBTEL la atención concedida para acercar su visión sobre temas relacionados con el desarrollo de las telecomunicaciones. Sin otro particular, le saludo atentamente. José F. Otero Muñoz. Vicepresidente para América Latina y el Caribe, 5G Americas. Los comentarios expresados en esta contribución están fundamentados en el reporte de 5G Americas "The Evolution of Security in 5G. A 'Slice' of Mobile Threats" (Julio 2019). Disponible en ww.5gamericas.org. Acerca de 5G Americas: 5G Americas es una asociación de la industria de telecomunicaciones que aboga por la promoción y desarrollo del ecosistema de tecnologías inalámbricas de banda ancha en las Américas. Para lograrlo tenemos como compromiso de trabajar con organismos gubernamentales, órganos regulatorios, órganos normalizadores y otras organizaciones mundiales de tecnologías inalámbricas de toda la región para promover e impartir conocimientos para la implantación exitosa de tecnologías inalámbricas de banda ancha, incluida la asignación del espectro adecuado y el desarrollo de políticas regulatorias coherentes, justas y efectivas. Nuestra asociación apoya las iniciativas regulatorias destinadas a promover el despliegue y desarrollo de servicios móviles avanzados en Chile y el resto de las

	Américas.