ICAT
Instituto de Ciencias Aplicadas y Tecnología

Universidad Nacional Autónoma de México

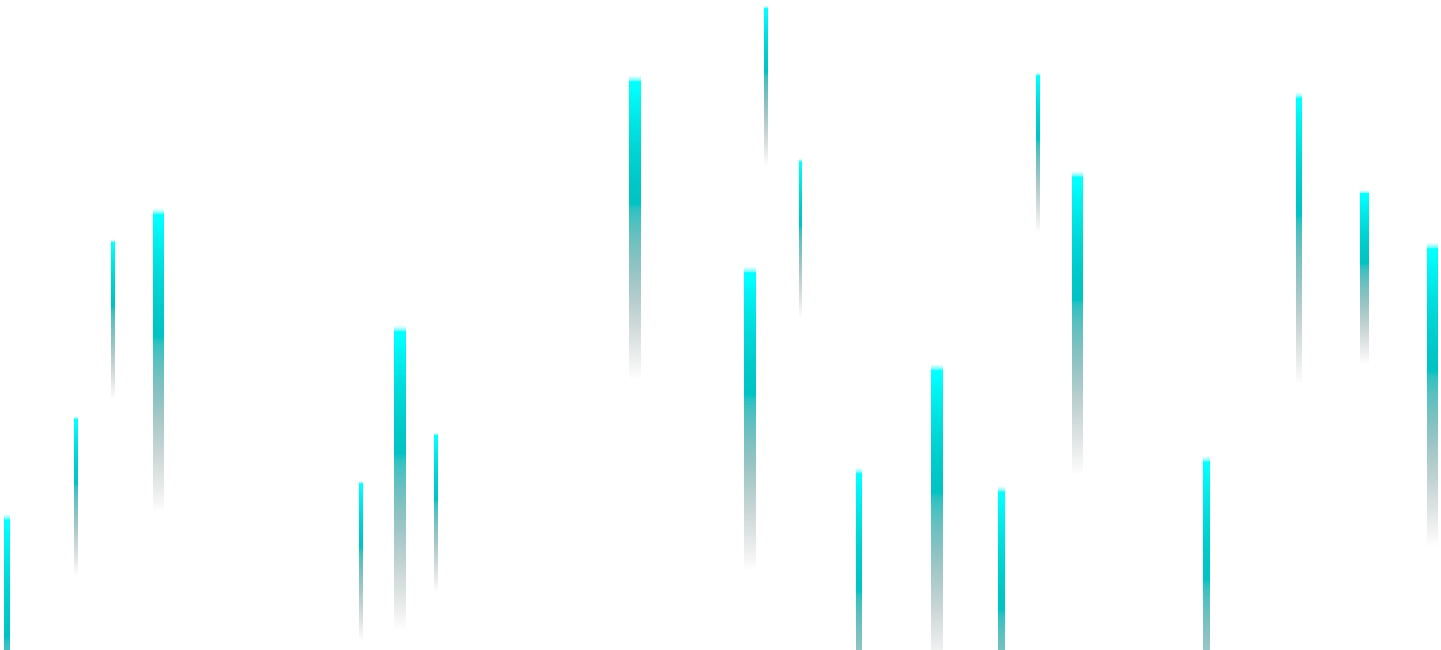
Buenas prácticas de Ciberseguridad:

El caso de la base de conocimiento de ciberseguridad de la comunicación móvil de la GSMA

Buenas prácticas de ciberseguridad: el caso de la base de conocimiento de ciberseguridad de la comunicación móvil de la GSMA

José Luis Solleiro Rebolledo y Rosario Castañón Ibarra

Junio, 2024



La definición más formal y amplia de 5G indica que es el conjunto de normas técnicas que definen el funcionamiento de una red celular, incluyendo las radiofrecuencias que utiliza y otros componentes como los chips informáticos y las antenas que gestionan las señales de radio e intercambio de datos (3GPP, s.f.)[1] (ITU, 2019).

La 5G también se define como la quinta generación de redes móviles, caracterizadas porque proporcionan una conectividad más rápida, segura y eficiente en comparación con las generaciones anteriores. La 5G utiliza tecnologías que permiten ofrecer velocidades de flujo de datos mucho más rápidas, menores tiempos de latencia; y capacidades de conexión masiva de dispositivos en forma simultánea. La importancia de las redes con tecnología de nueva generación radica en las siguientes ventajas:

- **Alta velocidad de transferencia inalámbrica de datos (*enhanced mobile broadband*—eMBB).** Permite descargas y envío de datos desde los dispositivos a la red más rápidas, como la transmisión de video de alta definición sin interrupciones y una experiencia de usuario más fluida en general. Esto es fundamental para el consumo de medios, el trabajo remoto, la educación en línea y muchas otras aplicaciones.

- **Baja y ultra baja latencia en las comunicaciones (*ultra-realiable and low latency communications*—URLLC).** Los dispositivos pueden comunicarse entre sí con tiempos de respuesta ultrarrápidos. Esto es esencial para aplicaciones que requieren una comunicación en tiempo real, como la realidad virtual, los vehículos autónomos, la telesalud y los juegos en línea.

- **Mayor capacidad de conexión simultánea (*massive machine communications*—mMTC).** Esto es fundamental para el crecimiento de la Internet de las cosas, pues significa soportar en forma masiva dentro de un área geográfica que más dispositivos inteligentes, sensores y máquinas pueden conectarse y comunicarse entre sí de manera más eficiente, lo que impulsa la automatización y la eficiencia en una amplia gama de industrias.

Las tres características descritas permiten que la 5G tenga el potencial de transformar industrias enteras como la salud, la manufactura, la logística y el transporte, por mencionar solo algunos ejemplos. Además, se la considera como esencial para la cuarta revolución industrial (I4.0), ya que se encuentran en el centro de la transformación digital al ser el principal canal a través del cual las personas se comunican entre sí y acceden a Internet y a las aplicaciones online (GSMA, 2019).

1 Estas normas técnicas son establecidas por la asociación industrial mundial denominada 3rd Generation Partnership Project (3GPP) la cual también hace recomendaciones a la Unión Internacional de Telecomunicaciones (UIT), ésta adopta y promueve formalmente las normas, para que finalmente se conviertan en la norma de las características 5G en todo el sector tecnológico en general.

El potencial de la tecnología 5G ha motivado un incremento acelerado en su adopción. De acuerdo con la GSMA, en enero de 2023, 223 operadores de 87 mercados habían lanzado servicios móviles 5G; en tanto que para el 2025, se estima que las conexiones totales de 5G superen los 2, 000 millones y hacia finales de esta década se espera que representen más de la mitad del total de conexiones móviles. Aunque la adopción de 5G variará alrededor del mundo, con cifras que irán desde el 85% en algunos mercados hasta menos del 20% en el África subsahariana (Castells, Joiner y Adamowicz, 2023)[2].

"Hacia abril de 2024, 29 operadores de 10 países de América Latina ya habían lanzado servicios 5G comerciales. Muchos otros tienen planificado hacerlo en los próximos años. Para los operadores pioneros, la adopción de 5G se acerca velozmente a niveles de mercado masivos. Por ejemplo, Movistar Chile reveló en el MWC Barcelona 2024 que había superado el millón y medio de clientes 5G, equivalentes a casi un quinto de sus conexiones móviles totales" (GSMA, 2024: 22).

En el caso de México, el despliegue de 5G comenzó en febrero de 2022 en las 18 principales ciudades, gracias a inversiones en infraestructura por parte de los dos principales operadores Telcel y AT&T que facilitaron que el país tenga una de las tasas de adopción más altas de América Latina. Actualmente, en México hay 6.6 millones de suscriptores en 125 ciudades. Fuentes como el Informe de Movilidad de Ericsson (Ericsson, 2024) estiman que para finales de 2024 habrá una aceleración en la adopción de la red 5G, alcanzando hasta el 51% de todas las suscripciones móviles.

2 Para el caso de América Latina, en marzo de 2023, la GSMA identificó que 8 países habían lanzado servicios 5G comerciales; asimismo, estimó que la adopción de 5G superará la de 2G en 2024; la de 3G en 2026 y la de 4G en 2029. Para 2030 la tecnología 5G representará casi el 60% del total de conexiones móviles en América Latina.

No obstante, lo acelerado de la incorporación de las redes 5G, en lo referente al tema de ciberseguridad, se reconoce que éstas introducen nuevos factores a considerar, debido a su naturaleza avanzada y a que incorpora elementos como la intensificación de servicios en la nube y las aplicaciones en industrias verticales, lo cual aumenta la complejidad de las redes. Algunos problemas potenciales que requieren respuestas específicas son los siguientes:

1. **Aumento de superficie de ataque.** Con más dispositivos conectados y una mayor cantidad de datos transmitidos a través de la red 5G, la superficie de ataque para los *hackers* se amplía significativamente. Cada dispositivo conectado representa un posible punto de entrada para los ciberataques.

2. **Vulnerabilidades de seguridad en el protocolo 5G[3].** Aunque el estándar 5G incluye mejoras significativas de seguridad con respecto a las generaciones anteriores, como la encriptación mejorada y la autenticación más sólida, la industria reconoce que es normal que pueden existir vulnerabilidades desconocidas en los protocolos de interconexión que podrían ser explotadas por los actores maliciosos.

3. **Amenazas de IoT.** La creciente adopción generalizada de dispositivos de Internet de las cosas (IoT) en las redes móviles introduce nuevos riesgos de seguridad. Muchos de estos dispositivos tienen medidas de seguridad limitadas por diseño o por tipo de aplicación y pueden ser comprometidos fácilmente, lo que podría usarse como vector de ataque para atacar otros dispositivos en la red.

4. **Riesgos de privacidad.** Con la mayor adopción de dispositivos de IoT que sirven para recopilar y transmitir grandes cantidades de datos en tiempo real, incluyendo datos personales sensibles, existe el riesgo de que se produzcan violaciones de privacidad, si estos datos caen en manos equivocadas o son mal utilizados.

5. **Amenazas de la red de acceso.** Los nodos de acceso a la red móvil, como las estaciones base y los puntos de acceso seguirán siendo un vector de ataque, son vulnerables a ataques físicos y de red. Si un atacante compromete uno de estos nodos, podría interrumpir o manipular el tráfico de la red.

6. **Amenazas de software y firmware.** Los dispositivos y la creciente adopción y uso de aplicaciones, como teléfonos inteligentes y equipos de red, pueden verse comprometidos si tienen vulnerabilidades de software o firmware que pueden ser explotadas por los atacantes.

7. **Amenazas de denegación de servicio (DoS).** Las redes móviles son susceptibles a ataques de denegación de servicio que pueden sobrecargar la red con tráfico malicioso, lo que resulta en una interrupción del servicio para los usuarios legítimos.

8. **Intercepción de datos.** Dado que la tecnología de redes móviles, por su naturaleza de acceso inalámbrico que permite velocidades de transferencia de datos mucho más rápidas, existe el riesgo de que los datos transmitidos a través de la red de acceso puedan ser interceptados si no se implementan medidas de seguridad adecuadas, como la encriptación de extremo a extremo.

3 El protocolo de despliegue de 5G ha implicado dos fases. Por un lado, es necesario actualizar los equipos de radio que comunica la red con los terminales compatibles con 5G. Por otro, hay que cambiar la infraestructura de la red actual de 4G para convertirla en 5G. En la primera fase se instalan los equipos de radio en las estaciones base, creando lo que se conoce como **5G NSA** (*Non Standalone* o 5G no independiente). El modo NSA permite que la red 5G comparta infraestructura con la red 4G. En el modo **5G SA** (*Standalone* o independiente), la infraestructura de red será completamente de tipo 5G.

Por otro lado, como respuesta a estos riesgos potenciales, el 3GPP (3rd Generation Partnership Project-Proyecto Asociación de Tercera Generación) ha analizado las amenazas y riesgos de las redes móviles y las ha clasificado en 17 áreas de seguridad: Arquitectura de seguridad, autenticación, contexto de seguridad y gestión de claves, seguridad de la red de acceso radioeléctrico (RAN), seguridad dentro de NG-UE, autorización, privacidad de las suscripciones, seguridad de segmentación de red, seguridad de retransmisión, seguridad de dominio de red, visibilidad y configuración de la seguridad, aprovisionamiento de credenciales, interfuncionamiento y migración, small data, seguridad de difusión/multidifusión, y seguridad de gestión (Cheang, Gong y Yang, 2021).

Hoy se tiene claro que muchas de las amenazas potenciales para las redes móviles se derivan de la ausencia o falta de cohesión y normalización entre las distintas plataformas. Por ello, según el Foro Económico Mundial, una sólida cooperación entre las múltiples partes interesadas (que incluya a reguladores y responsables de políticas públicas, asociaciones empresariales y alianzas internacionales, proveedores de servicios y tecnología, y organizaciones de colaboración público-privada) tiene un beneficio potencial de enorme valor social y económico, con un valor agregado estimado de 13.2 mil millones de dólares para 2035 en sectores industriales como la fabricación, los servicios financieros, la salud, el transporte, el comercio minorista, la energía y el ocio.

Los distintos análisis en torno a la seguridad y relevancia de las tecnologías móviles han llegado a la conclusión de que encarar los riesgos requiere una combinación de medidas técnicas, como la implementación de protocolos de seguridad sólidos, el monitoreo continuo de la red, y la educación de

los usuarios sobre prácticas seguras de uso de la red. Además, la cooperación entre gobiernos, proveedores de servicios de telecomunicaciones y fabricantes de equipos será crucial para garantizar la seguridad de las redes móviles, por lo que en ese sentido se habla de mejorar la seguridad del ecosistema digital desde los usuarios finales, las autoridades reguladoras, los operadores, los proveedores de tecnología y los organismos profesionales de normalización o ciberseguridad, para construir un ecosistema de cooperación abierto y transparente dirigido por la industria, con el fin de garantizar la existencia de una base común del conjunto de controles de seguridad y la seguridad de la cadena de suministro.

Al respecto, la GSMA, la organización global de la industria de los operadores de redes móviles, fabricantes y desarrolladores de aplicaciones, publicó en mayo de 2021 la ***Base de conocimientos sobre ciberseguridad de la comunicación móvil*** (MCKB, por sus siglas en inglés). El objetivo de la MCKB es ayudar a las partes interesadas a gestionar los riesgos en el ecosistema de redes móviles a través del entendimiento, mapeo y mitigación de las amenazas actuales y futuras de forma objetiva, rápida y eficaz (para referencia ir a https://www.gsma.com/security/mobile-cybersecurity-knowledge-base/).

La MCKB es también un complemento a una serie de publicaciones relacionadas con la ciberseguridad en Europa, tales como la directiva NIS, la *Ley de Ciberseguridad de la UE*, la *Evaluación Coordinada de Riesgos de la UE de la Ciberseguridad de las Redes 5G*, el *Panorama de Amenazas de ENISA para las redes 5G*, el *Esquema de Garantía de Seguridad de Equipos de Red* (NESAS[4]) (Cibersecurity Malaysia, 2022). De igual manera, la MCKB complementa prácticas de seguridad promovidas por la Unión Europea, en virtud de que la GSMA ha desarrollado un sistema de garantía de seguridad para los equipos de red, ha propuesto un marco de seguridad y ha establecido un centro de ciber-información para el sector de las telecomunicaciones.

La MCKB es la contribución de la industria móvil a los esfuerzos de ENISA, la Agencia de Ciberseguridad de la Unión Europea, en favor de un enfoque común basado en acciones verificables y estandarizadas.

4 Los fabricantes de equipos utilizan las normas NESAS para orientar el diseño de un proceso completo de desarrollo de productos con medidas de seguridad y fabrican equipos con características y elementos de seguridad estándar para su uso en redes de telecomunicaciones.

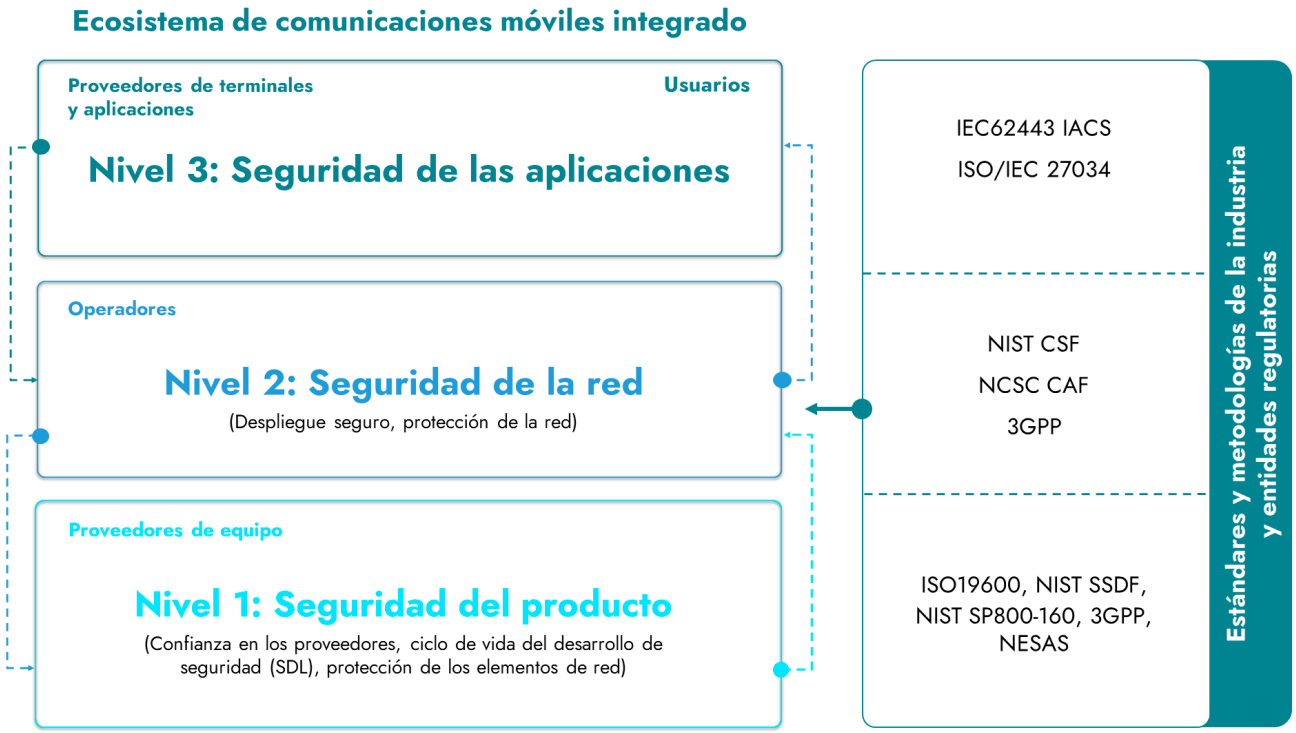
En la construcción de la MCKB, la GSMA ha realizado un análisis exhaustivo de las amenazas y las ha relacionado con controles de seguridad adecuados y eficaces. Tal análisis permite proporcionar información esencial para la estrategia de gestión de riesgos de las partes interesadas, así como orientaciones sobre mejores prácticas de ciberseguridad.

La iniciativa de la MCKB también es relevante por el alcance universal que tiene la GSMA. Ésta representa los intereses de los operadores móviles alrededor del mundo; abarca 220 países y reúne a casi 800 operadoras móviles, 200 empresas del ecosistema móvil incluyendo a fabricantes de teléfonos, empresas de software, proveedores de equipamiento, empresas de internet y medios de comunicación y empresas de entretenimiento. Los miembros de la GSMA representan a más de cinco mil millones de conexiones, lo cual representa la base de experiencia y evidencias más robusta que se pueda encontrar (GSMA, s.f.a.).

La base de conocimientos sobre ciberseguridad de la GSMA propone el concepto de seguridad con responsabilidad compartida y controles de seguridad básicos fundamentados en las amenazas típicas de las redes móviles y las soluciones de seguridad relevantes. Asimismo, la MCKB presenta una base de datos con casos reales donde la ciberseguridad se ha visto comprometida y la forma en que han sido resueltos, con la finalidad de que los miembros de la GSMA puedan tener elementos de soporte para solucionar problemas específicos (ICAT-UNAM, 2024).

Con respecto a la seguridad compartida, la GSMA contempla un modelo de tres capas que relaciona a todos los integrantes de la industria de redes móviles (los proveedores de interconexión, los vendedores de equipos, los proveedores de aplicaciones) (figura 1); asimismo, se identifican las normativas y/o metodologías de gestión de la seguridad aplicables a cada una de ellas elaboradas por diversas organizaciones, gobiernos y agencias reguladoras.

Figura 1. Modelo de seguridad compartida: hacia un ecosistema de comunicaciones móviles integrado



Fuente: adaptada de GSMA (s.f.b.).

El primer nivel de seguridad se refiere a los equipos de red; esta responsabilidad de los fabricantes, y la MCKB proporciona una base para evaluar si los equipos y componentes de red se han diseñado e implementado de conformidad con los requisitos de seguridad, en particular con lo establecido en NESAS.

NESAS. *Esquema de Garantía de la Seguridad de Equipo (GSMA Network Equipment Security Assurance Scheme). La Asociación para el Sistema Global de Comunicación Móvil (GSMA) facilita protocolos y estándares para la tecnología móvil, entre ellos su base de conocimientos para ciberseguridad que es seguida por los principales actores de la industria a nivel global. NESAS aporta un marco para garantizar la seguridad, lo cual eleva la confiabilidad y la confianza en el equipamiento de redes. El objetivo del esquema es auditar y examinar a los proveedores de equipo y sus productos, de acuerdo con una línea de base que constituye el estándar mínimo a cumplir, de tal manera que los operadores de redes móviles puedan verificar la conformidad de los equipos con el estándar deseado. También se cuenta con un protocolo de pruebas, conocido como Especificaciones de garantía de Seguridad (SCAS, por sus siglas en inglés), mediante las cuales los procesos de desarrollo y gestión del ciclo de vida de productos son auditados, a partir de pruebas de seguridad definidas por el 3GPP (3rd Generation Partnership Project - Proyecto Asociación de Tercera Generación)[5]. Las pruebas relativas a esos requisitos permiten medir objetivamente el nivel de seguridad de los productos de la red. Este esquema ha sido definido por expertos de la industria trabajando con GSMA y la 3GPP que es una colaboración de grupos de asociaciones de telecomunicaciones, para asentar las especificaciones de un sistema global de comunicaciones de tercera generación.*

La mayoría de los proveedores globales de equipo de telecomunicaciones se ha sometido a las auditorías de NESAS y SCAS, con lo cual aseguran la confiabilidad, la cual se traduce en confianza que se construye sobre hechos verificables.

5 Las especificaciones incluyen tecnologías para las comunicaciones por celular (equipo de acceso por señal de radio, capacidades de red y servicio) que aportan una descripción completa de los sistemas para comunicaciones móviles (https://www.3gpp.org/about-us).

El segundo nivel del modelo (***"Seguridad de la Red"***) es gestionado por los operadores de redes móviles públicas o redes inalámbricas privadas. Se centra en la evaluación de riesgos de todos los componentes y arquitectura de la red para garantizar una gestión eficaz de las amenazas a la seguridad. Existen especificaciones y metodologías maduras de referencia en el sector, por ejemplo, la metodología para Identificar, Proteger, Detectar, Responder y Recuperar (IPDRR) definida por el Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST-CSF) que puede ayudar a los operadores a abordar sistemáticamente los riesgos de ciberseguridad.

Los operadores de las redes móviles que prestan servicios de acceso a internet móvil, telecomunicaciones, y otros a los usuarios y, que estos usuarios usan para las aplicaciones que instalan en sus dispositivos, tienen la responsabilidad sobre la seguridad en la transmisión o transferencia de sus datos y su protección, incluyendo salvaguardar la privacidad. Es importante tener en cuenta que los operadores tienen la capacidad y se encargan de controlar sus propias redes y, por eso, son los únicos que tienen acceso a todos los nodos que la forman, además de que son quienes regulan el acceso de usuarios, así como de los diversos proveedores de equipo (Huawei, Ericsson, Nokia, etc.). A los operadores les corresponde este nivel de control de sus redes, puede afirmarse que son los que tienen la gobernanza sobre la red, los flujos de datos y su correspondiente seguridad.

El tercer nivel del modelo (***"Seguridad de las aplicaciones"***) se orienta a los dispositivos móviles y a las aplicaciones que instalan y usan en ellos los usuarios finales, incluyendo los relativos a las industrias. Esta capa de seguridad requiere la colaboración entre operadores, proveedores de dispositivos y desarrolladores/proveedores de aplicaciones para garantizar la seguridad por diseño de sus aplicaciones que utilizan las redes móviles, así como de los usuarios que disfrutan de los servicios que dichas aplicaciones soportan.

La MCKB está organizada por documentos que identifican las amenazas y controles de seguridad correspondientes para cada escenario. Para fácil referencia de los **controles de ciberseguridad,** la MCKB establece **una Línea de base de controles de seguridad,** que se encuentra en el documento FS.31 (versión 3.0 de septiembre de 2023); este documento esboza un conjunto específico de controles de seguridad que la industria de las telecomunicaciones móviles debería considerar desplegar.

La línea base de controles de ciberseguridad se refiere a controles de referencia (controles mínimos) y su intención es que sirvan de base para que los operadores comparen sus controles internos con los de referencia y establezcan si han implantado controles de seguridad más o menos seguros que los enumerados en el documento FS.31 y, en función de ello, puedan tomar acciones. Por supuesto que si los controles de los operadores requieren mayor seguridad, la recomendación es sumar y complementar la postura de seguridad.

Es relevante mencionar que los controles propuestos en la MCKB son independientes de la legislación y la reglamentación de los mercados locales, aunque pueden estar respaldados por ellas. No sustituyen ni anulan la normativa o legislación local de ningún territorio. Su objetivo es mejorar y complementar los niveles de seguridad en el sector de las telecomunicaciones móviles.

La línea base de controles de ciberseguridad es una herramienta que ayuda a evaluar la madurez de estrategias de ciberseguridad, mediante una escala de cinco niveles crecientes de madurez. La intención no es que toda organización se proponga como objetivo de madurez el Nivel 5 para todos sus controles, sino que pueda establecer lo que es apropiado y proporcionado para cada uno de esos controles dentro de cada organización particular.

Cuadro 1. Niveles de madurez establecidos por la línea base de controles de ciberseguridad

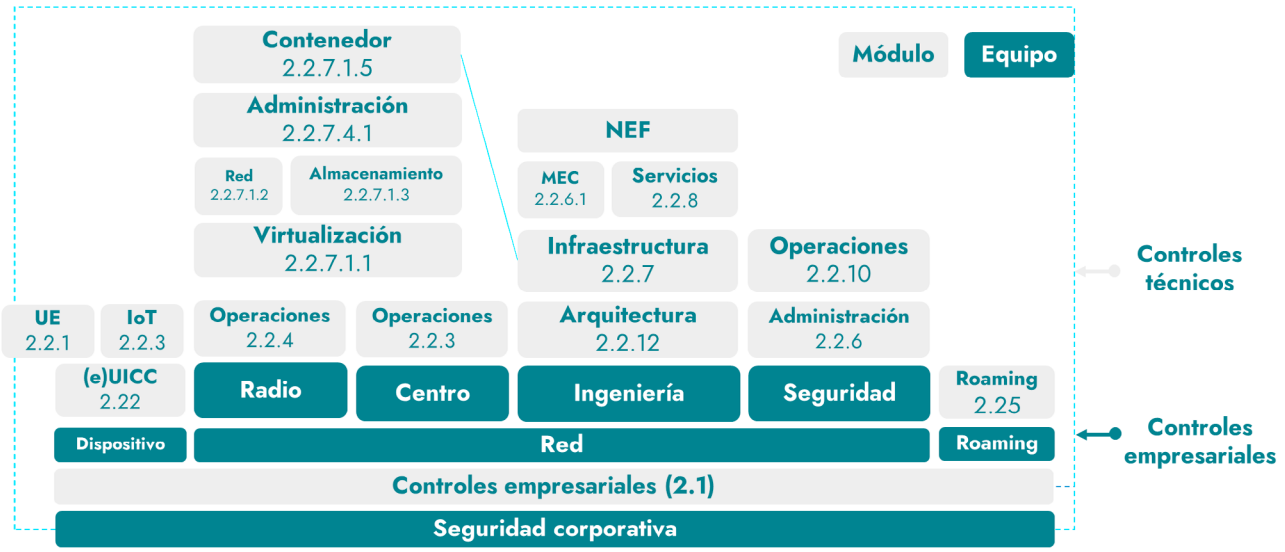
Nivel de madurez	Definición
No aplica	El objetivo básico de control de seguridad de la GSMA no se aplica al operador.
Nivel 0: Ninguno	Control no presente y aún no ha sido considerado para su implementación por el operador.
Nivel 1: Inicial	El operador ha estudiado la posibilidad de aplicar el control y ha realizado un análisis de las deficiencias del control en relación con la política y la práctica actuales. Puede haber una aplicación *ad hoc* o localizada del control, pero el control no está respaldado estratégicamente. Se ha preparado una hoja de ruta de mejora del control para aumentar el nivel de madurez hasta un nivel de madurez objetivo aplicable.
Nivel 2: Reproducible	El control ha empezado a adoptarse en las políticas y prácticas del operador. Se ha avanzado en su aplicación y se incluye en un programa de trabajo detallado que está en curso. Los avances son revisados periódicamente por un comité del programa y, cuando se aplica el control, se hace de forma coherente y repetible.
Nivel 3: Definido	El control se ha adoptado plenamente en las políticas y prácticas del operador. El control ha empezado a integrarse en los procesos de gobernanza y gestión, pero aún no se ha completado. Los planes de dotación de recursos y formación cubren la supervisión del control y han empezado a aplicarse.
Nivel 4: Gestionado	Los procesos de gobernanza y gestión que supervisan y hacen funcionar el control ya están plenamente implantados y cuentan con una amplia dotación de personal debidamente cualificado y formado. Se han elaborado planes para supervisar la eficacia del control y poner en marcha un proceso de revisión y mejora periódicas del mismo. Esto incluye tener en cuenta la información sobre la eficacia del control procedente de las investigaciones y revisiones de incidentes.
Nivel 5: Optimizado	Los procesos de revisión/mejora del control están integrados y funcionan eficazmente (este nivel de madurez no debe reclamarse hasta que dichos procesos hayan realizado varios ciclos de revisión, por ejemplo, seis meses o más). La supervisión del control ha pasado del modo programa a la situación habitual.

Fuente: GSMA (2023).

A nivel operativo, la línea de base de controles de seguridad los divide en controles empresariales y controles técnicos. **Los controles de gobernanza empresariales** se relacionan con la forma en que la empresa gestiona la seguridad; no son necesariamente de naturaleza técnica y pueden referirse a procedimientos de información o comunicación que son esenciales para que un operador respalde los objetivos de negocio.

Los **controles técnicos** se refieren a las tecnologías que ayudarán a crear un ambiente más resiliente para cuidar la ciberseguridad; cada uno de los controles técnicos es necesario para garantizar la seguridad de una red de telecomunicaciones móviles.

Figura 2. Controles empresariales y técnicos de la línea de base



Controles técnicos
Controles de equipos de usuario y equipos móviles
Controles de gestión de la UICC (Universal Integrated Circuit Card)
Controles de Internet de las cosas
Controles de la red de radiocomunicaciones
Controles de interconexión
Controles de gestión de la red principal
Controles de operación de la red
Controles de Seguridad de la operación

Controles empresariales	
BC-001	Compromiso de la alta Dirección
BC-002	Reconocimiento formal de la seguridad
BC-003	Políticas organizacionales
BC-004	Gobernanza, riesgo y cumplimiento
BC-005	Seguridad por diseño
BC-006	Evaluación de protección de datos
BC-007	Implementación del ciclo de vida de desarrollo de software (SDLS)
BC-008	Gestión de la continuidad del negocio
BC-009	Controles de seguridad física
BC-010	Controles de cadena de suministro
BC-011	Controles de subcontratación
BC-012	Controles de desmantelamiento de equipos
BC-013	Protección de equipos
BC-014	Ciberseguridad alineada a normas internacionales
BC-015	Objetivos de Ciberresiliencia

Fuente: adaptada de GSMA (2023).

La MCKB expone, para ambos tipos de controles, el objetivo que debe alcanzarse, mediante la aplicación de cada conjunto de controles y la descripción de la solución (conjunto de controles y normas aplicables, cuando existan). En el tema de controles empresariales, la línea base de ciberseguridad se compone de 15 controles, los cuales se muestran en el cuadro 2.

Cuadro 2. Controles empresariales considerados en la línea base de controles de seguridad de la MCKB

Control	Objetivo
BC-001	**Compromiso a nivel de la alta Dirección:** cuando las organizaciones no reconocen la seguridad a nivel directivo, es probable que exista una brecha en la forma en que la organización comprende su éxito, su posición ante el riesgo, sus prioridades y su inversión futura en programas. Esta brecha introduce riesgos innecesarios de seguridad y fraude.
BC-002	Las organizaciones **reconocen de manera formal la seguridad** como una responsabilidad, los CISO (Chief Information Security Officer) suelen desempeñar esta función. Alternativamente, puede ser cualquier persona de alto nivel, su papel debe ser capaz de influir y dirigir la inversión y el cambio a nivel empresarial.
BC-003	**Políticas organizacionales[6]:** conjunto de normas que la organización debe respetar. Se elaborarán políticas específicas en relación con la seguridad, que deberán ajustarse a la estrategia y los principios generales de seguridad de la organización.
BC0 04	**La gobernanza, el riesgo y el cumplimiento** son tres funciones que se complementan entre sí, proporcionando procesos de información para detallar el progreso operativo frente a los requisitos estratégicos. La gobernanza debe ajustarse a la política de la organización; los informes se comparten con la alta dirección para explicar el éxito de todo el programa de seguridad.
BC-005	**Evaluación de seguridad** de los proyectos para confirmar que son seguros desde su diseño.
BC-006	**Evaluación de protección de datos/privacidad** de los proyectos. Esta evaluación debe ajustarse a la política local, la normativa del sector y la legislación pertinente. En ella se basarán los principios locales de gestión de datos.

Continúa

6 Para las políticas organizacionales, la MCKB también ha diseñado lineamientos generales. Estos se muestran al final del documento.

BC-007	Implementación del **ciclo de vida de desarrollo de software seguro** (SDLC): debe incluir etapas de control de calidad, con revisión del código a nivel de módulo y de sistema, incluyendo pruebas estáticas y dinámicas. La elección del lenguaje de código tiene en cuenta aspectos de seguridad como la seguridad de tipos y las funciones vulnerables.
BC-008	**La Gestión de la Continuidad de Negocio** (BCM) mejora la resistencia de la organización. Desarrolla la capacidad de la organización para detectar, prevenir, minimizar y afrontar el impacto de sucesos perjudiciales. Tras un incidente, el plan de gestión de la continuidad de las actividades permitirá proseguir las actividades críticas de la organización. A largo plazo, ayudará a la empresa a recuperarse y volver a la normalidad.
BC-009	**Controles de seguridad física:** la estrategia de seguridad de un operador debe tener en cuenta los controles y procedimientos de seguridad física de forma holística.
BC-010	Los operadores deben implantar **controles eficaces de la cadena de suministro y proveeduría** para garantizar que los servicios que operan y prestan cumplen los requisitos legales y la gestión de las amenazas de la cadena de suministro.
BC-011	Los operadores deben implantar **controles para la subcontratación** de servicios, de tal forma que se garantice la seguridad de la información.
BC-012	El **desmantelamiento de los equipos** debe tener en cuenta controles seguros de saneamiento o eliminación para evitar el riesgo de fugas de datos.
BC-013	**Los productos (HW/SW) están protegidos** contra las amenazas internas y/o externas.
BC-014	Los operadores deben alinear sus prácticas de ciberseguridad a las **normas reconocidas** internacionalmente.
BC-015	Los operadores deben definir **objetivos estratégicos claros de cibe-resiliencia** e incorporar estos objetivos al marco de gestión de riesgos de la organización.

Fuente: adaptado de GSMA (2023).

Con relación a los controles tecnológicos, la línea de base de ciberseguridad incluye los mostrados en la figura 2. La línea base de controles de ciberseguridad se da como resultado de una revisión exhaustiva de las amenazas y soluciones aplicadas, que se encuentran en los siguientes documentos que están disponibles en la MCKB.

Cuadro 3. Amenazas de la 5G contempladas en la MCKB

Documento	Propósito
FS.30 Manual de seguridad	Describe una serie de amenazas conocidas a las que podrían estar expuestas las redes móviles y los servicios que prestan. El documento utiliza una taxonomía común para describir cada amenaza, su impacto, opciones de mitigación y referencias para ayudar a una mayor comprensión.
FS.33 Análisis de amenazas de NFV	Esboza una visión global de las amenazas relacionadas con la NFV y las infraestructuras y plataformas de alojamiento subyacentes. Este documento hace hincapié en la seguridad, directa e indirecta, de los entornos y funciones de la NFV.
FS.37 Seguridad de GTP-U	Proporciona recomendaciones para que los operadores de redes móviles detecten y prevengan los ataques que utilizan datos del plano GTP-U en la red, los servicios y las aplicaciones, y también contiene directrices sobre cómo desplegar lógicamente las capacidades de seguridad (interfaces específicas) y los modos de despliegue.
FS.57 Principios de Mobile Threat Intelligence Framework (MoTIF)	Especifica un marco para describir, de forma estructurada, cómo los adversarios atacan y utilizan las redes móviles, basándose en las tácticas, técnicas y procedimientos (TTP) que emplean.

Fuente: elaboración propia con base en GSMA (s.f.c.).

En lo referente a las soluciones, la MCKB ha elaborado las siguientes ayudas:

Cuadro 4. Guía de soluciones a las amenazas de la 5G contempladas en la MCKB

Documento	Breve descripción
FS.34 Gestión clave para la seguridad de 4G y 5G Inter -PLMN	Describe el proceso de gestión de claves, es decir, el intercambio de certificados y materiales clave que se utilizan entre las partes de la interconexión para proteger la comunicación de señalización.
FS.35 Security Guía para el despliegue de algoritmos	Describe los algoritmos de autenticación, privacidad y protección de integridad GSM, UMTS, LTE y 5G que se utilizan en dispositivos y redes celulares. Proporciona orientación y recomendaciones sobre las mejores opciones de despliegue.
FS.36 5G Seguridad de interconexión	Describe los posibles ataques basados en la interconexión 5G contra las redes móviles y sus clientes, y las contramedidas para esos ataques. Ayuda a comprender los riesgos potenciales, las amenazas y las contramedidas relacionadas con la seguridad de la interconexión 5G a los miembros de la GSMA.
FS.39 5G Guía de riesgos de fraude	Describe los ataques por fraude potenciales contra las redes 5G y los servicios que las soportan; asimismo se recomiendan las medidas para contrarrestar los ataques y mitigar los riesgos.
FS.40 5G Guía de Seguridad	Contiene una visión general de los aspectos de seguridad y las capacidades de las redes 5G. El documento sirve como un recurso educacional que describe las mejoras.

Fuente: elaboración propia con base en GSMA (s.f.c.).

De manera adicional a la consulta de estos documentos, la MCKB realiza una clasificación temática muy completa de las amenazas y las asocia con elementos clave tales como: su descripción, metodología del ataque, el impacto potencial; las medidas de mitigación asociándolas a los responsables; y la referencia a normas internacionales, cuando así se determine. La figura 3 muestra un ejemplo del tipo de información que se despliega.

Figura 3. Ejemplo de información relacionada con las amenazas que se despliega en la MCKB

Guías contenidas en la MCBK para gestionar la ciberseguridad de redes móviles

Análisis exhaustivo y estructurado de las amenazas para las redes móviles

Campos	Amenazas
Red Central	Ataque DoS contra la red central
	Espionaje de llamadas de voz
	Vigilancia de las comunicaciones móviles
	Espionaje de mensajes SMS
	Colecta de registros de llamadas
Nube	Uso indebido de máquinas virtuales
	Ataques DDoS contra la computación de borde de acceso múltiple (MEC)
	Uso indebido de las interfaces de programación de aplicaciones de MEC
	Acceso no autorizado al plano de administración de las secciones
	Network slice resource pre-emption
	Robo y manipulación de datos de la red
Interconexión	Ataque de suplantación de identidad para interconexiones en itinerancia
	Violación de datos de localización
	Espionaje/interferencias de datos en las interconexiones
	Interrupción de HLR (Home Location Register)
	Re-enrutamiento de SMS a2P
	SS7 RCE y tunelización
Redes de operadores y fabricantes de equipo	Robo de identidad
	Uso indebido de las debilidades de la configuración de red
	Alteración de registros

Métodos detallados de ataque y descripción de su impacto

Ataque DoS contra la red central	
Descripción de la amenaza	Un atacante inicia un ataque DoS contra la red central a través de equipos de usuario, interfaces de itinerancia, aplicaciones de terceros, Internet, estaciones base y dispositivos de transporte que consumen recursos de red y hacen que los servicios no estén disponibles.
Métodos de ataque	En un ataque DDoS, el tráfico entrante que inunda la red víctima procede de distintas fuentes. Los mensajes DDoS pueden crearse en una laptop conectada a la red central del operador víctima y enviarse a través de las interfaces N1/N32/N9/N6/N2/N3 El atacante puede enviar una gran cantidad de mensajes de señalización y de datos de usuario hacia los nodos de la red en un tiempo corto. Estos mensajes pueden desencadenar un tráfico que supere la capacidad de procesamiento de los dispositivos de red. Como resultado, se ocupan demasiados recursos de la red y no están disponibles para un servicio normal.
Impacto potencial	La indisponibilidad de los servicios normales de la red principal es un incidente crítico que impide a los clientes acceder o utilizar los servicios desde casa o en itinerancia. Los clientes afectados pueden ponerse en contacto con el servicio de atención al cliente, que podría verse desbordado. Además, estos ataques causan graves pérdidas de reputación al operador de red.

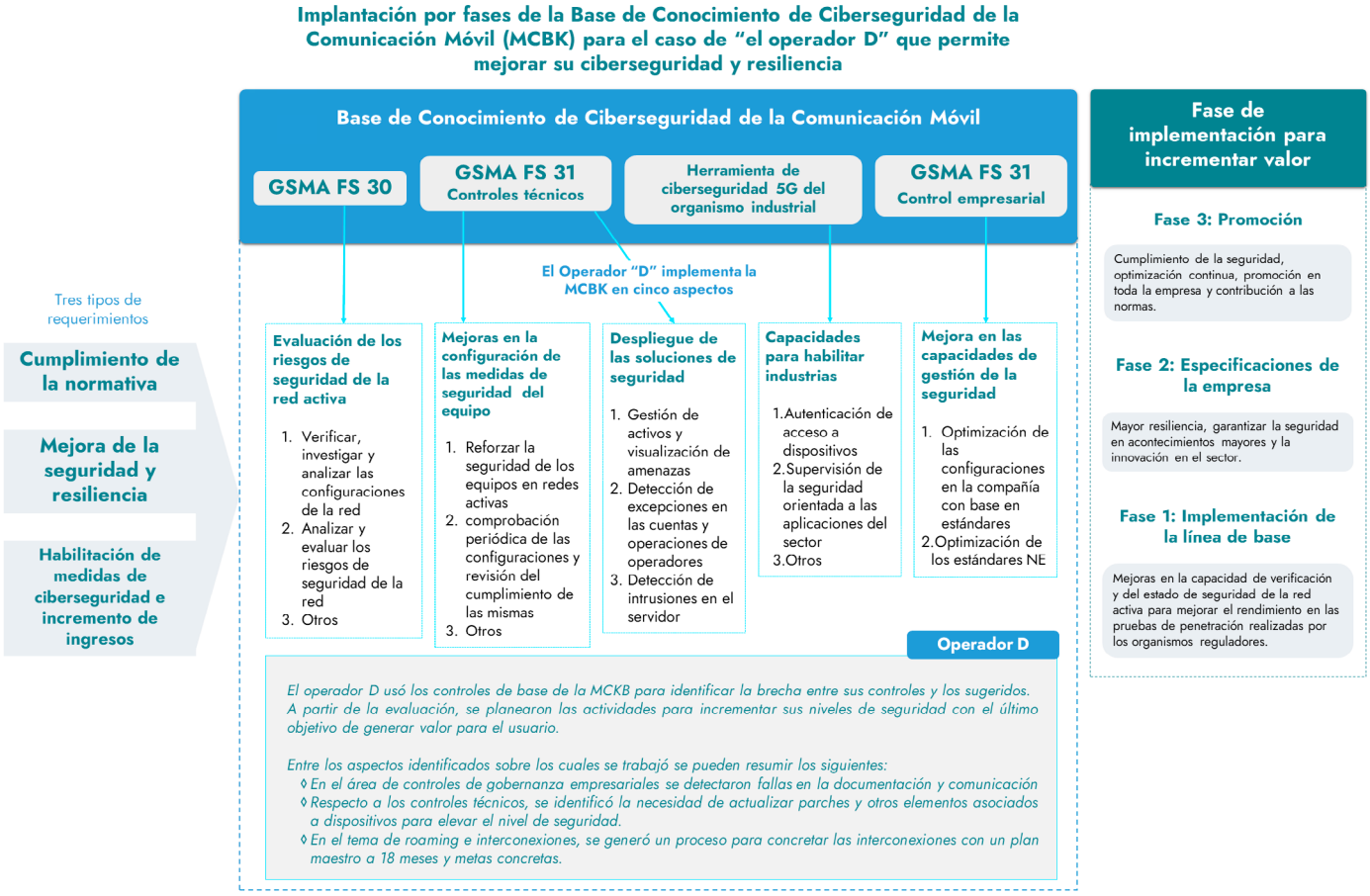
Medidas de mitigación recomendadas para los diferentes actores

Ataque DoS contra la red central		
Medidas de mitigación	Proveedores del servicio	Garantizar la seguridad de las aplicaciones y supervisar el comportamiento de los servidores de aplicaciones para evitar que los piratas informáticos controlen las aplicaciones para iniciar ataques DDoS.
	Operador	Solicite el cumplimiento del NESAS para garantizar que los equipos tienen un nivel de seguridad básico antes de su entrega. Despliegue de dispositivos anti_DDoS entre gnodebs y la red central y entre la red central e Internet. Despliegue de proxies de protección del borde de seguridad y cortafuegos de señalización en el plano de control de la red central para filtrar los paquetes de señalización de ataque procedentes de redes itinerantes. Habilitar mecanismos de control de flujo y filtrado de patrones de ataque DDoS en los dispositivos de la red central.
	Proveedor de equipo	Proveer mecanismos de control de flujo y filtrado de patrones de ataque DDoS en los dispositivos de la red central y/o equipos anti DDoS. Proporcionar la función SEPP basada en las especificaciones 3GPP para filtrar la señalización anómala en las interfaces de itinerancia.
Referencias	Rauters Staff "Vodafone hit by three hour mobile network outage in Germany" Reuter, 23 nov 2020. 3GPP 33.821	

Fuente: GSMA (s.f.c.).

Por último, toda la información presentada en la MCKB también se ha aglutinado a manera de casos, de tal forma que se puede consultar ejemplos concretos de amenazas y/o como usar los controles de seguridad, indicando el contexto, cómo se solucionó el caso y recomendaciones. La figura 4, muestra un ejemplo de ello.

Figura 4. Ejemplo de información, a manera de casos, contenida en la MCKB



Fuente: ICAT-UNAM (2024).

La MCKB es joven, pero sin duda alguna ofrece herramientas valiosas para todos los actores de las redes móviles que ayudarán a que éstas se despliegen con mayor seguridad. Los beneficios esperados a través del uso amplio y sostenido de la MCKB son los siguientes:

- La base de conocimientos es un documento vivo en continua actualización conforme se identifican riesgos, vulnerabilidades, avances tecnológicos, tácticas, técnicas y procedimientos de seguridad.
- Colaboración del alcance universal de la GSMA en el ecosistema de redes móviles.
- Aprendizaje de las herramientas de ciberseguridad a través de experiencias reales que han sido documentadas.
- Línea de base de referencia que, sin ser vinculante, ofrece ayuda para que los actores del ecosistema de las redes móviles, incluyendo la quinta generación puedan diagnosticarse, identificar las brechas de ciberseguridad y generar planes para superar sus debilidades.
- Los controles de seguridad también pueden servir de base a las agencias reguladoras para evaluar a los operadores, proveedores de equipos y aplicaciones.
- Un marco de referencia comprensivo que suma las visiones empresariales y técnicas, con lo cual se da un enfoque holístico al tema de ciberseguridad.
- Las evaluaciones se realizan siguiendo procedimientos estándar, lo que facilita la integración de actores y elevar la seguridad de todo el sistema.

- Facilita y fomenta la colaboración para proteger las redes y los servicios contra las interrupciones y el acceso no autorizado, dando también seguridad a los usuarios finales.
- Contribuirá a mejorar las competencias y capacidades en materia de seguridad 5G.
- Reforzará la labor de operadores, empresas, organismos de supervisión y reguladores.
- A nivel operativo, la MCBK ofrece instrucciones claras para adoptar medidas paso a paso con el fin de crear garantías de seguridad teniendo en cuenta todo el espectro de riesgos de las redes 5G de extremo a extremo.
- El mapeo de amenazas en colaboración con todos los actores permite documentar las soluciones técnicas de mitigación para todas aquellas que hayan sido identificadas. Considerar al mayor número de proveedores posible garantiza la diversidad de amenazas y soluciones
- Las soluciones de seguridad ofrecidas en la base de conocimientos de ciberseguridad 5G son eficaces independientemente del origen del proveedor.

Referencias

3GPP. (s.f.). About 3GPP. Recuperado de https://www.3gpp.org/about-us

Cheang, A., Gong, X. y Yang, M. (abril de 2021). Achieving 5G Security through Open Standards. *OIC-CERT Journal of Cyber Security,* 3(1), 55-64.

Castells, P., Joiner, J. y Adamowicz, A. (2023). 5G en América Latina, liberando el potencial. GSMA Intelligence. Recuperado de https://www.gsma.com/latinamerica/wp-content/uploads/2023/06/290623-5G-in-Latam-ESP.pdf

Cybersecurity Malaysia. (2022). GSMA 5G Cybersecurity Knowledgebase & NESAS [whitepaper]. Recuperado de https://www.cybersecurity.my/data/content_files/13/2383.pdf

Ericsson. (2024). *Ericsson mobility report. Business Review 2024*. Recuperado de https://www.ericsson.com/4912e3/assets/local/reports-papers/mobility-report/documents/2024br/emr-business-review-2024.pdf

Global System for Mobile Communications [GSMA]. (2019). *Manual de políticas públicas de comunicación móviles*. GSMA. Recuparado de https://www.gsma.com/latinamerica/wp-content/uploads/2019/03/GSMA_Mobile-Policy-Handbook_2019_ESP.pdf

GSMA. (2024). *La economía móvil en América Latina*. GSMA Intelligence. Recuperado de https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/06/La-economia-movil-en-America-Latina-2024.pdf

GSMA. (septiembbre de 2023). *Baseline Security Controls. Version 3.0*. Recuperado de https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

GSMA. (s.f. a). *Móviles y privacidad*. Recuperado de https://www.gsma.com/latinamerica/wp-content/uploads/2012/01/Privacy-leaflet-2012-Spanish.pdf

GSMA. (s.f. b). As MNOs launch 5G systems, networks face new security challenges. Recuperado de https://www.gsma.com/solutions-and-impact/technologies/security/5g-cybersecurity-knowledge-base/

GSMA. (s.f. c). GSMA Mobile Cybersecurity Knowledge Base. Recuperado de https://www.gsma.com/solutions-and-impact/technologies/security/5g-cybersecurity-knowledge-base/

Instituto de Ciencias Aplicadas y Tecnología [ICAT]-Universidad Nacional Autónoma de México [UNAM]. (2024). *Diplomado en gestión de la ciberseguridad,* [presentación *ppt, material* inédito].

International Telecomunication Union [ITU]. (2019). Focus Group on IMT-2020. GT IMT-2020. Recuperado de https://www.itu.int/es/ITU-T/focusgroups/imt-2020/Pages/default.aspx

ITU. [s.f.]. ITU Publications: General Secretariat and Telecom. Recuperado de https://www.itu.int/es/publications/gs/Pages/default.aspx

ISO. (s.f.). ISO IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en

Lineamientos generales de políticas organizacionales establecidas en la MCBK como complemento al control de gobernanza empresarial BC-003

Política	Descripción del lineamiento
Gestión de la seguridad de los datos de terceros y de la cadena de suministro	La gestión de la seguridad de los datos de terceros y de la cadena de suministro controlará los intercambios de información y el acceso remoto de terceros a los sistemas de información, así como el correcto funcionamiento de la política y los controles para garantizar que no se introducen vulnerabilidades en la cadena de suministro.
Control de acceso	La política de control de acceso abarcará el proceso de acceso interno y externo a los sistemas de información y a los datos. Esto incluye las políticas de inscripción y de altas/bajas, los controles de acceso a los datos, los controles de acceso a la red y la gestión de privilegios.
Gestión de activos	Políticas de gestión de activos; incluido el diseño arquitectónico, la gestión durante la vida útil y el desmantelamiento de activos, especialmente los que contienen información y datos. Esto garantiza que los sistemas que procesan esos activos puedan protegerlos eficazmente y que se evite la pérdida de datos (por ejemplo, tras su eliminación).
Políticas de continuidad	Las políticas y planes de gestión de la continuidad de la actividad se elaboran a partir de evaluaciones de impacto especializadas que garantizan el mantenimiento de los procesos críticos de la empresa con independencia de las eventualidades (catástrofes, pérdidas de personal clave y otras interrupciones de la actividad, por ejemplo, huelgas).
Seguridad en la nube	Las políticas de seguridad en la nube garantizan que se apliquen los controles de seguridad adecuados a los despliegues de computación en nube pública, privada o híbrida, prestando especial atención a la protección de los activos cuando se procesan en un entorno multiarrendatario en el que los arrendatarios dependen en gran medida del entorno de seguridad proporcionado por el proveedor de servicios en la nube.

Gestión de material criptográfico	La política de gestión del material criptográfico garantiza una gestión eficaz y sostenible de la tecnología de cifrado dentro de las soluciones. Esto incluye la gestión proactiva de claves para garantizar que la información y los datos puedan cifrarse/descifrarse como y cuando sea necesario (y solo por las partes comunicantes legítimas) y también que las técnicas criptográficas que soportan los marcos de integridad y confianza (PKI) funcionen eficazmente y sean fiables.
Seguridad de dispositivos, sistemas y redes	Las políticas de seguridad de dispositivos, sistemas y activos de red garantizan que se apliquen las configuraciones adecuadas a los dispositivos informáticos y de red para a) ayudar a aplicar las políticas de control de acceso y b) minimizar la exposición de vulnerabilidades (por ejemplo, desactivación de funciones no utilizadas/aplicación de bloqueos de compilación).
	La política de clasificación y tratamiento de la información definirá el enfoque de la clasificación de seguridad de la información tanto en papel como en formato electrónico. Es habitual que se identifique una jerarquía de clasificaciones de seguridad y que se definan los requisitos de tratamiento adecuados para cada clasificación.
	Las políticas de seguridad del personal abarcan los controles previos a la contratación y durante la misma, así como las condiciones de los contratos de trabajo y los acuerdos con agencias y otros contratistas. También abarca las sanciones por infracciones de seguridad en el marco de procesos y procedimientos disciplinarios o contractuales, así como la gestión de las autorizaciones de seguridad para trabajar con terceros (por ejemplo, organismos gubernamentales).
Seguridad física	Cabe esperar que se apliquen varias políticas y normas de seguridad física en todos los inmuebles de las organizaciones operadoras, con normas adecuadas y proporcionadas aplicadas a los distintos emplazamientos (centros de datos, centros de telecomunicaciones, oficinas, emplazamientos celulares, etc.).
Administración de riesgo	Una política de gestión de riesgos debe plasmar el enfoque de la gestión de los riesgos para la información (la confidencialidad, integridad y disponibilidad de dicha información). Esto incluye la consideración de amenazas y vulnerabilidades presentes tanto en entornos físicos como electrónicos. Esto debe integrarse con el enfoque empresarial del riesgo para que el SLT tenga visibilidad de los riesgos críticos para la seguridad de la información.

Gestión de incidentes de seguridad	La política y los procesos de gestión de incidentes de seguridad se ocupan del ciclo de vida completo de los incidentes relacionados con la seguridad (incluidas las violaciones), deben funcionar como un bucle de retroalimentación para reducir el riesgo de que se repitan y deben abarcar todos los aspectos: notificación (comportamiento real o sospechoso, puntos débiles, etc.), triaje, investigación, informática forense, notificación de violaciones (de acuerdo con la normativa local), comunicación con las partes interesadas, colaboración con las fuerzas de seguridad, recuperación, informes de gestión/escalada, equipos de gestión de incidentes críticos y revisiones posteriores al incidente.
Monitoreo de seguridad	La política y los procesos de supervisión de la seguridad se utilizan para establecer las competencias, las disciplinas y el marco necesarios para supervisar los sistemas en busca de comportamientos anómalos que indiquen posibles ciberataques o violaciones de la seguridad. Esto también incluye políticas de auditoría para aquellos sistemas que no están supervisados por sistemas electrónicos y también gestión y análisis de registros.
Gestión de la actualización de software	La política de gestión de actualizaciones de seguridad del software define los parámetros necesarios para la aplicación de actualizaciones de seguridad y otros parches al software y firmware de los equipos. También tiene en cuenta los ciclos de vida de los productos para garantizar que los sistemas reciben actualizaciones de seguridad y que los componentes que dejan de recibir asistencia se sustituyen antes de que queden obsoletos.
	La política de formación y concienciación del personal abarca tanto la formación especializada del personal de seguridad y de primera línea como una concienciación más amplia sobre cuestiones de seguridad para todo el personal y los contratistas (incluidas sesiones de iniciación, sesiones informativas/comunicaciones periódicas de repaso/actualización, carteles, etc.). También cubre la difusión urgente de avisos de seguridad a raíz de violaciones de la seguridad.
	La política de gestión de la divulgación de vulnerabilidades abarca la notificación responsable de las vulnerabilidades descubiertas en sistemas, servicios y soluciones. De este modo se evita que los detalles de esas vulnerabilidades caigan en manos de atacantes interesados en explotarlas y, en ocasiones, se divulga información pública para que esté en conjunción con la disponibilidad de soluciones.


ICAT
Instituto de Ciencias
Aplicadas y Tecnología


Universidad Nacional
Autónoma de
México


UNAM
La Universidad
de la Nación