Septiembre 2021

Instituto Dominicano de las Telecomunicaciones
Av. Abraham Lincoln No. 962
Santo Domingo, República Dominicana.
Código Postal 10148

Enviado al correo electrónico: consultapublica@indotel.gob.do

Ref.: Consulta pública para dictar el "Reglamento de Ciberseguridad para la Prestación del Servicio de Acceso a Internet".

Estimados Sres.,

Agradecemos al Instituto Dominicano de las Telecomunicaciones (INDOTEL) la oportunidad de presentar nuestros comentarios sobre la situación actual de las políticas públicas en torno a los servicios móviles en la República Dominicana.

Los comentarios expresados en esta comunicación están fundamentados en las siguientes publicaciones de 5G Americas[1]:

- "The Evolution of Security in 5G. A 'Slice' of Mobile Threats". Julio 2019.
- "Security Considerations for the 5G Era". Julio 2020.

Artículo 4 (marco de trabajo y gobernanza) – Párrafo I.

5G Americas sugiere considerar hacer más específico el alcance del párrafo de este artículo para los operadores de red móvil, ya que el proyecto de reglamento menciona que la función de ciberseguridad de las prestadoras de servicio de acceso a Internet debe estar segregada de las funciones de gestión y operación de las redes. Esta sugerencia se realiza en función de que la arquitectura de redes 5G integra funciones de red que se consideran aptas para ayudar en labores de ciberseguridad y protección de la integridad de redes.

[1] 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 entidades gubernamentales y otras organizaciones de tecnologías inalámbricas de toda la región Américas para impulsar la implantación exitosa de tecnologías inalámbricas de banda ancha, incluida la asignación del espectro radioeléctrico adecuado y el desarrollo de políticas regulatorias coherentes, justas y efectivas. Las publicaciones de 5G Americas están disponibles para su consulta en https://brechacero.com/white-papers/ y https://www.5gamericas.org/white-papers/

Las redes 5G se diseñan como arquitectura basada en servicios (SBA) que soporta funciones *"cloud-native"*, desagregación, segmentación de secciones de la red, software abierto y que incorpora plenamente la automatización y los conceptos de SDN y NFV. El 3GPP ha generado estándares para redes 5G enfocándose en mejorar la protección de elementos como la confidencialidad de la información, integridad de la red, autenticación y aislamiento de elementos de la red, considerando las vulnerabilidades futuras, pero también las relacionadas con la operación de redes 3G y 4G, que convivirán con las redes 5G por lo menos de manera transitoria.

En este sentido, la seguridad para los proveedores de acceso a Internet por medio de redes móviles sugiere la importancia de tener una relación con las áreas de gestión operativa de las redes. Concretamente, la capacidad de *network slicing* (definida en el estándar TS 23.501 del 3GPP) se está tornando en una de las funciones de ciberseguridad más visibles para las redes 5G (y para la mayoría de sus casos de uso), ya que en términos simplificados es la habilidad que tienen estas redes para configurar y administrar de manera automatizada múltiples redes lógicas que operen virtualmente como independientes, aunque compartan una misma infraestructura física. En la práctica, esto equivale a la segmentación de una red móvil de manera virtual en porciones que pueden ser asignadas a diferentes fines o servicios, como a una red privada.

La capacidad de *network slicing* es distinta a las redes privadas virtuales o VPN: *network slicing* implica aislamiento de punta a punta de una porción de la red, incluyendo la red de acceso radioeléctrica (RAN), la red de transporte y el núcleo de la red; los VPN se implementan encima de una capa de recursos físicos de red.

Artículo 7 (capacitación sobre ciberseguridad) - Inciso A.

Se sugiere considerar una definición más específica en torno a la clasificación de personal de nuevo ingreso que debe ser capacitado en materia de ciberseguridad, ya que el inciso es ambiguo en este sentido y pueden existir cargos laborales en los que no se justifique una capacitación con respecto a esta clase de temas, dependiendo de sus funciones dentro de la organización.

Artículo 22 (Gestión de vulnerabilidades) y Artículo 30 (seguridad en ambientes de nube).

Con respecto a estos dos artículos, 5G Americas desea compartir algunas de las características de seguridad desarrolladas como parte de la estandarización de tecnología para redes 5G, para consideración del INDOTEL.

El Grupo SA3 del 3GPP ha definido la arquitectura de seguridad para redes móviles 5G en la especificación TS 33.501, que incluye una estructura multidimensional en la que los

1000 112th Ave
Bellevue, WA. USA
+ 1 425 372 8928
www.5GAmericas.org

operadores mantienen labores de monitoreo, partiendo de una premisa de riesgos continuos en el desarrollo de las redes. La evolución de la seguridad de la red se fundamenta en activar controles adecuados ante amenazas emergentes.

En materia de autenticación, las redes 5G introducen funciones de protección en el plano del usuario, un elemento que no estaba presente en el diseño de redes móviles previas. Las técnicas de autenticación previstas para 5G mejoran las presentes en 4G desde áreas distintas, como con la adopción de un marco de autenticación unificado, por ejemplo. Las mejoras en protocolos y técnicas de autenticación también están diseñadas para mejorar la privacidad de la información de los usuarios, como se establece por ejemplo en la especificación TS 23.003 del 3GPP.

Network Slicing es otra de las funcionalidades clave de seguridad de 5G por su capacidad para aislar de punta a punta una porción de la red. Se recomienda consultar el comentario al artículo 4 del proyecto expuesto previamente en esta carta.

En la estandarización de 5G se observan beneficios de la adopción de software de código abierto, ya que esto permite a los operadores y fabricantes de tecnología trabajar con un entorno de desarrolladores más amplio que puede ayudar al personal con atribuciones de ciberseguridad dentro de las organizaciones. La revisión constante del software ayuda a mejorar su rendimiento y seguridad con la identificación y corrección constante de vulnerabilidades, creando un "repositorio confiable" que solo algunos desarrolladores confiables ("trusted developers") puede utilizar y modificar de manera directa. Este elemento es relevante conforme las redes van siendo definidas incrementalmente por software.

Para las redes 5G también se considera que la adopción de un modelo de seguridad "Zero-Trust" es adecuado por la incorporación de controles estrictos que incluye, por ejemplo, mejora en los procesos de encriptación para mitigar riesgos como el monitoreo por partes no autorizadas de dispositivos conectados. En este modelo es relevante la introducción de soluciones basadas en software y "nube". Para las redes móviles, este modelo se considera un complemento de la estrategia general que abarque la protección a infraestructura física más distribuida con ayuda de soluciones de virtualización. El modelo "Zero-Trust" es relevante considerando sobre todo que los centros de datos de aplicaciones en uso en la República Dominicana pueden estar ubicados en otras jurisdicciones.

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.

5G Americas agradece al INDOTEL la atención concedida para acercar su visión sobre temas relacionados con el desarrollo de las telecomunicaciones.

Sin otro particular, le saludo atentamente.

José Otero
Vicepresidente para América Latina y el Caribe

1000 112th Ave
Bellevue, WA. USA
+ 1 425 372 8928
www.5GAmericas.org