Ciberseguridad 5G

Periodo de estudios 2022-2025

Cuestión 3/2

Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad

Producto provisional 2024

Resumen ejecutivo

Este producto provisional hace hincapié en aspectos clave de la ciberseguridad 5G habida cuenta del aumento de las ciberamenazas mundiales y la naturaleza crítica de la infraestructura de telecomunicaciones. La tecnología 5G introduce **nuevos paradigmas de seguridad** con su software avanzado, su arquitectura basada en la nube y su amplia conectividad. Si bien ofrece importantes beneficios, también conlleva nuevos riesgos que requieren medidas de ciberseguridad sólidas para protegerse contra las amenazas.

La complejidad de las redes 5G exige estrategias de seguridad avanzadas y colaboración entre las diferentes partes interesadas. Varias **organizaciones de normalización** han empezado a normalizar los aspectos de ciberseguridad de las redes 5G, pero son necesarias una cooperación y comunicación continuas para evitar la duplicación de esfuerzos.

Las **medidas proactivas de ciberseguridad** son cruciales en todas las etapas del despliegue de la red, y los proveedores y operadores tienen responsabilidades en la gestión de los riesgos de ciberseguridad.

Se están elaborando **diversas políticas y reglamentaciones nacionales para la ciberseguridad 5G**. Muchos países ya han adoptado sus propios enfoques para reducir los riesgos de seguridad y ahora se están centrando en su implementación y en aplicar regímenes de conformidad.

Invertir en educación y formación es vital para hacer frente a la creciente demanda de profesionales cualificados en ciberseguridad.

De cara al futuro, la **planificación de la 6G** hace hincapié en la mejora de la ciberseguridad y la resiliencia desde el principio. El marco IMT-2030 de la UIT refleja el compromiso de integrar medidas de seguridad sólidas para respaldar futuros avances tecnológicos.

Introducción

Durante la última Conferencia Mundial de Desarrollo de las Telecomunicaciones, celebrada en Kigali (Rwanda) en junio de 2022, se examinó el mandato de la Cuestión de Estudio 3/2 de la Comisión de Estudio 2 del UIT-D, "Seguridad en las redes de información y comunicación: Prácticas idóneas para el desarrollo de una cultura de ciberseguridad". Uno de los temas de estudio específicos fue "Discutir acerca de los desafíos y enfoques para la ciberseguridad de 5G".

En el mandato aprobado para la Cuestión 3/2 se reconoce que las amenazas a la ciberseguridad siguen siendo una preocupación importante para los Gobiernos, las organizaciones y las personas de todo el mundo. A nivel mundial, la inseguridad cibernética está clasificada como el cuarto riesgo más grave a corto plazo según el Informe sobre Riesgos Mundiales (*Global Risks Report*) 2024 del Foro Económico Mundial[1]. Las redes de telecomunicaciones, que en muchas jurisdicciones se consideran un componente vital de la infraestructura nacional crítica o de los servicios esenciales, son vulnerables a ciberataques que pueden perturbar los servicios esenciales y la seguridad pública.

La introducción de la tecnología 5G representa un cambio significativo en las telecomunicaciones, ya que ofrece velocidades más rápidas y una mejor conectividad con el potencial de mejorar la economía, ampliar las aplicaciones de Internet de las cosas (IoT) y aportar nuevas soluciones a la comunicación digital. Con todo, la sofisticada arquitectura que permite estos avances también plantea complejos desafíos de ciberseguridad que requieren una comprensión exhaustiva y medidas de protección sólidas.

Reconociendo la importancia crítica de salvaguardar la infraestructura y los servicios 5G, en el marco de la Cuestión 3/2 la Comisión de Estudio 2 organizó un taller al respecto de un día de duración, el 2 de mayo de 2024, en el que participaron responsables políticos, reguladores, operadores y otros miembros del sector de las telecomunicaciones para debatir sobre la complejidad intrínseca de la ciberseguridad 5G, compartir prácticas existentes y explorar soluciones innovadoras a las nuevas amenazas. A medida que las redes 5G se despliegan en todo el mundo, es necesario establecer un ecosistema seguro para garantizar la integridad, disponibilidad y confidencialidad de la información, así como para proteger la infraestructura que se ha convertido en la columna vertebral de la economía digital.

En el presente informe se muestran los debates del taller y las contribuciones recibidas durante este ciclo de estudios. El documento no pretende ser un informe técnico sobre ciberseguridad 5G. El objetivo es más bien compartir reflexiones y buenas prácticas recopiladas por la Cuestión de Estudio, las cuales podrán tener en cuenta los Miembros de la UIT para aplicarlas en sus contextos nacionales. El presente informe se centra principalmente en la ciberseguridad 5G de las redes electrónicas públicas.

1. La 5G aporta nuevos paradigmas de seguridad a las redes de telecomunicaciones

Aspectos generales de la ciberseguridad 5G

La 5G se caracteriza por sus avanzados sistemas de software que permiten una fácil configuración y conectividad masiva de suscriptores y dispositivos. Esta tecnología soporta aplicaciones de baja latencia, como la realidad aumentada, la telecirugía y los servicios integrados de Internet, que dependen de la robustez y fiabilidad de la red. Uno de los principales casos de uso de la 5G es Internet de las cosas (IoT), que aprovecha la capacidad de la 5G para conectar un gran número de puntos extremos. La tecnología 5G está llamada a revolucionar la conectividad, lo que también plantea nuevos y dinámicos riesgos y desafíos en materia de ciberseguridad.

A diferencia de las generaciones anteriores de tecnologías inalámbricas, la 5G introduce un cambio significativo hacia la arquitectura basada en la nube, las redes definidas por software (SDN) y la virtualización de la función de red (NFV). Este cambio crea un panorama de ciberseguridad más complejo y dinámico.

A medida que la 5G se generalice, también se espera que la infraestructura de telecomunicaciones se convierta en un objetivo aún más atractivo para las actividades cibernéticas maliciosas que requieren medidas de seguridad avanzadas que se adaptan a las amenazas en evolución. La ciberseguridad para la 5G debería centrarse en aumentar la resiliencia de todo el ecosistema, incluidas la infraestructura y las aplicaciones. Esto incluye proteger dispositivos, datos y redes conectados contra las ciberamenazas.

Reconociendo que diferentes organizaciones emplean diferentes definiciones de ciberseguridad[2], cabe recordar que en este informe por "ciberseguridad 5G" debe entenderse la ciberseguridad en el contexto de la 5G con sus nuevos parámetros, normas y particularidades tecnológicas, que deben gestionarse adecuadamente para poner a salvo el ecosistema digital en su integridad y garantizar la ciberresiliencia.

[1] Global Risks Report 2024

[2] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Para la UIT, la ciberseguridad se define en la Recomendación UIT-T X.1205 del UIT-T como *"[...] el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Los objetivos generales de seguridad comprenden los siguientes:*

- *disponibilidad*
- *integridad, que puede incluir la autenticidad y el no repudio*
- *confidencialidad"*[3].

Despliegue de redes tradicionales

Los operadores tienden en un primer momento a desplegar las redes 5G de forma no autónoma, aprovechando la infraestructura 4G existente antes de desplegar una red 5G de extremo a extremo autónoma[4]. Las redes 5G no autónomas heredan las vulnerabilidades de la 4G e incluso de la 2G y la 3G, que deberán gestionarse debidamente. Para algunos operadores esto equivale a una "deuda técnica": la gestión de sistemas más antiguos implica que se ha de establecer un conjunto de controles de seguridad normalizados para medir el estado de seguridad de los componentes de la infraestructura en las distintas etapas de su madurez generacional[5].

Es importante destacar que la 5G autónoma presenta oportunidades para mejorar la ciberseguridad en comparación con las generaciones pasadas de tecnología móvil, ya que está diseñada para ser más segura que la 4G. Se han observado mejoras en ámbitos tales como la seguridad y privacidad de los abonados, la red de acceso radioeléctrico (RAN), el núcleo de red y la seguridad de la itinerancia[6,7].

2. Las actividades de normalización para proteger la 5G se llevan a cabo en múltiples organismos de normalización, por lo éstos deben concertarse para comunicarse y evitar la duplicación de sus trabajos

Organismos de normalización activos en la ciberseguridad 5G

Debido a la complejidad de la tecnología 5G y a los problemas que conlleva, ningún organismo de normalización tiene mandato exclusivo en materia de ciberseguridad de la 5G. Para evitar la duplicación se han desarrollado mecanismos para el intercambio de información entre organismos de normalización y para coordinar sus propuestas y temas de trabajo.

Para ayudar a conocer estas diferentes actividades y orientar la labor de normalización de la seguridad relacionada con la 5G en el UIT-T, la Comisión de Estudio 17 (CE 17) preparó un informe técnico en el que establecía la correspondencia entre las normas presentes y en desarrollo y sus correspondientes organismos y su aplicación en las redes 5G[8]. En el informe se identifican las normas del UIT-T, el 3rd Generation Partnership Project (proyecto de asociación de tercera generación, 3GPP), el Instituto Europeo de Normas de Telecomunicación (ETSI) y la IEEE Standards Association (IEEE SA), además de otros recursos no normalizados relevantes para la ciberseguridad 5G.

La Comisión de Estudio 17 del UIT-T ha publicado 11 Recomendaciones sobre seguridad de la 5G sobre la base de las contribuciones presentadas por operadores, proveedores, fabricantes de teléfonos inteligentes y proveedores de contenido, entre otros. Esas Recomendaciones se centran en cinco esferas: SDN-NFV, segmentación de red, computación periférica móvil, gestión de redes 5G y servicios 5G. La CE 17 ha establecido vínculos con otros organismos de normalización (como 3GPP y el Grupo de Tareas sobre Ingeniería de Internet (IETF)) y con grupos del sector que trabajan en especificaciones importantes para la normalización de la ciberseguridad 5G.

Uno de esos grupos industriales es la GSM Association (GSMA), que aunque no es un organismo de normalización, redacta especificaciones convocando a sus miembros y colaborando con los organismos de normalización para mejorar y/o adoptar dichas especificaciones como normas. GSMA ha publicado una lista de controles de seguridad básicos que los operadores móviles pueden voluntariamente tener en cuenta al desplegar redes 5G[9].

Dadas las numerosas fuentes de información relevantes para la seguridad 5G, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, ENISA, ha publicado un repositorio únificado de controles técnicos de seguridad para redes 5G denominado 5G Security Controls Matrix[10]. Este repositorio se publica actualmente

3 https://www.itu.int/rec/T-REC-X.1205-200804-I

4 Los dispositivos que utilicen redes 5G no autónomas normalmente se conectarán a las frecuencias 5G para la transmisión de datos cuando necesiten mayor ancho de banda y menor latencia (como para la comunicación entre automóviles inteligentes), o para reducir el consumo de energía de los dispositivos habilitados para IoT, pero seguirán dependiendo de las redes 4G e incluso 2G/3G para las llamadas de voz y los mensajes SMS. Fuente: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

5 Material de taller – Maxis.

6 https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

7 https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

8 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf

9 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

10 https://www.enisa.europa.eu/publications/5g-security-controls-matrix

como una hoja de cálculo, pero la agencia también está desarrollando una herramienta web para mejorar la facilidad de uso.

A medida que aumenta la complejidad de las redes y que las telecomunicaciones convergen con las redes IP, es cada vez más difícil atribuir cada esfera de normalización específica a un único organismo de normalización, lo que aumenta el riesgo de solapamiento y duplicación del trabajo y hace que la comunicación y el intercambio de información entre los organismos de normalización sean aún más importantes.

Integración de las normas en los requisitos reglamentarios obligatorios

Las normas ayudan a garantizar la interoperabilidad entre tecnologías y a reducir el tiempo necesario para que una innovación llegue a los mercados mundiales. Las normas de ciberseguridad pueden definir una base de referencia común que refleje las prácticas idóneas universales. Las normas son el resultado de un proceso basado en el consenso. Pueden ser de obligado cumplimiento, pero en la mayoría de los casos son opcionales, dando a proveedores y operadores una mayor flexibilidad a la hora de tomar decisiones de despliegue. En algunos casos, las normas pueden convertirse en obligatorias si la reglamentación técnica nacional integra una norma específica entre sus requisitos de seguridad. Las estrategias de ciberseguridad 5G nacionales deben equilibrar las prácticas idóneas mundiales con la realidad operativa local. Por lo general, los requisitos de regulación nacionales deben basarse en normas internacionales acordadas, adaptándolas al contexto y las necesidades locales para garantizar el éxito del despliegue y la ciberseguridad de las redes.

3. Las normas y especificaciones deben complementarse con medidas proactivas de ciberseguridad a lo largo de las diferentes etapas del despliegue de la red

Consideraciones de seguridad a nivel de proveedor

Las normas y especificaciones son solo uno de los componentes de la ciberseguridad 5G. La forma en que los proveedores y operadores implementan esas normas y las configuran define la postura segura de las redes 5G. Ericsson ha adoptado un enfoque integral de la seguridad 5G que atañe a cuatro capas: normas, desarrollo de productos de proveedores, despliegue de redes y operaciones de red[11]. La compañía considera que este enfoque integral puede garantizar que las medidas de mitigación se implementen de tal manera que las interdependencias entre las capas, así como los detalles específicos de una capa en cuestión, se aborden de manera efectiva.

Como ejemplo concreto de medida de seguridad 5G, el esquema de garantía de seguridad de equipos de red (NESAS)[12], desarrollado por GSMA y 3GPP, busca mejorar los niveles de seguridad de los equipos de redes móviles proporcionando un esquema de garantía que pueda aplicarse a nivel mundial. El sistema se basa en auditorías internas y expertos independientes (es una combinación de evaluación entre procesos de proveedores y evaluación de productos) para ofrecer acreditación. El objetivo de este plan es reducir la carga de las pruebas de seguridad para los proveedores de equipos de red, que suelen operar a escala mundial. Los principales proveedores ya han obtenido la acreditación NESAS. NESAS también es un candidato para el esquema de certificación de ciberseguridad de la UE en 5G[13], una certificación a nivel de la Unión que daría conformidad a todos sus Estados. Esta certificación no sustituiría al actual esquema NESAS, sino que ambos existirían en paralelo. Es esencial desarrollar esquemas/iniciativas de certificación de manera que sigan siendo flexibles y puedan actualizarse rápidamente, ya que el panorama de amenazas está en constante evolución.

En el Reino Unido, NCSC recomienda utilizar el marco de evaluación de proveedores[14], una guía que ayuda a los operadores a evaluar el riesgo cibernético asociado a la utilización del equipo del proveedor.

Consideraciones de seguridad a nivel de operador

NESAS puede garantizar la seguridad de un equipo de red antes de su despliegue. A medida que los operadores despliegan y explotan sus redes se han de integrar otras consideraciones de seguridad, por ejemplo, la detección de ataques y la respuesta automatizada. Aquí es donde los operadores deberían plantearse aprovechar la IA, la inteligencia de amenazas y el análisis para ayudar a respaldar su defensa cibernética. La ciberseguridad 5G ofrece beneficios, como la seguridad en tiempo real y estrategias como la confianza cero, que mejoran la visibilidad del sistema. Con todo, también trae consigo diversas dificultades, como mantener la conectividad entre diferentes redes con distintos niveles de seguridad, trabajar con componentes heredados y diversos tipos de redes, y las complejidades de integrar la IA en las medidas de seguridad. Al aplicar controles de acceso estrictos conformes con los principios del "menor privilegio" se reducen al mínimo diversos derechos en la red (por ejemplo, derechos de acceso entre funciones de red, derechos de administrador de red, configuración de virtualización). Existe una gran cantidad de literatura sobre las estrategias de ciberseguridad específicas de 5G que los operadores pueden tener en cuenta[15].

Las pruebas reales de redes de telecomunicaciones también son fundamentales para establecer el verdadero riesgo cibernético para estas redes. Los operadores pueden llevar a cabo algún tipo de prueba de seguridad en sus propias redes y sistemas, ya sea utilizando

[11] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

[12] https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/

[13] https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

[14] https://www.ncsc.gov.uk/report/vendor-security-assessment

[15] Véase por ejemplo: https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf y https://www.5gamericas.org/security-for-5g/

recursos internos o recurriendo a contratistas externos independientes. Por ejemplo, en el Reino Unido, TBEST es un programa de pruebas de penetración basado en resultados que simula las técnicas y tácticas que pueden utilizar ciberatacantes con muchos recursos. Mediante el programa se evalúa la capacidad de un proveedor de comunicaciones de detectar, contener y responder a un ataque de este tipo. El objetivo general es encontrar y eliminar vulnerabilidades de seguridad u otras debilidades en las funciones, procesos, políticas, sistemas o redes de un proveedor que podrían utilizarse en conjunto para poner en peligro los sistemas fundamentales de una empresa antes de su detección. Al someterse al programa TBEST voluntario, los proveedores de comunicaciones pueden conocer en qué áreas concretas podría mejorarse su seguridad. Ofcom, el regulador, trabaja con estos proveedores para ayudarlos a implementar los cambios apropiados de manera oportuna[16].

Es esencial que la ciberseguridad 5G sea comercialmente rentable, aunque, si bien los operadores deben rentabilizar sus inversiones en servicios 5G, es indispensable aplicar unas medidas de seguridad básicas y que éstas están adecuadamente presupuestadas.

Open RAN es la desagregación de la red de acceso radioeléctrico (RAN) y la normalización de las interfaces que los conectan que permite construir redes utilizando piezas de diferentes proveedores.

Por un lado, la arquitectura Open RAN puede añadir complejidad a la cadena de suministro de las redes de telecomunicaciones. Fomenta la diversidad de proveedores y nuevos vectores de ataque, por lo que exige mayores esfuerzos de integración en toda la cadena de suministro. Por otro lado, Open RAN añade transparencia a la cadena de suministro, da a los operadores más visibilidad y les permite supervisar y detectar riesgos de seguridad. En pocas palabras, les permite entender mejor la arquitectura y equipos de red y permite una detección y gestión de vulnerabilidades más completas. La O-RAN Alliance, principal fuente de especificaciones de Open RAN, está trabajando en especificaciones de seguridad para la arquitectura de estas redes con el objetivo de normalizar estas especificaciones en el ETSI.

NTT Docomo (Japón) es uno de los operadores que ha adoptado la arquitectura Open RAN por su flexibilidad en la elección de equipos. La decisión planteó cuestiones desde el punto de vista de la seguridad, ya que en general se considera que la apertura significa un aumento en el número de oportunidades de ataques. Ahora bien, el operador ha comparado la RAN tradicional y la Open RAN, y ha llegado a la conclusión de que hay poca diferencia de seguridad entre ambas[17].

4. Las redes 5G y la ciberseguridad son el centro de atención de recientes iniciativas de políticas y regulación que se encuentran en diferentes fases de implementación

Ejemplo de políticas y regulaciones nacionales para proteger las redes 5G

Además de las normas y prácticas de los proveedores y operadores, a nivel nacional pueden proponerse políticas y regulaciones para proteger las redes 5G. Estas adoptarán diversas formas, desde evaluaciones de proveedores, pruebas, certificaciones y definición de directrices o requisitos. Aunque los enfoques difieren en función de los contextos nacionales, todas estas iniciativas tienen por objeto reducir los riesgos de seguridad, incluidos los cibernéticos específicos, que presenta la 5G. Los regímenes de implementación y conformidad también deberían tenerse en cuenta como parte del marco general.

Los ejemplos siguientes ofrecen una instantánea de las diferentes medidas y su estado actual.

- El enfoque integral del **Brasil** para la ciberseguridad 5G se centra en la gestión de riesgos con los operadores. De acuerdo con los términos de la subasta de espectro 5G y el Reglamento de Ciberseguridad del Sector de las Telecomunicaciones[18], los operadores 5G están obligados a cumplir el marco reglamentario que incluye principios, directrices y controles *ex ante* para velar por la ciberseguridad en todo el sector. Estos controles combinan la gobernanza de ciberseguridad, la notificación obligatoria de incidentes, el intercambio de información, los ciclos de evaluación de vulnerabilidades y la presentación de informes sobre infraestructuras críticas, entre otras disposiciones. La Agencia Nacional de Telecomunicaciones del Brasil (Anatel) también se ha asociado con instituciones académicas para realizar estudios al respecto[19].
- El Gobierno del **Reino Unido** desarrolló un marco de seguridad para los proveedores de redes o servicios públicos de comunicaciones electrónicas mediante la Ley de Comunicaciones de 2003, modificada por la Ley de Telecomunicaciones (Seguridad) de 2021 (la TSA). Este marco se aplica a la 5G y a todas las demás redes: aunque que el Reino Unido está haciendo la transición a una futura 5G y a todas las redes de fibra completa, muchos proveedores de red incorporan tecnologías más antiguas en su infraestructura. En la TSA se establecen nuevas obligaciones de seguridad para todos los proveedores de telecomunicaciones públicas[20] y otorga nuevas facultades al Secretario de Estado para promulgar reglamentos y publicar códigos de práctica, que desde entonces han sido elaborados

16 https://www.itu.int/md/D22-SG02.RGQ-C-0074/es

17 Para más información sobre la seguridad de Open RAN, véase por ejemplo https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

18 https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740 (en portugués) y https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (en portugués)

19 Algunos de los resultados están disponibles en: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (en portugués)

20 Excepto microentidades.

e justificados mediante consulta pública[21]. En la Ley también se incluyen disposiciones que refuerzan las facultades reglamentarias de Ofcom para supervisar y hacer cumplir la forma en que los proveedores cumplen con sus nuevas obligaciones.

- Las regulaciones y políticas de ciberseguridad 5G de la **República de Corea** se reconocen como unas de las más estrictas del mundo, lo que refleja la posición de liderazgo del país en la adopción de la tecnología 5G. El Gobierno coreano, a través del Ministerio de Ciencia y TIC (MSIT) y la Agencia de Internet y Seguridad de Corea (KISA), ha implementado un marco integral para salvaguardar las redes 5G. El marco incluye requisitos estrictos para que los operadores de telecomunicaciones aseguren la infraestructura de red, protejan los datos de los usuarios y reduzcan los riesgos de ciberseguridad. Las regulaciones se centran en la necesidad de cadenas de suministro seguras, normas de cifrado avanzadas y el despliegue de principios de seguridad por diseño en la arquitectura de red. Además, la República de Corea colabora con asociados internacionales y organizaciones de normalización para que sus medidas de seguridad 5G se ajusten a las mejores prácticas mundiales, al tiempo que trabaja en solventar determinadas cuestiones preocupantes de seguridad nacional relacionadas con las posibles amenazas que plantean proveedores extranjeros.
- El marco jurídico y técnico de la **India** para fortalecer la ciberseguridad 5G incluye:
  - directivas de seguridad nacional en el sector de las telecomunicaciones, que garantizan la confianza de la cadena de suministro y la fuente de las telecomunicaciones;
  - pruebas y certificación obligatorias de equipos de telecomunicaciones, que garantizan el cumplimiento de los requisitos de seguridad esenciales de cada función de la red 5G; y
  - condiciones de concesión de licencias a los proveedores de servicios de telecomunicaciones, prevén la realización de auditorías públicas periódicas de seguridad de la infraestructura de telecomunicaciones.

  Para apoyar lo anteriormente expuesto, se han puesto en marcha diversos mecanismos: el National Centre for Communication Security (Centro nacional para la seguridad de las comunicaciones, NCCS), encargado de preparar requisitos/normas de seguridad de las telecomunicaciones, denominados Indian Telecom Security Assurance Requirements (Requisitos para velar por la seguridad de las comunicaciones de la India, ITSAR), y sus laboratorios de pruebas y certificación de seguridad asociados; la creación de Telecom-CSIRT, que es el Equipo de Intervención en caso de Incidentes de Seguridad Informática (EIISI) para el sector de las telecomunicaciones de la India, y varias medidas de gestión del fraude y de protección del consumidor centradas en el ciudadano. En lo que respecta a los protocolos y normas de seguridad como 3GPP, la India tuvo en cuenta las especificaciones propuestas en las normas del sector para la supervisión de la conformidad y otras condiciones de las licencias de telecomunicaciones donde se incluían auditorías de seguridad periódicas en las redes de los proveedores de servicios.
- En los **Emiratos Árabes Unidos** la seguridad de las redes 5G se trabaja mediante una estrategia múltiple que incluye rigurosos cibersimulacros y cursos de formación nacionales, la creación del National Security Operations Center (Centro nacional de operaciones de seguridad, SOC) para la visibilidad y respuesta a las amenazas en tiempo real, y la iniciativa Cyber Pulse, que sensibiliza y forma al personal en estrategias de defensa clave. Se hace hincapié en la colaboración y el intercambio de información con asociados internacionales, proveedores, instituciones académicas y otras partes interesadas para reforzar las medidas de ciberseguridad. Además, existe un marco de ciberseguridad resiliente conforme con normas internacionales como las de la ISO y NIST para garantizar el cumplimiento en todo el sector de las telecomunicaciones. Para fomentar la confianza de los consumidores y las empresas en la seguridad 5G, el país cuenta con políticas, procedimientos y leyes de gobernanza que promueven los principios de seguridad por diseño y las prácticas de seguridad responsables entre los proveedores. Por último, el país ha adoptado un enfoque de ciberseguridad centrado en las personas, la formación, la sensibilización y el apoyo para empoderar a los individuos y las organizaciones en la lucha contra las ciberamenazas, para cimentar así una sólida defensa contra las posibles amenazas en la red 5G.
- **Zimbabwe** está trabajando en la ciberseguridad 5G, centrándose en la reciente importancia que tiene la computación periférica y explorando la adopción de la tecnología Open RAN para ofrecer flexibilidad a los proveedores. Aunque no existe una ley de seguridad 5G como tal, la legislación vigente sobre protección de datos y un documento de gobernanza de la IA en curso sustentan el enfoque del país. Zimbabwe armonizará sus prácticas de seguridad con normas internacionales como la ISO/CEI 27001 y las normas de NIST, para que las nuevas interfaces radioeléctricas 5G cumplan con los protocolos de seguridad establecidos. La Postal and Telecommunications Regulatory Authority of Zimbabwe (Autoridad de regulación de correos y telecomunicaciones de Zimbabwe) vela por el cumplimiento de las directrices de seguridad y sensibiliza al sector sobre el mantenimiento de la integridad de la infraestructura nacional de telecomunicaciones.
- **Kenya** adoptó su hoja de ruta y estrategia para la 5G de comunicaciones móviles en abril de 2022. En la estrategia se reconoce que la seguridad es un aspecto importante de la arquitectura de red 5G. La naturaleza cambiante de los servicios conectados y el aumento significativo previsto en el número y los tipos de dispositivos conectados aumentan la importancia de la privacidad de los datos, la

[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made y https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

protección de estos y la ciberseguridad, lo que incluye la detección de amenazas, la autentificación de los usuarios y el empleo de prácticas operativas adecuadas. La 5G proporciona una mayor seguridad por diseño, integrando requisitos de seguridad mejorados sobre la base de la evolución de la red y adaptando las enseñanzas extraídas de tecnologías anteriores. La Communications Authority of Kenya (Autoridad de comunicaciones de Kenya) adoptó una norma internacional aprobada y elaborada por la UIT y 3GPP para velar por la interoperabilidad y seguridad de los sistemas móviles. El organismo tiene previsto aprovechar los conocimientos especializados de diversas partes interesadas y las prácticas idóneas internacionales en materia de ciberseguridad para elaborar códigos técnicos y aplicar una lista de comprobación mínima normalizada para la evaluación de la seguridad a fin de garantizar que las redes 5G cumplan las normas técnicas más modernas y estén en consonancia con las normas mundiales en relación con la seguridad 5G.

- Tras un amplio examen de los riesgos de ciberseguridad de las redes 5G, la **Unión Europea (UE)** elaboró una herramienta para reducir riesgos[22] con el objetivo de definir un conjunto común de medidas para atenuar los principales riesgos de ciberseguridad 5G y facilitar la selección de medidas prioritarias de mitigación a escala nacional y de la UE. En la Estrategia de Ciberseguridad para la Década Digital se destaca la importancia de salvaguardar la próxima generación de redes móviles de banda ancha y figura un apéndice específico sobre los próximos pasos para la ciberseguridad de las redes 5G[23]. El marco de certificación de la UE comprende la constante evolución de un esquema de certificación de ciberseguridad 5G[24].

Dificultades de implementación y conformidad

Aunque la formulación de políticas es esencial, la atención debería centrarse en la aplicación efectiva. Se necesitan mecanismos de información, conformidad de normas internacionales y medidas prácticas de aplicación para velar por la solidez de la ciberseguridad de las redes 5G. El nuevo marco por el que se introducirán cambios significativos en la seguridad de las redes de telecomunicaciones exigirá un proceso continuo de conformidad para los proveedores y, por lo tanto, un estrecho compromiso con el sector. En el **Reino Unido**, Ofcom adopta un modelo de supervisión en el marco de su régimen de seguridad de las telecomunicaciones y colabora con los equipos técnicos y regulatorios de los proveedores de telecomunicaciones. El regulador considera que la implementación no se limita a las medidas técnicas, sino que requiere un cambio cultural en la forma en que los proveedores de telecomunicaciones conciben la seguridad, exigiéndoles que identifiquen y rindan cuentas por las partes de sus redes y servicios que han subcontratado. Comprometerse al nivel superior y obtener el compromiso y el patrocinio de los Gobiernos, reguladores y el sector es un requisito previo para cualquier éxito.

En **Malasia**, el Gobierno ha aprobado un nuevo proyecto de ley de ciberseguridad por el que se establece un único organismo para gestionar todas las infraestructuras importantes, incluidas las telecomunicaciones. El regulador está elaborando un conjunto de requisitos para que los operadores informen sobre la conformidad relativa a la seguridad. Uno de los operadores del país destacó que la implementación de la nueva política podía suponer dificultades ya que implicaba comunicar el riesgo y elaborar requisitos mínimos de seguridad que requerían tiempo, costo y una concertación intensiva que probablemente incida en los intereses de los accionistas. Para los operadores con accionistas, las estructuras, políticas y regulaciones en materia de seguridad a veces no son congruentes, lo que puede suponer dificultades para los equipos de seguridad, de ahí la necesidad de hacer trabajar a todos los equipos, incluidos los altos directivos, al considerar nuevos marcos de seguridad.

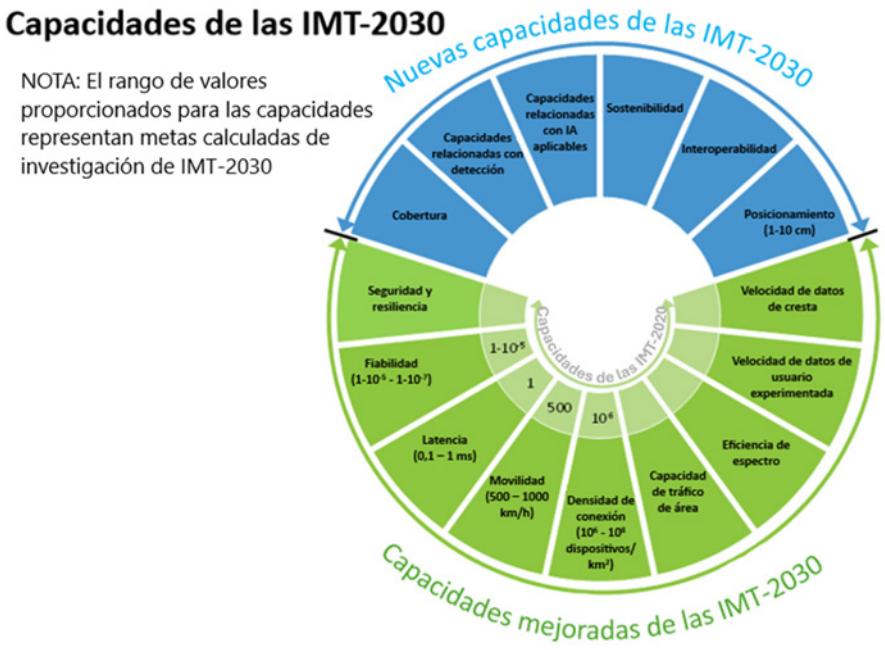
5. La inversión en la educación y capacitación de una fuerza laboral equipada para que maneje mejor las complejidades de la ciberseguridad 5G sigue siendo una gran prioridad

Según Allied Market Research[25], está previsto que el mercado mundial de seguridad 5G alcance los 37 800 USD en 2031. Junto a ello se producirá una creciente demanda de profesionales de la ciberseguridad, en particular aquellos con habilidades especializadas para proteger las redes 5G. Los países, las organizaciones y las instituciones deben priorizar la formación y contratación de personal para velar por el avance de la ciberseguridad 5G. Actualmente es difícil encontrar en la fuerza laboral las habilidades especializadas necesarias y, por otro lado, lograr el equilibrio de género en la contratación. Si la mano de obra no está preparada, la transición a la 5G se ralentizará y será cada vez más difícil. Aunque los países deberían dar prioridad a la formación y la educación a través de programas nacionales, el sector privado también puede explorar programas de formación y mejora de las competencias, ya que para satisfacer las necesidades se requiere la participación del sector en general.

Un ejemplo de país que está encontrando soluciones a los problemas ligados a la fuerza laboral es **Türkiye**, que ha aumentado la inversión en educación y capacitación de la fuerza laboral para poder gestionar las complejidades de la seguridad 5G. En el marco de este compromiso, instituciones clave como Information and Communication Technologies Authority, Middle East Technical University, İhsan Doğramacı Bilkent University y Hacettepe University, junto con los operadores de telecomunicaciones Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş. y Vodafone Telekomünikasyon A.Ş., crearon el sitio 5G Valley Open Test Site. Este sitio sirve como una plataforma fundamental para la investigación, el desarrollo y las pruebas de tecnologías 5G y posteriores, lo que brinda oportunidades para la colaboración académica y del

22 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
23 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
24 https://certification.enisa.europa.eu/index_en
25 https://www.alliedmarketresearch.com/5g-security-market-A12820

Figura 1: Capacidades de las IMT-2030



Fuente: Recomendación UIT-R M.2160

sector. El consejo ejecutivo de 5G Valley, integrado por representantes de las instituciones mencionadas, ha iniciado sus actividades para garantizar la implementación efectiva de esta iniciativa. Al proporcionar una plataforma en la que académicos, investigadores, estudiantes de doctorado y empresas emergentes pueden participar en trabajos relacionados con la 5G y tecnologías posteriores, el sitio de pruebas abierto no solo fomenta la innovación, sino que también contribuye al desarrollo de una fuerza laboral altamente calificada. Esta iniciativa forma parte integrante de la estrategia de Türkiye de priorizar y mejorar la seguridad de las redes 5G mediante inversiones continuas en educación, formación e investigación[26].

6. Más allá de la 5G: marcando el rumbo hacia la ciberseguridad 6G

Aunque la 5G aún se está planificando y desplegando en muchos países y regiones, la investigación y el desarrollo, así como los procesos de normalización, ya han comenzado a mirar más allá de estas redes. Así, a finales de 2023, el Sector de Radiocomunicaciones de la UIT (UIT-R) aprobó el marco y los objetivos generales del desarrollo futuro de las IMT para 2030 y posteriores[27], lo que comercialmente se conoce como 6G.

En el marco se destaca la esperanza de que las IMT-2030 sean un factor de facilitación importante para lograr una mayor seguridad y resiliencia. Se cuenta con que la tecnología sea segura por diseño y tenga la capacidad de seguir funcionando durante un evento perturbador, ya sea natural o provocado por el hombre, y recuperarse rápidamente de él. En el documento también se reafirma que la seguridad y la resiliencia de los sistemas IMT-2030 son fundamentales para alcanzar objetivos sociales y económicos más amplios.

En el contexto de las IMT-2030, el marco define la seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información, como los datos de usuario y la señalización, y la protección de redes, dispositivos y sistemas contra ciberataques como el pirateo, la denegación de servicio distribuida, los ataques de intermediarios, etc. La resiliencia es la capacidad de las redes y sistemas para seguir funcionando correctamente durante y después de una perturbación natural o provocada por el hombre, como la pérdida de una fuente primaria de energía, etc.

Ha quedado claro que ya existe una visión de la 6G y que se ha planteado el inicio de sus procesos de normalización con una firme preocupación por la seguridad y la resiliencia, a diferencia de las primeras fases de diseño de la tecnología 5G, incluso desde el punto de vista de la normalización. La comparación con la perspectiva para las IMT-2020 (conocida comercialmente como 5G), que se aprobó en 2015[28], pone de manifiesto el cambio de planteamiento al reconocerse la necesidad de abordar adecuadamente la ciberseguridad y la ciberresiliencia, como pilar facilitador de la transformación digital y la economía digital.

[26] https://5gtrforum.org.tr/en
[27] Recomendación UIT-R M.2160 disponible en: https://www.itu.int/rec/R-REC-M.2160-0-202311-I/es
[28] Recomendación UIT-R M.2083 disponible en: https://www.itu.int/rec/R-REC-M.2083-0-201509-I/es

Siga los trabajos de la **Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D para el periodo 2022-2025**, Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad.

Sitio web de la Cuestión 3/2 http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx

Listas de correo: d22sg3q2@lists.itu.int . Inscríbase aquí.

Página web de las Comisiones de Estudio del UIT-D: www.itu.int/itu-d/sites/studygroups/

Envíe sus comentarios a: devSG@itu.int ; Tel: +41 22 730 5999

ITUPublicaciones
Publicado en Suiza, Ginebra, 2024

Unión Internacional de Telecomunicaciones
Place des Nations, CH-1211 Ginebra Suiza