GSMA

Seguridad y privacidad a lo largo del ecosistema móvil

Seguridad y privacidad a lo largo del ecosistema móvil

El presente informe es una edición actualizada del informe “Seguridad, privacidad y protección del ecosistema móvil”, publicado originalmente en 2017.

GSMA

La GSMA es una organización global que une al ecosistema móvil para descubrir, desarrollar y ofrecer la innovación esencial para entornos comerciales positivos y cambios sociales. Nuestra visión consiste en aprovechar al máximo la conectividad para que las personas, la industria y la sociedad prosperen. Como representante de los operadores móviles y organizaciones de todo el ecosistema móvil e industrias adyacentes, la GSMA realiza su contribución a sus miembros bajo tres grandes pilares: Conectividad para el Bien, Servicios y Soluciones de Industria, y Alcance y Difusión. Esta actividad incluye promover políticas públicas, abordar los mayores desafíos sociales de la actualidad, apuntalar la tecnología y la interoperabilidad que hacen funcionar a la conectividad móvil, y proporcionar la plataforma más grande del mundo que reúne al ecosistema móvil en las series de eventos MWC y M360.

Obtenga más información en gsma.com

Siga a la GSMA en Twitter: @GSMA

GSMA

Contenidos

Resumen ejecutivo

En las últimas tres décadas, el mercado de servicios de telecomunicaciones móviles ha crecido hasta superar los 10.700 millones de conexiones,[1] brindándoles servicios móviles a 5.300 millones de suscriptores únicos a nivel mundial.[2]

En 2021, la cantidad de suscriptores de Internet móvil alcanzó los 4.200 millones de personas a escala global;[3] la adopción de 5G también continúa creciendo rápidamente, para marzo de 2022, los servicios 5G móviles ya estaban disponibles en 73 países y representaban más del 8 por ciento de las conexiones móviles globales.[4]

El impacto de este crecimiento se puede observar tanto en mercados desarrollados como en vías de desarrollo. Los servicios móviles han permitido que las personas, las empresas y los gobiernos puedan innovar en formas originales y, a menudo, inesperadas. Al mismo tiempo, los consumidores de todo el mundo han demostrado un apetito voraz por adoptar nuevas tecnologías. Por otro lado, la pandemia de COVID-19 exacerbó las desigualdades socioeconómicas prexistentes. Cuando se impusieron las restricciones de confinamiento y distanciamiento social, las personas recurrieron a las redes móviles para mantenerse conectadas y acceder a servicios para mejorar sus vidas. La ubicuidad de los servicios móviles y los smartphones en muchos países de bajos y medianos ingresos (LMIC) ha permitido la aparición de modelos de negocio completamente nuevos que posibilitan nuevas formas de interacción personal y comercial permitiendo que el ecosistema móvil en general aportara USD 4,5 billones en 2021 en valor económico agregado.[5]

La industria móvil trabaja denodadamente por educar a los consumidores y ha desarrollado nuevas funcionalidades para fomentar la confianza en sus servicios. Con cada iteración tecnológica adicional, se introdujeron nuevas características, como el cifrado y la validación de la identificación del usuario, que aumentaron cada vez más la seguridad de los servicios móviles minimizando el potencial de fraude, robo de identidad y muchas otras posibles amenazas. Cabe destacar que la confianza que sustenta estos servicios y permite que todas las personas del mundo puedan comunicarse, hacer negocios, compartir ideas e interactuar, no puede darse por sentada.

1 Conexiones móviles incluyendo IoT www.gsma.com
2 https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf
3 ibíd.
4 5G in Context, Data-driven insight into areas influential to the development of 5G (T1 2022)
5 https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

Aumento de posibles amenazas

A medida que se desarrollan servicios más avanzados y complejos, aumenta la lista de posibles amenazas y el alcance de los daños que pueden causar. Las estafas y los ataques son cada vez más sofisticados y penetrantes, y la capacidad de los criminales de interceptar comunicaciones aumenta con frecuencia: va desde el robo de grandes cantidades de datos hasta el hackeo y la divulgación de comunicaciones privadas durante las elecciones estadounidenses de 2016.

Aunque con un perfil más bajo, la prevalencia de estafas relacionadas con phishing, ransomware y fraude de dinero son igualmente perjudiciales para el individuo.[6] Está claro que el objetivo de estas estafas son las comunicaciones en general y no solo las de dispositivos móviles, por lo que las soluciones deben tener una visión integral de los servicios en cuestión.

Lógicamente, los gobiernos y los formuladores de políticas desean prevenir este tipo de incidentes y proteger a los ciudadanos en la mayor medida de lo posible. Sin embargo, en un entorno tan complicado, el objetivo de cualquier intervención debe ser el apropiado. Aunque bien intencionada, toda acción puede tener un costo desproporcionado o restringir el acceso a los mismos servicios que intenta proteger.

Asimismo, existen complejas concesiones entre la protección de la seguridad de las comunicaciones personales y la necesidad de las agencias de aplicación de la ley que, en ocasiones, deben interceptar ciertas comunicaciones para proteger el bien público. Debe tenerse en cuenta la naturaleza compleja y multipartita de muchos de estos servicios. Por ejemplo, cuando dos personas se comunican a través de un servicio de mensajería, en realidad, están utilizando dos dispositivos diferentes, posiblemente dos sistemas operativos y aplicaciones de interfaces diferentes y múltiples redes para conectarse a través de dicha plataforma, la cual generalmente se encuentra alojada en una jurisdicción legal diferente de la de uno o ambos usuarios.

Cada uno de los eslabones de esta cadena tiene sus propias debilidades, vacíos legales y amenazas potenciales, desde la interceptación y el abuso hasta el hackeo y el software malicioso (malware). Los esfuerzos por proteger al consumidor pueden desviarse si se enfocan en una única posible debilidad, sin considerar todas las demás. Toda acción destinada a fortalecer una parte de la cadena de servicios que ya es robusta, no soluciona las debilidades de las otras partes de la cadena.

La industria móvil invierte importantes sumas de dinero para la protección y la seguridad del uso de sus servicios, a la vez que también intenta proteger la privacidad de sus clientes en la mayor medida posible. Está claro que estos esfuerzos se enmarcan dentro de una dimensión tecnológica: estándares en constante mejora, despliegues de mejores versiones de la tecnología, pruebas de redes para identificar debilidades y desarrollo de la capacidad de detectar e impedir ataques maliciosos.

6 Vea el informe de la GSMA sobre: https://www.gsma.com/security/resources/t-isac-insight-report-flubot/

La GSMA desempeña un papel clave en la coordinación de actividades y en la provisión de servicios, como la Verificación de Dispositivos de la GSMA (Device Check™),[7] y los Esquemas de Acreditación de Seguridad para SIM, eSIM y equipos de red (SAS,[8] NESAS[9]).

Existen distintas iniciativas de la industria que tienen el objetivo de concientizar a los operadores acerca de los riesgos y las opciones de mitigación disponibles para proteger a sus redes y clientes. Muchos operadores móviles y otros actores del ecosistema están trabajando activamente en sus mercados y en organismos internacionales para maximizar la efectividad de toda respuesta tecnológica.

No obstante, la tecnología por sí sola no es suficiente para dar respuesta a innumerables amenazas y desafíos. La industria, con el respaldo de la GSMA, ha participado muy activamente en programas para educar a consumidores y empresas sobre el uso seguro de las tecnologías móviles y las aplicaciones que soportan, con el objeto de minimizar conductas ilícitas, como el abuso, el fraude y las violaciones a la privacidad en línea. En esas instancias, es esencial dar una respuesta holística en la que participen gobiernos, otros organismos y organizaciones sin fines de lucro, además de los proveedores finales de los servicios proporcionados en línea o a través de dispositivos móviles, como banca y pagos.

Son mucho más comunes las instancias en las que el usuario comparte sus datos personales voluntariamente a fin de obtener acceso a servicios comerciales legítimos. En estos casos, la industria móvil enfrenta un desafío distinto: dado que, supuestamente, ocho de cada diez consumidores no están tranquilos con la cantidad de datos personales que se comparten; puede existir una tendencia natural en políticos y consumidores a esperar que los operadores de redes resuelvan este asunto. Sin embargo, las consideraciones sobre tecnología y defensa de la competencia dificultan demasiado (y, en ocasiones, hasta impiden) la intervención de los operadores de redes móviles en los intercambios que tienen lugar entre el proveedor de servicios en línea y el usuario final. Asimismo, existe una gran diferencia entre los estándares de protección de datos que se aplican en las distintas jurisdicciones y, especialmente, entre el sector de telecomunicaciones y los sectores de los proveedores de servicios en línea. Por lo tanto, un operador de redes móviles solo puede comprometerse a proteger los datos que posee de sus usuarios finales y a concientizar a estos de que posiblemente estén compartiendo demasiados datos con organizaciones que exceden el control del operador. Los gobiernos y todo el ecosistema móvil en general deberían colaborar para garantizar soluciones prácticas que permitan a los consumidores tomar decisiones informadas y efectivas, encontrando un equilibrio entre el deseo de privacidad de las personas y el de tener acceso, desde un dispositivo móvil, a contenido y aplicaciones interesantes que se financian a través de la publicidad.

Algunos desafíos relacionados con la provisión de servicios móviles privados y seguros son causados por los gobiernos y organismos de aplicación de la ley. El mandato legítimo, y cada vez más delicado, de proteger a los ciudadanos, los ha llevado a buscar poderes de amplio alcance para acceder y utilizar datos personales, así como para intervenir y bloquear o restringir los servicios de comunicación en circunstancias especiales.

La industria reconoce su obligación legal y moral de respaldar la seguridad pública y respetar los mandatos legítimos de los gobiernos, observando el debido proceso, al igual que su obligación legal y moral de respetar los derechos humanos. Cada vez con más frecuencia, en todo el mundo, los operadores han debido oponerse a ciertas intervenciones que han considerado desproporcionadas y no alineadas con los marcos de derechos humanos internacionales o hasta posiblemente contraproducentes para los fines de la seguridad pública.

Como se trata de un área sumamente compleja, con diferencias sustanciales entre jurisdicciones nacionales, la GSMA se centra en establecer principios comunes y educar a todas las partes sobre las mejores prácticas. Los operadores de redes móviles enfrentan otros dos desafíos adicionales: son la primera línea de ataque cuando los gobiernos intentan poner en tela de juicio a las empresas internacionales de Internet, sobre las cuales tienen poca o ninguna influencia y, en ocasiones, se les exige guardar silencio al respecto, a pesar de sus deseos de transparencia frente a los consumidores que confiaron en ellos.

7 https://devicecheck.gsma.com/
8 https://www.gsma.com/sas
9 https://www.gsma.com/nesas

Acciones de los gobiernos, la industria y otras partes interesadas

El presente informe aborda cada una de las problemáticas principales sobre la protección del consumidor, la privacidad, la seguridad pública y la seguridad de la infraestructura. Asimismo, pone de relieve los posibles problemas, las medidas que se están implementando para resolverlos y las acciones adicionales que podrían ser necesarias. Estos problemas son tan importantes que los operadores móviles miembros de la GSMA han concluido que deben trabajar en conjunto y más estrechamente, tanto a nivel nacional como internacional, para poder garantizar la respuesta más efectiva.

Ninguno de estos problemas multidimensionales puede "resolverse" en forma simple ni mediante las acciones aisladas de una única organización o sector. Para obtener los mejores resultados, tanto para los usuarios móviles como para la sociedad en general, se debe contar con el compromiso y la acción de los gobiernos, las agencias de aplicación de la ley, y las organizaciones multilaterales y no gubernamentales. También son importantes los esfuerzos de las empresas de todo el ecosistema digital, así como los esfuerzos personales de los propios consumidores.

Si bien no todas las cuestiones son de alta prioridad para todos los países y, por consiguiente, para todos los operadores, la necesidad de lograr una cooperación más estrecha entre las múltiples partes involucradas en la prestación de servicios al usuario final es común a todos los problemas y geografías, a fin de garantizar la maximización de la seguridad y la confianza como también el desarrollo e implementación de soluciones que brinden el mejor beneficio generalizado para toda la sociedad.

La naturaleza global de los sistemas de comunicaciones modernos, desde los estándares y los equipos de infraestructura hasta los servicios y los operadores, implica que las acciones aisladas y unilaterales no son tan efectivas como una estrategia coordinada.

Este informe incluye un conjunto de principios que sostienen los operadores móviles miembros de la GSMA para guiarse en sus acciones de protección del consumidor y la seguridad de las redes de comunicaciones móviles. También insta a los formuladores de políticas y reguladores a adoptar una visión ampliada sobre las cuestiones en juego y así colaborar en el desarrollo de las mejores soluciones (elaboradas por todas las partes interesadas) que protejan los intereses generales de los consumidores, las empresas y la sociedad civil.

Este claro compromiso con la seguridad, la privacidad y la protección de los servicios de comunicaciones móviles refleja la intención de la industria de garantizar que el crecimiento de los beneficios de las comunicaciones móviles continúe en el futuro próximo, enriqueciendo la vida de las personas y la sociedad con el máximo potencial de estas tecnologías apasionantes y dinámicas.

Protección del consumidor

Para promover el uso seguro y responsable de los servicios y dispositivos móviles en línea, es indispensable contar con los esfuerzos de las múltiples partes interesadas. En particular, los gobiernos y sus agencias de aplicación de la ley deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar las conductas delictivas. A menudo, esto requerirá de una cooperación global. Otros actores del ecosistema de la industria, como los fabricantes de dispositivos y los proveedores de servicios móviles, deberían participar en las iniciativas destinadas a proteger al consumidor al momento de usar servicios y dispositivos móviles y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios de forma segura. Los operadores pueden desempeñar un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, y en alentarlo a utilizar todo el conjunto de medidas de seguridad disponibles. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para tratar las cuestiones relacionadas con la protección del consumidor y las actividades ilegales y perjudiciales vinculadas al uso de teléfonos celulares o facilitadas por estos, mediante los siguientes esfuerzos:

- Trabajar en colaboración con otros organismos en pos de brindar soluciones multilaterales adecuadas.
- Implementar soluciones diseñadas para prevenir el uso de las redes para la comisión de fraudes y actividades delictivas y el uso de los dispositivos para perjudicar al consumidor.
- Educar al consumidor acerca de las conductas seguras relacionadas con el uso de aplicaciones y servicios móviles, para así aumentar su confianza.

Protección de la privacidad del consumidor

El objetivo principal de la protección de la privacidad es generar confianza en que los datos privados son protegidos de forma adecuada conforme con la regulación y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia en todos los servicios, sectores y geografías. Los gobiernos pueden ayudar a garantizar este resultado, y a la vez ofrecer la flexibilidad necesaria para la innovación, mediante la adopción de marcos legales basados en riesgos para así salvaguardar los datos privados y promover prácticas de gobernanza digital responsables que estén alineadas con la regulación local. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para proteger y respetar los intereses de privacidad del consumidor y facilitar la toma de decisiones informadas sobre qué datos personales se recopilan y cómo se utilizan, mediante la implementación de políticas que promuevan lo siguiente:

- El almacenamiento y procesamiento seguro de toda la información personal y privada, conforme a los requisitos legales, cuando corresponda.
- La transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y el pleno cumplimiento de las exigencias legales.
- La entrega de información y herramientas para que el consumidor pueda tomar decisiones simples y significativas sobre su privacidad.

Protección de la seguridad pública

En línea con el objetivo general de proteger la seguridad pública, los operadores de redes móviles deben asumir responsabilidades adicionales y colaborar con las agencias de aplicación de la ley, conforme a las leyes y la regulación, las obligaciones de las licencias y la legislación local. Es importante que los gobiernos garanticen la existencia de un marco legal proporcional que describa claramente las facultades de las que disponen las agencias nacionales de aplicación de la ley. Dicho marco legal debe garantizar también que las solicitudes de asistencia sean efectivamente necesarias y proporcionadas, que estén dirigidas al proveedor de tecnología o de servicios de comunicaciones más apropiado y que respeten los principios de derechos humanos. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores cumplirán toda obligación, establecida por ley o por licencias, relacionadas con temas de protección o seguridad pública en los países en los que operan, a la vez que darán su apoyo en cuestiones de derechos humanos. Además, colaborarán con las agencias de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- Trabajar con las agencias pertinentes cuando la situación particular así lo requiera, a fin de desarrollar e implementar soluciones adecuadas para lograr el objetivo final con mínimas molestias al consumidor y los servicios críticos.
- Construir redes que tengan la funcionalidad de abordar situaciones de emergencia y seguridad, cuando corresponda.
- Brindar claridad sobre las limitaciones de las acciones que se pueden tomar en la cadena de valor e indicar cuándo se deben implementar acciones por parte de terceros.

Protección de la seguridad de las redes y la integridad de los dispositivos

Los actores de la industria deben trabajar en conjunto y coordinar con las agencias internacionales de aplicación de la ley para compartir inteligencia sobre amenazas para así responder a ataques maliciosos a las redes y dispositivos móviles e identificar a los responsables. Esto se puede lograr a través de la participación de los equipos de respuesta ante incidentes de seguridad existentes y la creación de nuevos, si fuese necesario, para contrarrestar cualquier deficiencia. Cuando corresponda, la regulación debería aplicarse de manera coherente a todos los proveedores de la cadena de valor, con neutralidad respecto de los servicios y la tecnología. Preservando al mismo tiempo el modelo de gobernanza de Internet de múltiples partes interesadas y permitiendo su evolución. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas para proteger la infraestructura subyacente y asegurar que se provea al cliente el servicio de comunicaciones más seguro y confiable posible, mediante las siguientes acciones:

- Tomar medidas para garantizar la seguridad de la infraestructura de red que operan y controlan.
- Promover las asociaciones entre el sector público y el privado para minimizar el riesgo de hackeo o uso de la red para fines maliciosos a través de estrategias globales y coordinadas.
- Brindar claridad sobre qué parte de la infraestructura es responsabilidad de los operadores y dónde se encuentran las fronteras con otros servicios o infraestructura.

01

Capítul 1

Introducción

En todas las regiones del mundo, se observa un aumento de las amenazas, ya sean reales o percibidas, a la seguridad nacional, la seguridad pública y la privacidad individual.

Las redes móviles desempeñan un papel importante en la protección de la seguridad pública. Por ejemplo; cuando las agencias de aplicación de la ley, siguiendo su mandato, realizan investigaciones criminales en base a información sobre llamadas e interceptación de comunicaciones, dan soporte a comunicaciones sobre incidentes graves o cuando rastrean amenazas a la salud pública, como el uso de datos de datos de ubicación para monitorear y prevenir los brotes y la propagación del virus COVID-19. Por otro lado, a nivel del individuo, existen casos de fraude, robo de identidad, ciberacoso y otras actividades ilegales que se cometen tanto a través de las redes móviles como de los servicios digitales (o en línea) a los cuales se accede a través de redes fijas. Algunos acontecimientos recientes, como casos de violaciones de datos de alto perfil, también han generado intranquilidad en muchos consumidores acerca de la seguridad y la privacidad de los detalles de su vida personal, por ejemplo.

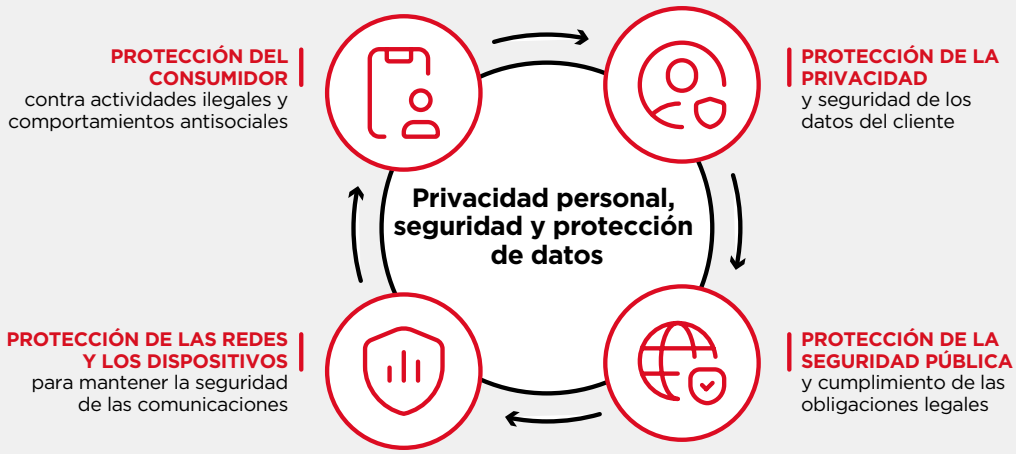
En este contexto, los operadores de redes móviles se enfrentan al desafío continuo de brindar a los clientes una experiencia móvil segura y protegida, cumpliendo a su vez, las obligaciones de protección de la seguridad pública. La GSMA y sus operadores miembros ya están trabajando para enfrentar y solucionar los problemas de privacidad y seguridad, así como para promover el uso seguro y beneficioso de los servicios móviles y la gran variedad de aplicaciones que soportan.

Este informe pretende explicar las cuestiones y los desafíos más importantes en torno a la seguridad y la privacidad en el ámbito móvil, destacando tanto las complejidades como las concesiones, describiendo las iniciativas y acciones de la industria que ya se encuentran en curso. En los casos donde exista la posibilidad de hacer aún más, este informe identifica dichas áreas y también describe qué hace falta para que estas respuestas se conviertan en realidad, ya sea para educar al consumidor, formar asociaciones en el ecosistema o desarrollar e implementar soluciones técnicas multipartitas. Si bien se aborda cada cuestión individualmente, también se reconocen las diferentes interdependencias y superposiciones entre ellas.

Estructura

En general, el tema de la seguridad y la privacidad es sumamente amplio, pero puede considerarse bajo cuatro pilares principales, como lo ilustra la Figura 1.

Figura 1
Marco de seguridad y privacidad



Las siguientes cuatro secciones del presente informe abordan cada área de forma individual, es decir:

1. **Protección del consumidor**: promover el uso seguro de los servicios móviles
2. **Cuestiones de privacidad y datos**: proteger la privacidad del consumidor y el almacenamiento y procesamiento seguros de los datos personales del individuo
3. **Protección de la seguridad pública**: definir el rol y las responsabilidades de los operadores móviles respecto a su colaboración con las agencias de gobierno para proteger al público
4. **Protección de la infraestructura de red y los dispositivos**: garantizar la integridad y seguridad de la infraestructura de redes móviles y de los dispositivos utilizados para acceder a ellas

La última sección describe los principios de alto nivel acordados entre los operadores miembros y resume los planes para incorporarlos a las futuras actividades de la GSMA.

Tal como se demostrará en este informe, la naturaleza de estas cuestiones exige una acción coordinada en todas las geografías y segmentos de la industria. Si bien la industria móvil lidera los esfuerzos para abordar estas cuestiones, existen muchos otros grupos activos en este espacio, desde organismos de normalización como el 3GPP, ETSI, ENISA, IETF y NIST, hasta entes internacionales, como la UIT, el Diálogo de la Industria (ID) de las Telecomunicaciones, la Iniciativa de Red Global (GNI) y UNICEF.

A todos ellos les toca desempeñar un papel valioso e importante para encauzar el debate y desarrollar soluciones. La GSMA recibe con gusto toda colaboración y participación adicional del ecosistema móvil y de la industria de las TIC en general en todos estos temas.

02

Capítulo 2

Protección del consumidor

A fin de que los consumidores de todo el mundo sigan disfrutando de los múltiples beneficios de la tecnología móvil, es importante que usen estos servicios de forma segura y con confianza.

Protección del consumidor

Para promover el uso seguro y responsable de servicios en línea y dispositivos basados en tecnologías móviles, es indispensable contar con los esfuerzos de las múltiples partes interesadas. En particular, los gobiernos y sus agencias de aplicación de la ley deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar conductas delictivas. A menudo, esto requerirá de una cooperación global. Otros actores del ecosistema de la industria, como los fabricantes de dispositivos y los proveedores de servicios basados en conectividad móvil, deberían participar en las iniciativas destinadas a proteger al consumidor al momento de usar servicios y dispositivos móviles, y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios de forma segura. Los operadores pueden desempeñar un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, alentándolo a utilizar todo el conjunto de medidas de seguridad disponibles. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para tratar las cuestiones relacionadas con la protección del consumidor y las actividades ilegales y perjudiciales vinculadas al uso de teléfonos celulares o facilitadas por estos, mediante los siguientes esfuerzos:

- Trabajar en colaboración con otros organismos en pos de brindar soluciones multilaterales adecuadas.
- Implementar soluciones diseñadas con el objetivo de prevenir el uso de las redes para la comisión de fraudes, actividades delictivas y el uso de los dispositivos para perjudicar al consumidor.
- Educar al consumidor acerca de las conductas seguras en el uso de aplicaciones y servicios móviles para así aumentar su confianza.

Con el rápido crecimiento de la importancia y el alcance de los servicios móviles, las personas están cambiando rotundamente la manera en la que se conectan e interactúan, tanto personal como comercialmente. Es inevitable que, con su uso tan extendido, haya personas que intentan usar la tecnología móvil para perjudicar a otros.

Esta sección aborda los problemas que afectan de manera directa la seguridad y el bienestar del consumidor de servicios móviles, en especial, aquellos en los que los usuarios de dispositivos y servicios móviles quedan expuestos a amenazas provenientes de conductas ilegales, delictivas o antisociales. Se incluyen los siguientes:

- **Protección de infancias y personas vulnerables**
- **Robo y tráfico de dispositivos robados y la compra y uso de dispositivos falsificados**
- **Fraude y seguridad de los dispositivos móviles**

Cada una de estas cuestiones conlleva varias implicancias importantes para los gobiernos, la industria y otras partes interesadas. Dichas implicancias se detallan minuciosamente en este capítulo.

Infancias y personas vulnerables

La tecnología móvil cumple un papel importante en permitir que las infancias tengan un mejor acceso a los derechos fundamentales que se establecen en la Convención sobre los Derechos del Niño (CDN) de la ONU. Por ejemplo, la tecnología móvil puede facilitar que los niños accedan a una educación de calidad y a información adecuada, a la vez que puede darles el poder de expresar sus opiniones y participar en la toma de decisiones en su comunidad. No obstante, existen riesgos asociados con la conectividad. Por ello, para algunos grupos de usuarios potencialmente vulnerables, en los que se incluyen, entre otros, las infancias y algunas mujeres, es tan importante brindar oportunidades y beneficios como combatir los posibles riesgos.

Por ejemplo, un estudio de la GSMA analizó la brecha de género en términos de propiedad y uso de dispositivos móviles e identificó que la seguridad sigue estando entre los tres principales obstáculos para la propiedad y el uso de teléfonos celulares por parte de las mujeres en países de bajos y medianos ingresos. Esta barrera abarca preocupaciones acerca de la seguridad de la información, del contacto no deseado por parte de desconocidos y de la exposición a contenido dañino.[10] Si bien cabe destacar que solo se puede considerar vulnerable a un subgrupo de mujeres, al igual que de hombres, estas inquietudes deben ser reconocidas y resueltas para garantizar que todas las personas puedan tener acceso a los diferentes beneficios que ofrece la conectividad, en especial aquellos grupos que tienen mayores probabilidades de obtener beneficios a partir del uso de los servicios móviles.

Es necesario que los consumidores se familiaricen con el uso seguro de las funcionalidades de los dispositivos (p. ej., las cámaras) y los servicios móviles. Esta necesidad se incrementa aún más a medida que los dispositivos móviles se vuelven más poderosos y pueden usarse para realizar tareas comunes, como acceder a aplicaciones de educación formal y aprendizaje informal, la banca y la salud electrónica. A medida que el consumidor aprende a aceptar estos diversos beneficios, se presenta la oportunidad de ampliar proactivamente sus habilidades digitales, ya en constante evolución, y empezar a incluir las consideraciones sobre seguridad en Internet a través de programas de educación y concientización. Los programas diseñados para ayudar a desarrollar esta “resiliencia digital” requerirán de los aportes de diferentes partes interesadas. Es importante que los operadores de redes móviles participen en el diseño de estos programas para asegurarse de satisfacer las necesidades de una industria en rápida evolución y aclarar el rol de los diferentes actores del ecosistema

10 The Mobile Gender Gap Report 2022 https://www.gsma.com/r/gender-gap/

de las tecnologías de la información y comunicación (TIC).

Los operadores de redes móviles ya tienen un papel importante en la promoción de los beneficios de la tecnología móvil, al tiempo que enseñan a los potenciales grupos vulnerables a desarrollar su resiliencia digital, a utilizar los servicios de forma segura y a responder y denunciar cualquier abuso en el momento en que ocurra.

Apoyo a la inclusión y seguridad de las mujeres

En promedio, la probabilidad de que una mujer tenga un dispositivo móvil es 7 por ciento menor que la de un hombre en los países de bajos y medianos ingresos, mientras que la probabilidad de que use Internet móvil es un 16 por ciento menor. Estos porcentajes se traducen en que hay 264 millones de mujeres menos que hombres que no pueden acceder a la Internet móvil. Si bien los motivos de esta brecha son diversos, el programa Connected Women de la GSMA trabaja continuamente para identificarlos y solucionarlos. Las preocupaciones por la seguridad y el acoso surgieron como importantes barreras para la adopción de dispositivos y servicios móviles por parte de algunas mujeres.[11]

Los operadores de redes móviles reconocen que, al utilizar servicios de protección para móviles, las mujeres pueden seguir beneficiándose de la seguridad que ofrece la conectividad al tiempo que se reduce la probabilidad de acoso. Por ejemplo, en varios mercados, los operadores móviles han lanzado servicios que automáticamente bloquean llamadas no deseadas, los cuales son de particular interés para las usuarias. Además, existen

servicios para quienes poseen teléfonos básicos, tales como “Banglalink Emergency” (Emergencia Banglalink), que envía automáticamente una alerta por SMS a tres contactos previamente registrados cuando la usuaria marca un número corto. También se envía la ubicación de la usuaria a esos contactos, lo que mejora su nivel de seguridad.

Salvaguarda de usuarios jóvenes y protección de la infancia en línea

La infancia es el segundo grupo de usuarios de servicios móviles potencialmente vulnerables. Para comprender el tema de la protección infantil en línea, es importante hacer dos distinciones:

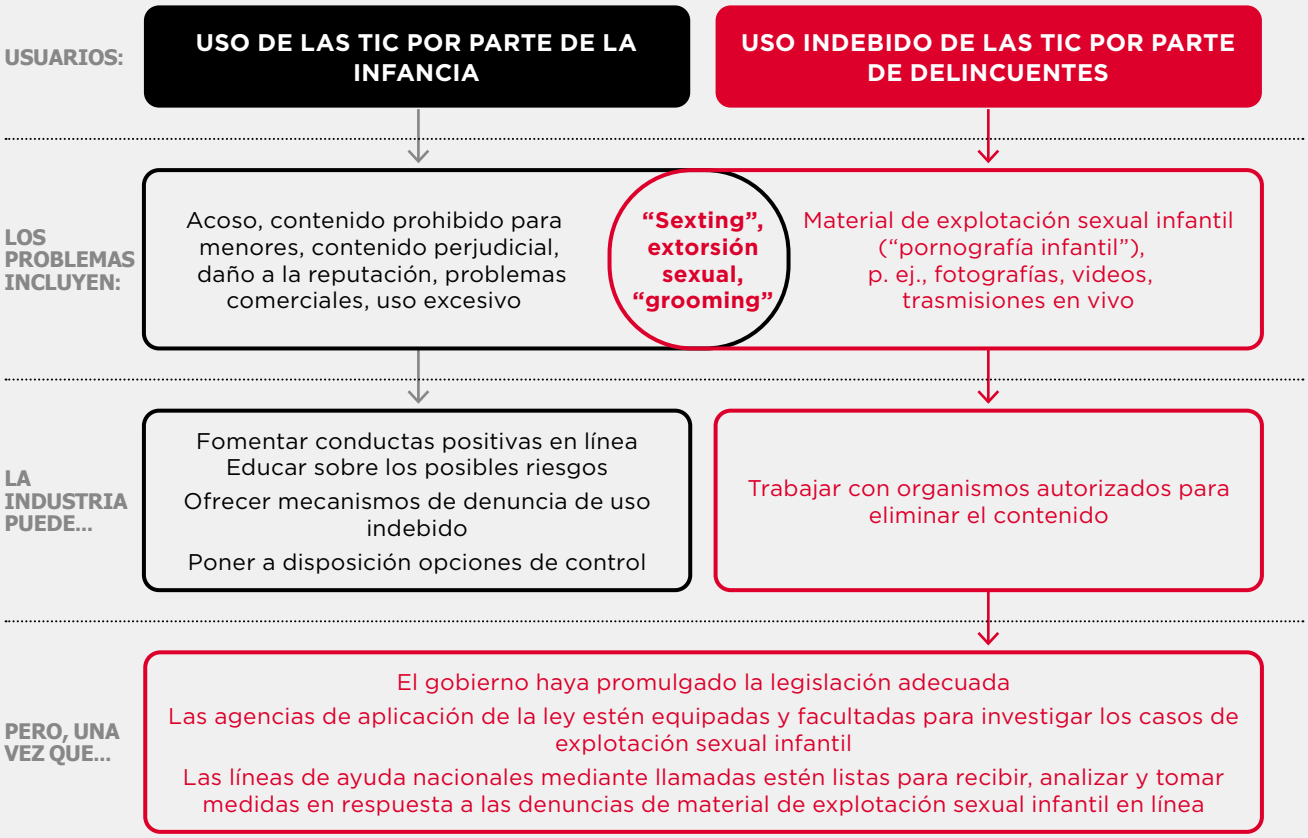
1. Estimular el uso seguro y responsable de los servicios móviles por parte de la infancia.
2. Combatir el uso indebido de los servicios móviles por parte de adultos/delincuentes, por ejemplo, para crear, distribuir o acceder a material ilegal de explotación sexual infantil.

Como ilustra la Figura 2, es conveniente separar estas cuestiones, porque los grupos afectados y los mecanismos de respuesta necesarios para cada uno son muy diferentes.

11 ibíd.

Figura 2

Protección de la infancia en línea:



Un elemento clave para que la infancia y los jóvenes lleven una vida digital más segura es el fomento de conductas positivas en línea, así como la concientización acerca de los riesgos potenciales y el empoderamiento para navegar la Internet con mayor seguridad y confianza. Junto a otras partes interesadas, como docentes, padres y grupos de niños, el aporte de la industria móvil a este proceso es implementar y aplicar políticas de uso aceptables, ofrecer mecanismos de denuncia de uso indebido y poner a disposición opciones de control parental.

Para enfrentar el segundo problema y combatir enérgicamente el uso indebido de la tecnología para el acceso a material de explotación sexual infantil, su distribución o comercialización, se requiere de una serie de acciones por parte de las diferentes partes interesadas. Los gobiernos deben contar con la legislación adecuada, las agencias de aplicación de la ley deben estar equipadas y facultadas para investigar todos los aspectos de abuso sexual infantil (desde la captación de niños y jóvenes con fines sexuales, conocido como "*grooming*", hasta la distribución de material de explotación sexual infantil). También deben implementarse líneas de ayuda nacionales de atención telefónica para denunciar el abuso sexual infantil en línea.

A partir de esto, la industria puede colaborar con esta acción colectiva, por ejemplo, trabajando en conjunto con las líneas nacionales de atención telefónica para eliminar el material de explotación sexual infantil de sus servicios tan pronto sea de su conocimiento y, con el gobierno, en toda circunstancia relevante en la que haya un proceso legal.

En las áreas que se superponen, ilustradas en la Figura 2, se requieren ambas respuestas. Por ejemplo, para mitigar el riesgo de que los jóvenes compartan imágenes sexuales de ellos mismos ("*sexting*"), deben entender las posibles consecuencias de compartir y perder el control de dichas imágenes. Cuando un delincuente obtiene y comparte este material sexual autogenerado, se debe iniciar un proceso para eliminar el material (lo que se describirá en mayor detalle en la subsección sobre material de explotación sexual infantil), además de investigar y procesar al responsable.

La industria móvil y otras partes interesadas tomaron medidas proactivas para fomentar un uso más seguro

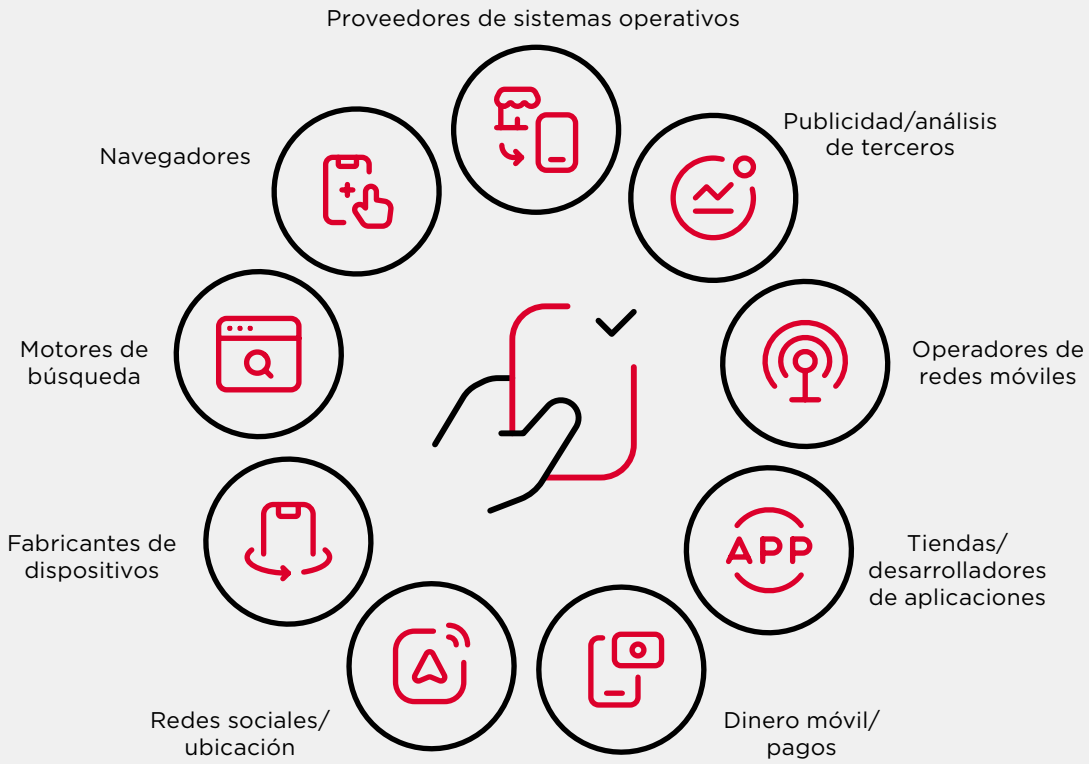
de los servicios móviles por parte de las infancias y los jóvenes.

La GSMA y su iniciativa mPower Youth[12] se dedican a asistir a jóvenes para que obtengan la mejor experiencia móvil posible y colaboran con partes interesadas de todo el ecosistema móvil, así como también con ONG y organizaciones gubernamentales. Entre otras actividades, el programa mPower Youth distribuye información para promover un uso seguro y responsable de los dispositivos móviles. Las iniciativas de los operadores móviles incluyen programas de educación y concientización de amplio alcance y la provisión de soluciones técnicas, como la prestación de servicios de control parental. Mediante su asociación con la Child Helpline International (CHI), la GSMA elaboró directrices para lograr una Internet más segura fin de respaldar a la comunidad de líneas de ayuda para la infancia, de modo que, cuando un niño se enfrente a problemas en línea, puedan derivarlo a un consejero capacitado que pueda darle el apoyo que necesite.[13]

Cuando se trata de proteger los derechos de las infancias en línea, tanto las empresas como otras partes interesadas deben lograr un delicado equilibrio entre el derecho de las infancias a la protección, al acceso a la información y a la libertad de expresión. Por lo tanto, las empresas deben garantizar que las medidas en pos de la protección en línea de las infancias sean específicas y no indebidamente restrictivas para los niños ni otros usuarios. Las Directrices de la UIT y UNICEF sobre la protección de la infancia en línea para la industria de 2020 exponen las medidas que deben tomarse para proteger y promover los derechos de la infancia en el mundo digital.[14]

La rápida evolución del ecosistema móvil crea una mayor complejidad en este tema. El modelo de servicios de contenido curado por el operador evolucionó; en el panorama actual, los usuarios cuentan con diversos medios para acceder a todas las variedades de contenido digital a través de sus dispositivos móviles. Muchos actores, incluidos los operadores móviles, cumplen un papel importante en habilitar esta capacidad, tal como se ilustra en la Figura 3

Figura 3
El ecosistema móvil



12 http://www.gsma.com/mpoweryouth
13 https://www.gsma.com/mpoweryouth/resources/internet-safety-guides/
14 https://www.unicef.org/documents/guidelines-industry-online-child-protection

Las distinciones tradicionales entre las diversas partes del sector de telecomunicaciones y entre las empresas de Internet y de radiodifusión se están desmoronando o volviéndose irrelevantes rápidamente. Los gobiernos, el sector privado, los formuladores de políticas públicas, los educadores, la sociedad civil y los padres cumplen una función vital para fomentar un uso más seguro de los servicios móviles por parte de la infancia y los jóvenes. La cooperación y la asociación entre estas partes son clave para construir los cimientos para un uso más seguro de Internet y tecnologías relacionadas.

La GSMA tiene un papel protagónico en las iniciativas de autorregulación de la industria móvil y fueron fundamentales sus aportes a las Directrices 2020 para la protección de la infancia en línea de la UIT.[15] La GSMA participa de manera activa con gobiernos y reguladores, formuladores de políticas públicas, agencias de aplicación de la ley y la industria para facilitar el desarrollo de estrategias colaborativas que fomenten un uso seguro y responsable de Internet.

En profundidad

Directrices para la protección de la infancia en línea de la UIT

Las Directrices para la Protección de la Infancia En Línea tienen como propósito establecer los cimientos para un uso más seguro de los servicios de Internet y tecnologías relacionadas por parte de la infancia del presente y las generaciones del futuro.

Estas directrices resultan de diálogos con miembros de la Iniciativa para la Protección de la Infancia en Línea, al igual que de una charla abierta que reunió a miembros de la sociedad civil, empresas, académicos, gobiernos, medios de comunicación, organizaciones internacionales y jóvenes para hacer comentarios sobre las directrices.

La cooperación y la asociación son clave para sentar las bases para un uso más seguro de Internet y tecnologías relacionadas. Los gobiernos, el sector privado, los formuladores de políticas públicas, los educadores, la sociedad civil, los padres y los encargados del cuidado de niños cumplen una función vital para lograr esta meta. Las iniciativas de autorregulación de la industria pueden ser útiles en cinco áreas clave:

1. **Incorporar las consideraciones de los derechos de la infancia a todas las políticas empresariales y procesos administrativos.**
2. **Desarrollar procesos estandarizados para la gestión del material de explotación sexual infantil (CSAM).**
3. **Crear un entorno en línea más seguro y adecuado para cada edad.**
4. **Educar a menores, padres y docentes sobre la seguridad de los niños y el uso responsable de las TIC.**
5. **Promover la tecnología digital como modo de aumentar la participación cívica.**

15 https://www.itu-cop-guidelines.com/

La lucha contra el contenido de explotación sexual infantil en línea

Las leyes en materia de contenido ilegal varían considerablemente de país a país; sin embargo, el CSAM se considera ilegal en casi todo el mundo. Indudablemente, la explotación sexual infantil en manos de individuos u organizaciones que buscan consumir, distribuir o lucrar mediante el CSAM, es considerada universalmente inaceptable.

Como se menciona anteriormente, hacer frente al uso indebido de la tecnología con respecto al CSAM exige que los gobiernos promulguen la legislación adecuada, que las agencias de aplicación de la ley estén equipadas y facultadas para investigar, y que existan líneas de ayuda telefónica preparadas para las denuncias de abuso sexual infantil en línea.

Los proveedores de servicios de Internet y los operadores de redes móviles pueden tener una función esencial en la prevención de la revictimización de menores que han sufrido abusos sexuales y tomar medidas para restringir el acceso al CSAM. Por ejemplo, los miembros de la Alianza Móvil contra Contenidos de Abuso Sexual Infantil (Alianza Móvil)[16] de la GSMA se esfuerzan por evitar el uso de los servicios móviles por parte de individuos y organizaciones que desean consumir o lucrar con el CSAM. Para lograrlo, colaboran y comparten información; trabajan con las líneas de denuncia de Internet nacionales, establecen procesos de "notificación y baja" y restringen el acceso a URL o sitios web que, según una autoridad competente, contengan CSAM. Cabe destacar que debe ser una autoridad competente (como la INTERPOL, una línea de ayuda nacional o una agencia de aplicación de la ley) quien determine cuáles son las URL o los dominios que deben bloquearse. Luego, los operadores de redes móviles pueden consultar esta lista y asegurarse de que se implemente sin ponerse en una situación en la que se requiera que analicen la legalidad de un contenido específico.

Los miembros de la Alianza Móvil de la GSMA se comprometen a monitorear las tendencias emergentes que afectan a esta área y a implementar las respuestas adecuadas.

16 https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

En profundidad

Alianza Móvil contra Contenidos de Abuso Sexual Infantil de la GSMA

La Alianza Móvil fue fundada por un grupo internacional de operadores móviles dentro de la GSMA con el fin de trabajar en conjunto en pos de evitar que personas y organizaciones usen el entorno móvil para consumir o lucrar a partir de CSAM.

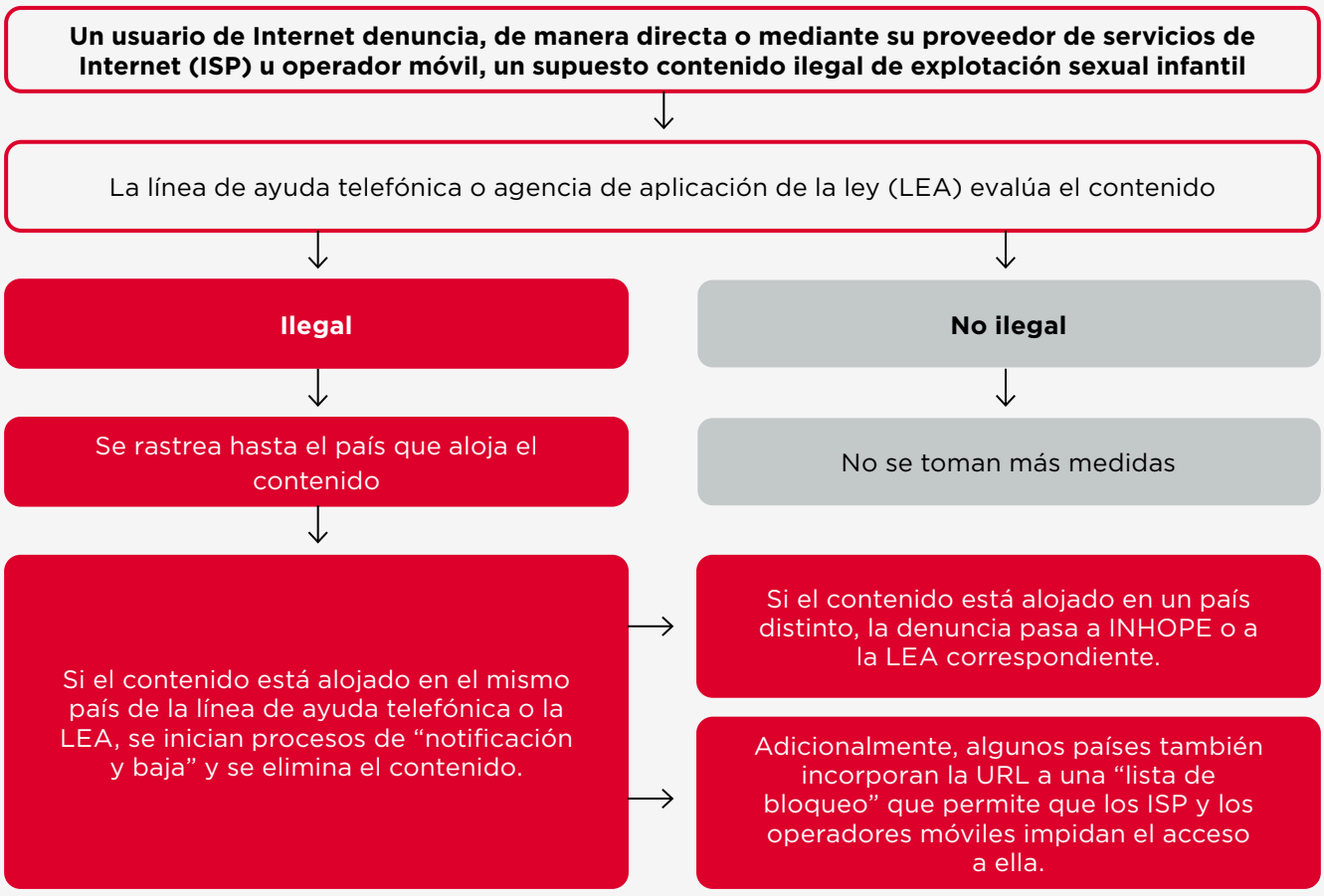
Los miembros de la Alianza Móvil se comprometieron a combatir el CSAM mediante una serie de acciones, como la implementación de procesos de "notificación y baja" para permitir la eliminación de cualquier CSAM publicado en sus propios servicios. Otras acciones incluyen el apoyo o la promoción de líneas de ayuda u otros mecanismos para que los consumidores denuncien CSAM y medidas técnicas para restringir el acceso a URL o sitios web que, según una agencia competente y reconocida a nivel internacional, alojen CSAM.

Mediante una combinación de medidas técnicas, cooperación e intercambio de información, la Alianza Móvil trabaja para luchar contra el abuso y la explotación sexual infantil en línea en todo el mundo.

La Alianza Móvil también contribuye en labores más amplias para erradicar el CSAM en línea mediante la publicación de guías y herramientas para el beneficio de toda la industria móvil. Por ejemplo, elaboró una guía para la creación y la administración de una línea de ayuda en colaboración con INHOPE, una organización paraguas de líneas de ayuda, y una guía de procesos de "notificación y baja" en colaboración con UNICEF.

En profundidad

Ejemplo de cómo una línea de atención telefónica y sus socios gestionan una denuncia de contenido de explotación sexual infantil



Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Los dispositivos y los servicios móviles mejoran la vida y los derechos de los jóvenes. Todas las partes interesadas deben aceptar, promover y entender mejor esta perspectiva para asegurar que los jóvenes aprovechen al máximo los beneficios que ofrece la tecnología móvil. En marzo de 2021, el Comité de los Derechos del Niño (CDN) de la ONU

adoptó la Observación general N.° 25 relativa a los derechos de los niños en relación con el entorno digital.[17] Esta adopción es un hito importante en los derechos de la infancia, ya que se confirma por primera vez que los derechos de los niños aplican tanto dentro como fuera del entorno digital y que los gobiernos deben tomar medidas para aprovechar oportunidades y también para combatir riesgos.

La mejor estrategia para abordar la protección de la infancia en línea es mediante el esfuerzo de las partes interesadas para fomentar el uso seguro y responsable de los servicios en línea y los dispositivos de Internet por parte de niños y jóvenes, así como empoderar a los padres y encargados de cuidar niños para que se involucren y ayuden a proteger a los menores en el mundo digital.[18]

Asimismo, el conjunto de respuestas para abordar y combatir el CSAM incluye legislación adecuada, líneas de ayuda telefónica para hacer denuncias, el compromiso de las agencias de aplicación de la ley, acompañamiento a las víctimas, y medidas y procesos técnicos que apoyen todas las anteriores. Si bien los operadores de redes móviles desean tener un papel protagónico en ayudar a enfrentar este problema, por ejemplo, a través de la Alianza Móvil, necesitan el apoyo, el liderazgo y la rendición de cuentas de todos los demás organismos y agencias pertinentes para causar un impacto real.

La industria móvil repudia el uso indebido de sus servicios para distribuir CSAM.

- La Alianza Móvil contra Contenidos de Abuso Sexual Infantil de la GSMA ofrece liderazgo en esta área y trabaja de manera proactiva para combatir el uso indebido de las redes y los servicios móviles por parte de delincuentes que buscan acceder o distribuir CSAM.[19]
- Los operadores de redes móviles recurren a términos y condiciones, procesos de "notificación y baja" y canales de denuncia para mantener sus servicios libres de este tipo de contenido.[20]
- La industria móvil se compromete a colaborar con las agencias de aplicación de la ley y las autoridades competentes para facilitar la rápida remoción o inhabilitación de casos confirmados de contenido ilegal alojado en sus servicios,[21] incluido el CSAM.

Los gobiernos nacionales deben ser abiertos y transparentes respecto de qué tipo de contenido es ilegal en su país, antes de trasladar la responsabilidad de aplicar la ley a las líneas de ayuda telefónica, agencias de seguridad y la industria, sujetas a procesos legales.[22] No obstante, estas iniciativas proactivas no deben extenderse a acciones que violen los tratados internacionales de derechos humanos o la responsabilidad del sector privado, según se define en los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas. Los gobiernos pueden hacer su parte con iniciativas como la Alianza Mundial WePROTECT y consultar su Respuesta Nacional Modelo o su Herramienta de Seguridad Infantil en Línea, una guía útil hecha a partir de una recopilación de directrices internacionales para dar apoyo al desarrollo de estrategias y respuestas gubernamentales relativas a la seguridad en línea.[23]

17 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
18 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Los niños y la tecnología móvil
19 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Contenido ilegal
20 ibíd.
21 ibíd.
22 ibíd.
23 http://www.weprotect.org/the-model-national-response/ y https://childonlinesafetytoolkit.org/

Dispositivos robados y falsificados

Robo y tráfico de dispositivos móviles

La naturaleza de los dispositivos móviles (pequeños, portátiles y de alto valor) junto a la información que almacenan los hacen atractivos para los delincuentes. Consecuentemente, se ha desarrollado un mercado clandestino internacional para la comercialización de *smartphones* y otros dispositivos móviles robados. Los encargados de la formulación de políticas públicas de muchos países expresan preocupación sobre las consecuencias del robo de dispositivos móviles y la participación del crimen organizado en la exportación masiva de dispositivos robados y falsificados, los cuales generalmente cruzan fronteras para explotar oportunidades de arbitraje de precios y para sortear las iniciativas de bloqueo nacionales. A fin de hacer frente a este tipo de actividad y quitar valor a este tráfico ilícito, los operadores móviles deben intercambiar información dentro de un mismo país y también con otros países.

Prevención del robo y tráfico de dispositivos móviles

La GSMA coordina un sistema de intercambio de información entre los operadores móviles mediante su servicio de Registro de Dispositivos[24] para prevenir que los dispositivos móviles denunciados como robados se conecten a cualquier otra red móvil del mundo. También ofrece a las agencias de aplicación de la ley y otros organismos la capacidad de identificar si un dispositivo se denunció como perdido, robado o falsificado.

La recomendación de la GSMA es que los operadores móviles desplieguen la capacidad de bloquear la conexión de dispositivos denunciados como perdidos o robados, o en otras circunstancias aprobadas.[25] Apenas una víctima informe a su proveedor de servicios móviles que su dispositivo ya no está en su poder, el operador puede actuar rápidamente para prevenir que dicho dispositivo acceda a la red. Para combatir satisfactoriamente el tráfico de teléfonos robados, sería ideal que el dispositivo robado quede bloqueado y no pueda conectarse a ninguna red.

Si un dispositivo robado no puede conectarse, su valor en el mercado clandestino resulta significativamente reducido. El bloqueo de dispositivos también puede utilizarse para limitar servicios que no son de red, como el de aseguramiento y reparación.

Los esfuerzos de la industria para bloquear el uso de dispositivos robados comienzan con el Identificador Internacional de Equipo Móvil (IMEI) asignado a cada dispositivo móvil. El Registro de Dispositivos de la GSMA lleva una lista central de los dispositivos denunciados como perdidos o robados, la cual se conoce como “Lista de Bloqueo de la GSMA”. Los operadores móviles que están conectados a ella cuentan con una lista siempre actualizada de identificadores de dispositivos, y se los alienta a denegar el acceso a la red a tales equipos.[26] De esta manera, el Registro de Dispositivos de la GSMA permite que los operadores móviles de todo el mundo impidan que los dispositivos robados y transportados a otros países puedan tener acceso a la red.

La Lista de Bloqueo se basa en información recopilada a partir de operadores móviles, fabricantes de dispositivos y otras organizaciones aprobadas por la GSMA que fabrican, aseguran o venden dispositivos móviles.

24 https://www.gsma.com/services/deviceregistry/
25 https://www.gsma.com/services/deviceregistry/
26 Otros casos en los que se aprueba el bloqueo de dispositivos son: dispositivos robados, fallados u obtenidos de manera fraudulenta; indicios de IMEI duplicado; o bloqueos ordenados por un tribunal.

Las Prácticas recomendadas para el bloqueo de dispositivos y el intercambio de datos de la GSMA[27] exponen las mejores prácticas para que los operadores móviles bloqueen dispositivos en sus redes.

Si bien la GSMA no gestiona los datos personales asociados a los dispositivos móviles, en el marco de una regulación de privacidad de datos cada vez más amplia, se recomienda que los operadores móviles procesen los datos de identificación de los dispositivos, como el IMEI y la información en la Lista de Bloqueo de la GSMA, como si fueran datos personales. Únicamente los operadores pueden vincular el IMEI de un dispositivo móvil a su propio cliente, por lo que cada operador móvil es responsable de respetar las leyes y los principios de la industria que regulan la protección de datos y la privacidad.

Actualmente, más de 125 operadores móviles utilizan el servicio de Registro de Dispositivos de la GSMA, ayudando a proteger a más de 1.000 millones de clientes móviles. En América Latina, donde el robo de dispositivos es común, la mayoría de los operadores móviles en 18 países comparte datos de dispositivos a través de la GSMA con este propósito. De todos modos, un dispositivo bloqueado por todos los operadores móviles en una región podría usarse en otra ubicación si un operador de ese lugar no usa la Lista de Bloqueo global. El robo y la venta de dispositivos móviles es un problema mundial que solo podrá atenuarse una vez que la mayoría de los operadores haya adoptado esta práctica.

El bloqueo de IMEI depende de que los fabricantes implementen el IMEI de manera segura para evitar la alteración o falsificación. El Registro de Dispositivos de la GSMA también permite registrar casos de IMEI duplicados y alerta a los operadores acerca de dispositivos falsificados. Los fabricantes más importantes del mundo apoyan dos iniciativas clave de la GSMA para robustecer la seguridad de los IMEI: la definición de los principios de diseño técnico para la implementación segura de los IMEI, y la participación en el Proceso de Denuncia y Corrección de Debilidades de Seguridad del IMEI de la GSMA.

Algunos fabricantes de dispositivos podrían llevar a cabo más acciones para mejorar la integridad del IMEI, que es esencial para el bloqueo efectivo del dispositivo. Los operadores móviles y otros grandes proveedores y vendedores de dispositivos móviles pueden tomar sabias decisiones de compra al elegir qué dispositivos vender a sus consumidores, teniendo como consideración clave la implementación de seguridad del IMEI. Es importante el trabajo en conjunto de todas las partes interesadas (fabricantes, operadores móviles, gobiernos y consumidores) para garantizar la plena integridad del IMEI y la oportuna resolución de problemas que puedan surgir.

Se recomienda que los gobiernos penalicen la alteración no autorizada de IMEI en dispositivos móviles (también conocida como reprogramación o adulteración de IMEI). Algunos países, como la India, Canadá y el Reino Unido, tipificaron penalmente el acto de cambiar el IMEI de un dispositivo móvil tras su fabricación. Se recomienda que otros países sigan sus pasos y sancionen proactivamente a quienes obvien los controles de seguridad.

Para que más partes interesadas puedan combatir los delitos relacionados con los dispositivos, la GSMA brinda servicios, incluida la Verificación de Dispositivos de la GSMA,[28] que permite que partes habilitadas, como las agencias de aplicación de la ley, los comerciantes de dispositivos y las aseguradoras, verifiquen el estado de los dispositivos consultando la Lista de Bloqueo de la GSMA y, en algunos casos, alerten sobre dispositivos robados.

El servicio de Verificación de Dispositivos de la GSMA también ofrece a las empresas de reciclaje la oportunidad de identificar y eliminar dispositivos denunciados como robados o perdidos por los operadores participantes antes de que entren en el proceso de reciclado. El reciclaje de teléfonos celulares, tablets y otros dispositivos móviles se ha convertido en un gran negocio que reutiliza millones de unidades cada año. Sin embargo, con este crecimiento también aumentó el riesgo de robo y pérdida de dispositivos. Si las compañías de reciclaje de dispositivos aceptan dispositivos robados o perdidos, su reputación se ve comprometida y aumentan los costos y las pérdidas.

Otra forma de impedir el robo de dispositivos móviles es el interruptor de desactivación, o "*kill switch*", el cual desactiva funciones cruciales de los dispositivos. Por ejemplo, los fabricantes de dispositivos pueden incluir software de seguridad en el sistema operativo de un *smartphone* para que el usuario pueda desactivarlo de manera remota en caso de robo y así hacer que el software quede inoperativo. Luego, el dispositivo solo se puede reactivar si su propietario legítimo lo autoriza. El documento Requisitos de funciones antirrobo para dispositivos elaborado por

27 Comúnmente, esto se logra mediante la implementación de un Registro de Identidad de Equipos (EIR) basado en estándares. https://devicecheck.gsma.com/fs45/FS.45_v2.0

28 https://www.gsma.com/services/tac/about-device-check/

la GSMA define un conjunto de funciones que pueden aplicar los propietarios de dispositivos para localizar, inhabilitar y rehabilitar sus dispositivos en caso de extravío, pérdida o robo.[29]

Figura 4
Unidos contra el robo de dispositivos móviles

Implicancias clave para los gobiernos, Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

La GSMA pretende restringir la venta y el uso de dispositivos robados o perdidos, por lo que ofrece conocimiento experto y recursos a los gobiernos, la industria y otras partes interesadas que quieran desarrollar soluciones locales de manera colaborativa.

Es esencial que las principales partes interesadas tengan un enfoque colaborativo:

- El usuario puede denunciar el robo de su dispositivo ante su proveedor de servicios, habilitar las funcionalidades antirrobo en su dispositivo y, en países donde los operadores están conectados al Registro de Dispositivos de la GSMA, utilizar el IMEI para verificar el estado del dispositivo que planea comprar.
- Los operadores móviles pueden bloquear dispositivos robados desde sus redes, conectarse al Registro de Dispositivos para compartir la Lista de Bloqueo y motivar a sus proveedores de dispositivos a que protejan adecuadamente la integridad de las implementaciones de IMEI en sus productos.
- Los fabricantes de dispositivos pueden diseñar equipos más seguros (p. ej., hacer imposible la reprogramación de IMEI) e implementar la funcionalidad de interruptor de desactivación para que los usuarios puedan inhabilitar de manera remota sus dispositivos perdidos o robados.
- Los propietarios de tiendas de aplicaciones y los operadores pueden obtener los IMEI de dispositivos robados a partir de la lista de la GSMA y usarlos para denegar el acceso a las tiendas de aplicaciones a aquellos dispositivos que hayan sido denunciados como robados.

29 GSMA, 2016. Anti-Theft Device Feature Requirements, Version 3.0

— Los gobiernos pueden promulgar legislación que penalice la reprogramación no autorizada de IMEI y apoyar de otras maneras los esfuerzos de la industria y las agencias de aplicación de la ley para combatir el robo de dispositivos.

— Los reguladores pueden alentar a las redes locales a conectarse al Registro de Dispositivos de la GSMA para compartir información sobre dispositivos robados, proporcionar servicios de verificación de IMEI para que el usuario pueda constatar el estado de un dispositivo antes de comprarlo, y crear un entorno regulatorio favorable para la implementación de soluciones efectivas y fáciles para el consumidor, a fin de combatir el robo de dispositivos.

— Las agencias de aplicación de la ley pueden aprovechar el libre acceso a la información de dispositivos robados procurada por la GSMA y destinar recursos suficientes para garantizar la identificación y el procesamiento de los delincuentes.

Es importante evitar soluciones que puedan ser menos efectivas o tener consecuencias negativas:

— El uso de listas de bloqueo es la mejor solución, a nivel de red, para prevenir el uso de dispositivos perdidos o robados.

— Se debe evitar el uso de soluciones que no estén basadas en estándares para combatir el robo de dispositivos móviles, debido a que son patentadas y su implementación suele ser compleja y costosa. Los métodos que van en contra de los estándares móviles mundiales, como la vinculación de un dispositivo específico a un determinado usuario móvil, suelen ser difíciles de cumplir para los usuarios y sus proveedores de servicios, y podrían causar varios problemas jurídicos complejos y limitar la competencia.

— La creación de una base de datos nacional para la identificación de dispositivos es costosa e innecesaria. Los servicios de Verificación de Dispositivos y Registro de Dispositivos de la GSMA pueden satisfacer las necesidades de bloqueo e información sobre dispositivos. Además, es preferible mantener un único repositorio global de información sobre los aparatos, ya que así se garantiza la coherencia, un intercambio de datos más amplio y se evita la fragmentación, lo cual podría, en última instancia, debilitar la efectividad de todos los métodos.

Colombia y Ecuador revierten algunas iniciativas contra el robo de dispositivos

Los operadores móviles de América Latina estuvieron entre los primeros en adoptar políticas para identificar y bloquear el acceso a la red de dispositivos robados o no autorizados. Contribuyendo hace casi una década al Registro de Dispositivos de la GSMA y bloqueando equipos denunciados. Solo durante 2021, se bloquearon casi 5 millones de dispositivos en América Latina usando el Registro de Dispositivos de la GSMA, lo que representa aproximadamente un 40 por ciento de la actividad en la Lista de Bloqueo global.

Como respuesta a la magnitud del problema, algunos gobiernos de la región optaron por tomar más medidas y establecieron sistemas y procesos nacionales para controlar la importación de terminales móviles y el uso de dispositivos robados. Sin embargo, puede que las nuevas complejidades creadas por estas iniciativas públicas representen una carga para los operadores y un obstáculo para la adopción por parte de los consumidores, mientras se logran, en el mejor de los casos, resultados poco significativos. Colombia y Ecuador, por ejemplo, son países que reconsideraron su visión original.

Colombia

En Colombia, la autoridad de telecomunicaciones, llamada Comisión de Regulación de Comunicaciones (CRC), junto con el Ministerio de TIC y operadores móviles, implementó un sistema para identificar, registrar y gestionar el acceso de los dispositivos a las redes móviles del país y para establecer un proceso de bloqueo de aquellos identificados como robados. Esta estrategia basada en el IMEI, fue pionera en la región al ser implementada por primera vez en 2011.

Para sentar las bases normativas, la CRC promulgó una serie de resoluciones abarcando temas como el intercambio de información entre operadores móviles y asignando a los operadores la responsabilidad legal y financiera de una base de datos centralizada. Dicha base de datos consistía en una “lista positiva” de todos los dispositivos móviles importados y adquiridos de manera legal, y de ese modo, aprobados para su uso en el país; junto con los nombres de los propietarios registrados de cada dispositivo, y una “lista negativa” de dispositivos a los que se les debía denegar el acceso a la red.

Lamentablemente, además de introducir el riesgo a la filtración de datos, la recopilación y reporte de esta información suponía una gran carga para su cumplimiento y creaba una barrera para la venta o traspaso de equipos. Como resultado, el admirable esfuerzo del gobierno por resolver este grave problema social no tuvo éxito ni logró hacer una diferencia y, a la vez, impuso obligaciones costosas al ecosistema móvil. Más de una década después, viendo que los resultados no justificaban los costos, Colombia está reevaluando la situación y podría eliminar por completo las exigencias de registro de equipos, como parte de un esquema general de simplificación normativa.

Case Study

Ecuador

El regulador de Ecuador decidió implementar una lista positiva que incluía los códigos de asignación de tipo (TAC) de dispositivos móviles legítimos y aprobados, bloqueando entonces los IMEIs inválidos. No obstante, durante el confinamiento por COVID-19 entre 2019 y 2020, el gobierno decidió flexibilizar la restricción, ya que reconoció que representaba un posible obstáculo para que los ciudadanos adopten los servicios de comunicación móvil. Actualmente, reanudará la política de bloqueo, pero añadirá un periodo de gracia de 30 días para que los usuarios puedan adquirir otro dispositivo.

Las moralejas de estos casos destacan la importancia de hacer análisis de impacto rigurosos que ayuden a los reguladores a lograr un equilibrio entre la seguridad del consumidor y la facilidad de acceso al servicio móvil.

Cómo impedir la venta y el uso de dispositivos falsificados

Un dispositivo móvil falsificado infringe expresamente la marca comercial o el diseño de un producto "de marca" original o auténtico, incluso cuando hay una mínima variación en el nombre comercial.

Por su naturaleza ilícita, estos dispositivos móviles generalmente son despachados y vendidos por redes de crimen organizado en mercados clandestinos. Como resultado, los consumidores y los gobiernos no tienen mucha consciencia sobre la verdadera magnitud y el impacto del tráfico de dispositivos móviles falsificados. Según un informe publicado en 2017 por EUIPO y la UIT sobre el costo económico de la violación de los DPI en el sector de los *smartphones*, el impacto mundial de la venta de *smartphones* falsificados en 2015 se calculó en 184 millones de unidades, valuadas en EUR 45.300 millones (12,9 por ciento de las ventas totales).[30]

30 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study11/smartphone_sector_en.pdf

La falsificación de dispositivos móviles es un delito que viola la propiedad intelectual y las normas de comercio legítimo, provoca pérdidas en los ingresos de los fabricantes y en la recaudación tributaria de los gobiernos.

Los consumidores también se ven afectados por el tráfico de dispositivos falsificados. En muchos mercados, la prevalencia de los dispositivos falsificados puede ser tan alta que el consumidor ni siquiera sabe que el dispositivo es falsificado y lo compra sin darse cuenta. Más allá de la mala experiencia de servicio frecuentemente asociada a los dispositivos falsificados, se ha denunciado que muchos de estos dispositivos contienen materiales peligrosos para el medio ambiente. Por ejemplo, varios estudios midieron los niveles de plomo en las soldaduras de las juntas que exceden los límites permitidos a nivel mundial. Tales dispositivos representan una amenaza para el medioambiente si no se los desecha siguiendo procesos ambientales idóneos.

No es fácil identificar y bloquear los dispositivos móviles falsificados porque muchos tienen un IMEI que parece legítimo. Para ayudar a resolver este problema, la base de datos de dispositivos de la GSMA puede ser útil en la detección de discrepancias entre el IMEI de un dispositivo y las características registradas que debería tener tal dispositivo si fuese original. Los dispositivos que tengan IMEI inexistentes o inválidos se añaden a la lista de bloqueo. Sin embargo, en el caso de los IMEI que pertenezcan a dispositivos legítimos pero hayan sido usados en productos falsificados, será difícil diferenciar y separar el dispositivo original del falso.

Además, los dispositivos falsificados solo se pueden bloquear después de que el consumidor, a menudo sin saberlo, compra el dispositivo móvil falsificado e intenta conectarlo a la red móvil.

Una acción disruptiva, como el bloqueo del dispositivo ya comercializado, generalmente castiga al consumidor inocente y no al comerciante de productos falsificados. Las medidas que se tomen no deberían causar ningún inconveniente al usuario inocente ni resultar disruptivas para el mercado legítimo mientras los falsificadores y comerciantes ilegales siguen aprovechándose de la situación. Las autoridades correspondientes deberían atacar específicamente la fabricación y distribución de dispositivos falsificados para sacarlos de circulación antes de que lleguen a un consumidor desprevenido.

En 2016, la GSMA y la Organización Mundial de Aduanas (OMA) se aliaron para colaborar en la lucha contra la falsificación y el tráfico fraudulento de dispositivos móviles. Según su acuerdo, los funcionarios aduaneros de la OMA pueden acceder a la base de datos de la GSMA para verificar y filtrar los dispositivos falsificados en el punto de importación. No obstante, esta solución no se puede aplicar a aquellos dispositivos móviles que obvian los procesos aduaneros, en cuyo caso las aduanas y las agencias de aplicación de la ley deben enfocarse en el tráfico ilegal. Debido a la complejidad de este asunto, los esfuerzos de las agencias de seguridad por combatir la distribución y venta de dispositivos falsificados no han resultado suficientes para contener el problema. Es limitado el efecto que ha tenido la legislación y regulación nacional actual, puesto que la distribución de dispositivos falsificados se da, por lo general, a escala internacional, y las iniciativas de cada país por separado son fáciles de evadir.

Adicionalmente, no hay evidencia de que sea efectivo establecer registros nacionales de dispositivos autorizados para combatir la venta y el uso de dispositivos falsificados.

Dicha estrategia podría impedir la libre circulación de dispositivos móviles en el mundo y, en algunos países, se consideraría ilegal. En cambio, es necesario el desarrollo de soluciones globales de múltiples partes interesadas, como se explica a continuación.

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

La GSMA reconoce los problemas que plantea la falsificación de dispositivos para los usuarios, los operadores, los fabricantes legítimos y los gobiernos, y apoya la necesidad de conservar la integridad del mercado de dispositivos móviles. La GSMA está dispuesta a trabajar con sus miembros, los gobiernos y otras partes interesadas para desarrollar soluciones efectivas para combatir la producción y oferta de dispositivos falsificados.

Es esencial la colaboración entre las partes interesadas:

- Los reguladores pueden trabajar con los fabricantes de dispositivos y los operadores móviles para entender el alcance de la penetración de dispositivos falsificados y acordar las medidas que se deberían tomar para no penalizar a los fabricantes de dispositivos legítimos ni a los usuarios víctimas de los falsificadores.
- Los gobiernos pueden desmantelar el mercado clandestino de dispositivos mediante la reducción de tarifas e impuestos aduaneros a los dispositivos legítimos importados. Hacerlo reduciría el costo de los dispositivos legítimos. Además, pueden apoyar los programas de concientización y educación del consumidor para exponer los riesgos que conlleva comprar un dispositivo falsificado.
- Las agencias aduaneras pueden verificar en los puntos de importación si los dispositivos contienen identificadores legítimos mediante el acceso gratuito a la información de IMEI en el Registro de Dispositivos de la GSMA.
- También deberían centrar su atención y recursos en la identificación y el procesamiento de los delincuentes.
- Los fabricantes de dispositivos pueden trabajar en conjunto con los gobiernos, los reguladores y las agencias aduaneras en educar a las partes interesadas acerca de los dispositivos falsificados y ofrecer inteligencia sobre las actividades relacionadas con su fabricación, distribución y venta a las autoridades correspondientes.
- Los operadores móviles pueden utilizar la Base de Datos de Dispositivos de la GSMA para obtener la lista definitiva de identificadores de dispositivos legítimos y luego, si fuese necesario, denegar el acceso a todo dispositivo identificado como falsificado.
- El usuario puede verificar la legitimidad del dispositivo que piensa comprar a través de los servicios de verificación que ofrezcan otras partes interesadas, en los casos en que estuvieran disponibles.

Es importante evitar soluciones que puedan ser menos efectivas o provocar consecuencias negativas no deseadas:

- Se debe evitar el uso de soluciones que no estén basadas en estándares para combatir los dispositivos móviles falsificados, dado su carácter patentado y el hecho de que su implementación es, por lo general, costosa y difícil a nivel técnico. Los métodos que van en contra de los estándares móviles mundiales, como la vinculación de un dispositivo específico a un determinado usuario móvil, suelen uelen ser difíciles de cumplir pudiendo llegar a tener implicancias legales y de limitación de la competencia.

Fraude con dispositivos móviles

El fraude puede llevarse a cabo de muchas formas. Algunas de ellas utilizan los dispositivos móviles como canal. Aquí se incluyen ataques como el fraude de servicios (p. ej., fraude de identidad o de dinero móvil), el *spam* móvil[31] y, cada vez más, estafas de "ingeniería social" (p. ej., *phishing*, *SMiShing ovishing*), por los que se engaña a la víctima para que revele información sensible sobre su persona y los servicios que consume, sin que se dé cuenta de que su seguridad está siendo puesta en peligro.

El año 2020 planteó desafíos sin precedentes, dado que la pandemia de COVID-19

favoreció un entorno de oportunidades para los estafadores, en forma de consumidores nuevos en el mundo digital, vulnerabilidades y ansiedades exacerbadas y nuevos canales para explotar.

El fraude de ingeniería social manipula e influencia a una persona para que lleve a cabo acciones perjudiciales, como revelar datos personales o contraseñas. Una vez que tienen acceso a la información privada, los delincuentes pueden registrarla y utilizarla para

cometer otros tipos de fraude, como el robo de identidad y el fraude bancario. Usualmente, los estafadores que interactúan con sus víctimas entablan una relación de confianza con ellas, a veces haciendo uso de información disponible públicamente. Durante la pandemia, delincuentes en el Reino Unido enviaban mensajes de texto, correos electrónicos o hacían llamadas haciéndose pasar por organizaciones confiables, como el Servicio Nacional de Salud (NHS), la policía o el gobierno, para engañar a las personas y hacer que revelen su información personal y financiera.

Este tipo de fraude está en auge y la agencia de policía internacional INTERPOL lo identificó como una de las tendencias fraudulentas emergentes en el mundo. Por ejemplo, el fraude y los delitos cibernéticos cometidos en el Reino Unido representaron más del 50 por ciento del crimen en general y una pérdida financiera total de GBP 1.260 millones en 2020.[32] El éxito de estas estafas reside en que los delincuentes convencen a la víctima de que son legítimos, ya sea en persona o mediante un servicio o sitio web. Las soluciones tecnológicas ofrecen cierta defensa: por ejemplo, los operadores móviles adoptaron las técnicas recomendadas por la GSMA para detectar y afrontar la transmisión internacional de *spam* móvil fraudulento.

Con menor frecuencia hoy en día, los sistemas de correo de voz se usaron como medio para comprometer la seguridad de los usuarios móviles permitiendo que partes no autorizadas escuchen los mensajes de correo de voz o hagan llamadas fraudulentas. Dado que los sistemas de correo de voz pueden ser utilizados para realizar fraudes, la GSMA ha proporcionado directrices para operadores y consumidores sobre cómo asegurarse de que se implemente una autenticación robusta del usuario para proteger sus cuentas de correo de voz, garantizando que solo el usuario legítimo tenga acceso a los servicios correspondientes, de manera tal que se logre un equilibrio entre usabilidad y seguridad.

La GSMA ofrece a sus miembros una gran cantidad de conocimiento experto y servicios de seguridad mediante actividades que, de manera colectiva, construyen una base de saber, directrices y servicios que logran una resiliencia en la seguridad de la red móvil más robusta. El Grupo de Seguridad y Fraude (FASG)[33] de la GSMA tiene como propósito mantener o mejorar la protección de la tecnología y la infraestructura de los operadores móviles, así como también de la identidad, la seguridad y la privacidad del consumidor, de manera tal que la reputación de la industria móvil siga siendo sólida y los operadores móviles continúen siendo socios confiables en el ecosistema. El Centro de Análisis e Intercambio de Información de las Telecomunicaciones (T-ISAC)[34] de la GSMA es el nodo central para el intercambio de información de seguridad de la industria de las telecomunicaciones. Aprovechando el conocimiento colectivo de los operadores móviles, los distribuidores y los profesionales de seguridad, el T-ISAC recopila y difunde información y consejos acerca de incidentes de seguridad dentro de la comunidad móvil, de manera confiable y anonimizada. La GSMA promueve el intercambio de

31 El *spam* móvil hace referencia a los mensajes móviles masivos no solicitados. La mayor parte del *spam* tiene el fin de engañar y estafar al usuario y depende del modelo de cobro implementado (es decir, hay una barrera baja para el emisor si el cobro se hace al receptor).

32 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1015382/Crime-plan-v10.pdf y https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

33 https://www.gsma.com/aboutus/workinggroups/fraud-security-group

34 https://www.gsma.com/security/t-isac/

información para luchar contra todo tipo de fraudes, incluido el fraude en la red. Los operadores móviles pueden reducir los efectos negativos al compartir sus rangos de números de alto riesgo tan rápida y ampliamente como sea posible.

Así, los operadores pueden crear y mantener un recurso global preciso de los números de alto riesgo.[35] A tal efecto, la GSMA colabora con organizaciones como la Asociación de Control de Fraude en Comunicaciones (CFCA)[36] y el Foro de Fraude en Telecomunicaciones del Reino Unido (TUFF)[37].

Sin embargo, el comportamiento humano también es un elemento central del problema del fraude móvil, por lo que es clave la educación sobre cómo proteger la información personal y la concientización sobre las posibles amenazas a fin de minimizar los riesgos. Los operadores de redes móviles están bien posicionados para ayudar a educar a los consumidores acerca de la necesidad de mantenerse alertas y atentos. De todos modos, los proveedores finales de servicios, como los bancos y los minoristas, deberían destacar mensajes más específicos, ya que son los más aptos para ofrecer y aplicar medidas técnicas de seguridad relacionadas con sus servicios.

Para apoyar a los operadores móviles en esta tarea, la GSMA recomienda tres principios rectores[38] para la elaboración de mensajes al consumidor sobre este problema:

1. **El mensaje debe ser relevante y específico.**
2. **El mensaje debe ser simple y fácil de entender.**
3. **El mensaje se debe reforzar durante toda interacción con el consumidor.**

Terminología

Ejemplos de fraude basado en ingeniería social:

Phishing: método utilizado para infectar una computadora o un dispositivo móvil y acceder a valiosa información personal. El *phishing* generalmente utiliza las comunicaciones, como el correo electrónico, para incitar a las personas a entrar a sitios web o servicios que simulan ser auténticos para extraer su información personal.

SMiShing: o "*SMS phishing*" es el uso de mensajes de texto para enviar un "señuelo" que luego conduce a las personas a divulgar su información personal.

Vishing*:* los estafadores persuaden a la víctima a suministrar información personal o transferir dinero, por teléfono, haciéndose pasar por un servicio legítimo, como un banco.

Cambio fraudulento de SIMe ingeniería social de personal de centros de llamadas: los estafadores hacen que la SIM de la víctima se reasigne a ellos para obtener acceso a la cuenta de teléfono celular de la víctima y, subsecuentemente, acceder a una serie de cuentas con las que la víctima interactúa, como bancos, comercios, y agencias de viajes

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

El fraude es un problema complejo en todas sus formas y ya es ilegal en la mayoría de los países. Las medidas de los operadores de redes móviles solo pueden influenciar la conducta del consumidor a fin de mitigar y prevenir los riesgos de fraude. La legislación y la regulación deben centrarse en los culpables; la educación y la concientización deben ser las principales maneras de promover la habilidad del consumidor de protegerse a sí mismo. Particularmente, en los mercados donde hay un bajo nivel de conocimiento tecnológico, el consumidor de hoy en día no aprovecha al máximo las funciones de protección tecnológicas disponibles.

35 https://www.gsma.com/services/fis-hrn/
36 https://cfca.org/
37 https://www.tuff.co.uk/
38 L. Gilman, 2012. "Mitigating the risk of fraud through consumer communication", GSMA

— Es importante que los proveedores finales de servicios (p. ej., los bancos en el caso de los servicios de dinero) implementen los más altos niveles de seguridad adecuados para su mercado.

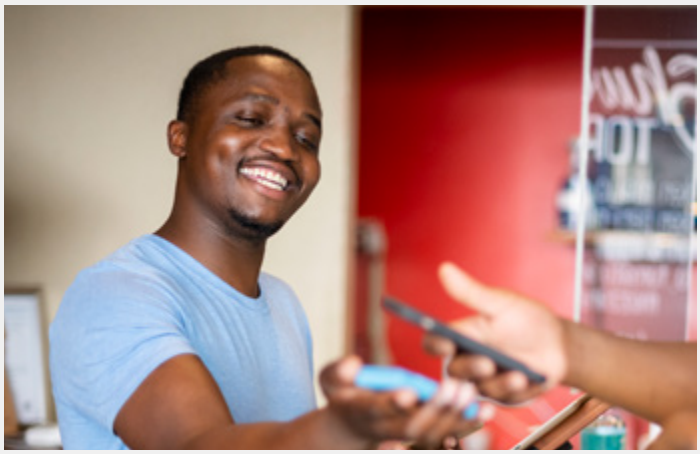
— Los controles preventivos, como las campañas de concientización para mejorar la educación y la protección del consumidor, deben utilizarse y fomentarse para minimizar la exposición al fraude.

— Los operadores de redes móviles deben diseñar fuertes estrategias de gestión de riesgos para mitigar los riesgos de fraude. Las medidas que se tomen y el nivel de implementación estarán determinados por las evaluaciones de amenazas de cada operador y serán específicas para los servicios que cada uno ofrezca y los consumidores de su mercado.

Caso de estudio

Gestión de riesgos de dinero móvil: comunicación con el consumidor

El caso del servicio M-PESA de Safaricom es un ejemplo de cómo se utilizaron las comunicaciones como herramienta para ayudar a prevenir el fraude relacionado con el dinero móvil. Una de las prioridades del servicio M-PESA de Safaricom es mitigar los riesgos de estafas al consumidor. Además de las medidas reactivas, y en lugar de intentar usar solo controles de detección (es decir, monitorear y denunciar tendencias posteriormente), Safaricom recurre en gran medida al control preventivo para reducir el riesgo de dichas estafas. Safaricom concluyó que el control preventivo más efectivo es la concientización del consumidor a través de comunicaciones claras. En 2021, Safaricom lanzó una campaña de concientización del consumidor para proteger a las partes interesadas contra el robo de identidad y el fraude basado en ingeniería social. En una campaña de gran tirada, se destacaron estos problemas bajo el eslogan “Jichanue and Take Control”, que recurrió a la radio, la televisión y los canales digitales. Creó Escuadrones de Gestión de Fraudes especializados en realizar análisis, concientizar a los consumidores y revisar los procesos para impulsar la seguridad del cliente mediante un uso acelerado de *machine learning* y automatización, concientización continua sobre fraudes a clientes y revisión de procesos. Para el éxito de Safaricom en la gestión de fraudes a los consumidores de M-PESA[39], fue vital aumentar la concientización de los consumidores a través de comunicaciones claras.



La comunicación con el consumidor es una herramienta que debe utilizarse como parte de una estrategia de gestión de riesgos más amplia y que debe complementarse con datos, paneles de control relevantes, y procedimientos internos definidos. Por ejemplo, la GSMA desarrolló un marco integral de gestión de riesgos de dinero móvil y un conjunto de herramientas para operadores.

El informe de la GSMA titulado “Cybersecurity: A governance framework for mobile money providers” proporciona un marco integral que pueden usar los proveedores de servicios de dinero móvil para mejorar la seguridad y brindar salvaguardas contra el ciberdelito. Dicho marco tiene tres dimensiones: las personas, los procesos y la tecnología. Brinda una guía para que los proveedores de dinero móvil garanticen la seguridad de sus operaciones y sus clientes.[40]

39 Consulte el informe anual y los estados financieros de 2021 de Safaricom
40 https://www.gsma.com/mobilefordevelopment/resources/cybersecurity-a-governance-framework-for-mobile-money-providers/

03

Capítulo 3

Protección de la privacidad del consumidor

Para materializar los beneficios de la innovación impulsada por datos para la sociedad y la economía, las personas deben empoderarse y confiar en que sus datos personales están debidamente protegidos.

Protección de la privacidad del consumidor

El objetivo principal de la protección de la privacidad es generar confianza en que los datos privados están protegidos de forma adecuada, y conforme con la regulación y los requerimientos de privacidad aplicables. Para lograrlo, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y consistencia en todos los servicios, sectores y geografías.

Los gobiernos pueden ayudar a garantizar este resultado y, a la vez, ofrecer la flexibilidad necesaria para la innovación, mediante la adopción de marcos legales basados en los riesgos, para así salvaguardar los datos privados y promover prácticas de gobernanza digital responsables que estén alineadas con la regulación local. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para proteger y respetar los intereses de privacidad del consumidor y facilitar la toma de decisiones informadas sobre qué datos personales se recopilan y cómo se utilizan, mediante la implementación de políticas que promuevan lo siguiente:

- El almacenamiento y procesamiento seguro de toda la información personal y privada, conforme a los requisitos legales, cuando corresponda.
- La transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y en pleno cumplimiento de las exigencias legales.
- La entrega de información y herramientas para que el consumidor pueda tomar decisiones simples y significativas sobre su privacidad.

Esta última década fue testigo del enorme incremento en el enriquecimiento de los servicios de comunicaciones. La propia naturaleza de estos servicios implica que las empresas de Internet que los proveen tienen acceso a mucha información sobre los usuarios, desde su identidad, con quién se comunican y su ubicación hasta datos sobre sus intereses personales, extraídos de los sitios y servicios a los cuales acceden.

Los proveedores de servicios en línea pueden analizar las comunicaciones, como las palabras ingresadas en los motores de búsqueda o las ubicaciones buscadas en una aplicación de mapas, y combinar todos estos datos para inferir intereses e intenciones.

El uso de la tecnología se hace cada vez más ubicuo y la privacidad del consumidor sigue estando en el centro de la atención. Los operadores móviles utilizan apenas un conjunto limitado de datos personales para prestar los servicios de comunicación; mientras que otras empresas del ecosistema de Internet hacen un uso más intenso de la información personal.[41] Si bien los usuarios no siempre se dan cuenta de esto, muchos de los servicios en línea son gratuitos porque el proveedor puede usar los datos personales para vender publicidades u ofrecer servicios pagos al usuario. Esta sección aborda la recopilación de datos del usuario en todo el ecosistema de Internet y la forma en que se almacenan y utilizan, cómo se accede a ellos, y cuáles son las implicancias para la privacidad.

Las áreas de análisis específicas son las siguientes:

- **Recopilación y uso de datos, con foco en el sustento a la innovación**
- **Elección del consumidor, con foco en la incorporación de la posibilidad de elección en servicios y aplicaciones en línea**
- **Flujo transfronterizo de datos, reconociendo las preocupaciones de seguridad nacional**

Cada una de estas cuestiones conlleva varias implicancias importantes para los gobiernos, la industria y otras partes interesadas. Dichas implicancias se detallan minuciosamente en este capítulo.

Recopilación y uso de datos

La GSMA prevé que habrá 1.600 millones de conexiones adicionales de *smartphones* para 2025, lo que llevará al nivel general de adopción de *smartphones* a más del 80 por ciento de las conexiones móviles totales.[42] A medida que la conectividad sea más fluida y flexible, la tecnología 5G modificará de maneras inesperadas los tipos de servicios y modelos de negocio posibles, así como la economía de intercambio y las aplicaciones cambiaron la forma en que interactuamos con organizaciones, gobiernos y otras personas. Aumentará el volumen y la granularidad de los datos de tráfico y ubicación que se generen durante comunicaciones 5G y las nuevas aplicaciones basadas en datos que hagan uso de 5G podrían resultar en mayores volúmenes y variedad de uso de datos personales.

Si bien el 5G representa un cambio considerable en el uso de las redes móviles, los regímenes de privacidad de datos existentes que tienen neutralidad tecnológica ya abarcan un amplio rango de usos de los datos recopilados a través de aplicaciones, sistemas operativos de dispositivos móviles, redes sociales, sitios web y operadores de red. Por lo tanto, es probable que sean suficientes para cubrir el uso de nuevas capacidades 5G dentro del ecosistema en línea.[43]

Sin embargo, investigaciones muestran que los consumidores se preocupan por su privacidad y quieren garantías de que pueden confiarles sus datos a las empresas. Un estudio de la GSMA realizado en 2019 determinó que los consumidores de Europa y EE. UU. en particular son reacios a compartir datos personales, independientemente del propósito:

- Más de dos tercios de los encuestados estaban muy o relativamente preocupados por la privacidad de sus datos; la mitad de ellos estaban más preocupados en ese momento que en 2018.

41 Informe de la GSMA: The Internet Value Chain 2022 https://www.gsma.com/publicpolicy/wp-content/uploads/2022/05/Internet-Value-Chain-2022.pdf
42 Informe de la GSMA: 5G in Context, Q1 2022 Data-driven insight into areas influential to the development of 5G, mayo de 2022
43 5G y privacidad de los datos https://www.gsma.com/publicpolicy/resources/5g-and-data-privacy

— La mayoría de ellos se sentían incómodos con el uso de sus datos personales para publicidad segmentada o servicios personalizados (en promedio, 90 y 84 por ciento de los encuestados europeos y estadounidenses, respectivamente).

— Lo mismo sucede cuando se trata de otros propósitos, incluso ayudar a las empresas con la innovación de sus productos, obtener algún tipo de beneficio financiero o ayudar a la innovación por el bien público. Al menos 75 por ciento de los encuestados rechazaron compartir datos con estos propósitos.[44]

Al considerar cuestiones en torno a la recopilación y el uso de datos personales, es importante hacer dos distinciones clave:

— Las leyes de privacidad, cuando las hubiere, varían de una jurisdicción a otra. Si bien el Reglamento General de Protección de Datos de la Unión Europea creó un punto de referencia para muchos países, no existe un marco interoperable a nivel mundial. A menudo, las organizaciones regidas por estas leyes tienen presencia internacional, lo que puede generar incertidumbre respecto de la base de referencia legal pertinente y plantear más complicaciones si el proveedor de servicios almacena y procesa los datos en un país tercero.

— La segunda distinción tiene que ver con el operador móvil y los servicios y aplicaciones en línea provistos por terceros, a los que los usuarios pueden acceder a través de la red. Estas organizaciones de terceros no están sujetas a las leyes y obligaciones de licencias relacionadas con la protección de la privacidad que sí se aplican a los operadores móviles.

Terminología

Datos personales: pueden significar muchas cosas para muchas personas en el universo en línea. Existen diferentes significados según las leyes, pero no es el propósito del presente documento reinterpretar la ley. Habiendo dicho esto, cuando aquí se usa el término "datos personales", se incluye, entre otras cosas, la información que se relaciona con una persona física y que:

— se recopila directamente del usuario (p. ej., el usuario la ingresa en la interfaz de usuario de una aplicación y puede incluir su nombre, dirección y detalles de la tarjeta de crédito);

— se recopila indirectamente (p. ej., número de teléfono celular, dirección de correo electrónico, nombre, sexo, fecha de nacimiento, datos de ubicación, dirección IP, IMEI, identificación única del teléfono);

— tiene que ver con la conducta del usuario (p. ej., datos de ubicación, datos de uso de servicios y productos, visitas a sitios web);

— el usuario genera y que se conserva en su dispositivo (p. ej., registros de llamadas, mensajes, imágenes generadas por el usuario, listas de contactos o libretas de direcciones, notas y credenciales de seguridad).

Usuario: cuando aquí se hace referencia al usuario, generalmente significa el usuario final del dispositivo móvil que comienza a utilizar una aplicación o servicio y que puede ser o no el "cliente" de un proveedor de servicios o aplicaciones.

44 GSMA Intelligence: Encuesta Consumer Insights Survey, 2019

Las normas que rigen el uso de datos personales varían considerablemente de un sector a otro, de una tecnología a otra y de un país a otro. Esto puede resultar desconcertante para aquellos que, con razón, esperan la misma protección independientemente de quién use sus datos y cómo los procese. Además, es posible que las leyes se vuelvan obsoletas rápidamente debido al cambiante y dinámico ecosistema digital, donde el tradicional enfoque sectorial es cada vez menos relevante.

Las inconsistencias en los requerimientos de privacidad en los diferentes servicios y aplicaciones pueden causar una experiencia en la que el usuario, sin saberlo, permita el fácil acceso a sus datos personales, exponiéndolo a resultados no deseados.

Asimismo, algunas prácticas de los servicios y aplicaciones en línea hacen que el consumidor "dé su consentimiento" a términos y condiciones de privacidad sin que el usuario lea el aviso ni entienda las implicancias de sus decisiones. Según New Scientist, las políticas de privacidad son cuatro veces más largas que hace 25 años.[45] Debido a la distinción confusa entre operadores móviles y otros servicios a los que accede el usuario a través de sus dispositivos móviles, existe el riesgo de que el consumidor no sepa quién gestiona sus datos y, en algunos casos, crea que su privacidad tendrá una mejor protección que la que realmente tiene.

En profundidad

Big data e IA

El aumento en el poder de cómputo, la reducción de los costos y los avances en el análisis de datos, la IA de *machine learning* y disciplinas asociadas hacen posible procesar y analizar enormes volúmenes de datos.

De esta forma, se puede extraer información importante, cuando corresponda, a partir de meras correlaciones de datos, en lugar de tener que identificar conexiones causales. Estas capacidades, a las que se refiere como técnicas de análisis de *big data*, representan un cambio abismal en la capacidad de la sociedad de no solo crear nuevos productos y servicios sino también de resolver algunas de las necesidades de políticas públicas más urgentes de nuestro tiempo, desde la gestión vial en zonas urbanas congestionadas y contaminadas hasta la comprensión y prevención de la propagación de enfermedades.

Los operadores móviles usan cada vez más los datos que recopilan y acceden a datos contextuales a partir de otras fuentes, como parte de servicios de *big data*.

Por lo tanto, deben desempeñar un papel importante como administradores responsables de estos datos y, potencialmente, como facilitadores del acceso a este tipo de datos en un futuro mercado.

En la práctica, el análisis de *big data* y la IA se pueden usar para hallar patrones comunes en grandes conjuntos de datos mediante el uso de técnicas estadísticas que agrupan grandes cantidades de usuarios, dispositivos y datos. Por eso, estas técnicas estadísticas pueden considerarse, en gran medida, como técnicas de mejora de la privacidad cuando son aplicadas correctamente.

Con la colaboración de representantes del ecosistema móvil, la GSMA identificó salvaguardas que pueden ser adoptadas por las organizaciones para identificar y reducir los riesgos de privacidad al participar en servicios o proyectos que involucren el análisis de *big data*.[46] Además, la GSMA desarrolló una conjunto de herramientas (toolkit) digital que describe los componentes necesarios para implementar soluciones móviles basadas en datos.[47]

A medida que se acelera la adopción de la IA, será vital que los sistemas de IA estén diseñados, desarrollados y desplegados de manera ética. La GSMA brinda principios que, cuando se aplican en conjunto con las leyes, las regulaciones y los principios de privacidad existentes, como los Principios de Privacidad Móvil de la GSMA, pueden ayudar a mitigar los riesgos éticos y de privacidad asociados a la IA. Asimismo, la IA se encuentra en el centro de los modelos operativos y de negocio de una cantidad cada vez mayor de operadores de redes móviles. El Libro de Ética de IA de la GSMA es una herramienta práctica para ayudar a que las organizaciones puedan diseñar, desarrollar y desplegar la IA con ética.

45 https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/
46 https://www.gsma.com/publicpolicy/resources/mobile-privacy-big-data-analytics
47 https://aiforimpacttoolkit.gsma.com/

Caso de estudio

Durante la pandemia de COVID-19 en Nigeria, se implementaron estrictas medidas para contener la propagación del virus. Antes del COVID-19, aproximadamente cuatro de cada 10 personas de Nigeria vivían por debajo de la línea nacional de pobreza, con millones más que vivían apenas por encima, lo que los hacía vulnerables a caer por debajo fácilmente. MTN colaboró con el Foro de Gobernadores de Nigeria para usar conocimientos basados en datos para crear las medidas de respuesta y planificación de recursos. Fueron limitados pero indicativos los datos que se proporcionaron para garantizar la privacidad de los clientes, lo cual fue suficiente para producir los conocimientos necesarios. Los conjuntos de datos se utilizaron para predecir los peores panoramas de infección en cada estado y dar apoyo a los comités de salud mediante decisiones de planificación de recursos locales. El análisis predictivo utilizado anonimizó y agregó los datos de redes móviles, combinados con conjuntos de datos de referencia geoespacial extraídos de repositorios de datos públicos de código abierto y aplicados a un modelo epidemiológico. A partir de este análisis, se identificaron las geografías con las poblaciones más vulnerables a través de la aplicación de transacciones de dinero móvil anonimizadas y agregadas.[48]

La privacidad del consumidor en la recopilación y el uso de datos

La GSMA elaboró un conjunto de Principios de Privacidad Móvil que describen la forma en que se debería respetar y proteger la privacidad del consumidor móvil cuando se utilizan aplicaciones y servicios que tienen acceso, usan o recopilan sus datos personales. Estos principios no reemplazan ni sustituyen la legislación aplicable, pero se basan en los preceptos de privacidad y protección de datos reconocidos y aceptados internacionalmente.[49] El objetivo de estos principios es lograr la protección de la privacidad de las personas, asegurar que se las trate de manera justa y, a la vez, permitir que las organizaciones alcancen sus metas comerciales, sociales y de políticas públicas. En términos generales, son lo suficientemente flexibles como para incorporar las nuevas tecnologías y métodos de negocios a medida que van surgiendo. De los nueve principios, seis son especialmente relevantes para la recopilación y el uso de los datos personales:

- **Apertura, transparencia y notificación**
- **Seguridad**
- **Propósito y uso**
- **Infancia y adolescentes**
- **Minimización y retención de datos**
- **Rendición de cuentas y aplicación**

48 https://www.gsma.com/betterfuture/wp-content/uploads/2021/03/GSMA-AI4I-Covid-Response-Report_March2021.pdf
49 GSMA Mobile Privacy Principles (2016) http://www.gsma.com/publicpolicy/mobile-privacy-principles

Principios de Privacidad Móvil de la GSMA

Apertura, transparencia y notificación

Las personas responsables deben ser abiertas y honestas con los usuarios garantizandoles información clara, prominente y oportuna acerca de sus prácticas de privacidad de datos e identidad. Los usuarios deben recibir información sobre las personas que recopilen su información personal, los propósitos para hacerlo de una aplicación o servicio, y acerca del acceso, recopilación, distribución y otros usos de dicha información personal, incluyendo a quién puede ser revelada, para permitir así a los usuarios tomar decisiones informadas acerca del uso de una aplicación o servicio móvil.

Propósito y uso

El acceso, recopilación, distribución, divulgación y otros usos de la información personal del usuario estarán limitados a fines comerciales legítimos, como la provisión de aplicaciones o servicios solicitados por el usuario o para cumplir con las obligaciones legales correspondientes.

Elección y control del usuario

El usuario debe tener la oportunidad de hacer una elección significativa y tener el control de su información personal.

Respeto por los derechos del usuario

El usuario debe recibir información sobre sus derechos en el uso de su información personal y tener una manera sencilla de ejercer tales derechos.

Minimización y retención de datos

Solo se debe recopilar, acceder o usar aquella información personal necesaria para cumplir los propósitos comerciales y prestar, mantener o desarrollar las aplicaciones o servicios. La información personal no debe retenerse por más tiempo del necesario para cumplir los propósitos comerciales o las obligaciones legales. Luego de dicho tiempo, la información debe ser eliminada o anonimizada.

Seguridad

La información personal debe estar protegida mediante salvaguardas razonables y adecuadas a la sensibilidad de tal información.

Educación

El usuario debe recibir información sobre los problemas de privacidad y seguridad y las maneras de gestionar y proteger su privacidad.

Children and Adolescents

Una aplicación o servicio dirigidos a niños o adolescentes debe garantizar que la recopilación, el acceso y el uso de la información personal sean adecuados en todas las circunstancias posibles y sean compatibles con la legislación nacional.

Rendición de cuentas y aplicación

Todos los responsables deben rendir cuentas para garantizar el cumplimiento de estos principios.

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

La GSMA y sus miembros están convencidos de que la privacidad y la seguridad son fundamentales para que el consumidor confíe en los servicios móviles y se comprometen a trabajar con todas las partes interesadas de la industria móvil para elaborar una estrategia coherente para proteger la privacidad. En el caso de los servicios que ellos mismos prestan a sus usuarios, los operadores móviles velarán por proteger las identidades digitales, la seguridad de las comunicaciones y los datos personales. El amplio rango de servicios prestados por terceros disponibles en los dispositivos móviles brinda diferentes grados de protección de la privacidad. Por lo tanto:

— A fin de que el consumidor tenga la confianza de que sus datos personales estarán protegidos, independientemente del servicio o el dispositivo, se debe implementar un nivel coherente de protección.

— Las salvaguardas necesarias deben provenir de una combinación de enfoques acordados a nivel internacional, legislaciones nacionales y acciones de la industria.

Desde la perspectiva de transparencia e información al consumidor, la industria, las autoridades de protección de datos y otros reguladores deberían:

— Ser claros con el consumidor sobre qué se protege y qué debe esperar en términos de privacidad.

— Dejar en claro qué cosas no se pueden controlar, como es el caso de las aplicaciones y servicios de terceros. Para un consumidor informado, esto puede ser obvio pero, para muchos consumidores de distintos segmentos, no lo es.

Al momento de formular o revisar la legislación y la regulación:

— Los gobiernos deben asegurar que la legislación sea neutra respecto de los servicios y la tecnología para que sus normas se apliquen de forma coherente a todas las entidades que recopilan, procesan y almacenan datos personales.

— Debido al alto nivel de innovación en los servicios móviles, la legislación debe enfocarse en el riesgo general de la privacidad de las personas en lugar de intentar legislar sobre tipos de datos específicos. Por ejemplo, el mismo elemento de datos se puede utilizar para obtener un valor comercial (p. ej., se vende a organizaciones de terceros), operativo (p. ej., ayuda a determinar la toma de decisiones interna y la asignación de recursos) o público (p. ej., ayuda a planificar las respuestas de recuperación tras una catástrofe).

Elección del consumidor

Empoderando al consumidor para que pueda elegir

Muchos servicios en línea son ofrecidos a los consumidores de forma gratuita, ya que el proveedor obtiene sus ganancias mediante flujos de publicidad en dicho servicio. Para maximizar dichos flujos, la mayoría de los servicios en línea, desde sitios web hasta aplicaciones personalizadas, utilizan la información del usuario para que los anunciantes que deseen llegar a ese perfil realicen ofertas para publicar un anuncio (en diferentes formatos) frente a él.

Este tipo de microsegmentos y subastas de milisegundos son cada vez más frecuentes y dependen de que el proveedor de servicios utilice la información específica del usuario que haya comprado u obtenido en forma directa. Indudablemente, se debe lograr un equilibrio entre la entrega de cierta información a cambio del uso de servicios gratuitos. Sin embargo, es importante que el usuario pueda tomar decisiones claras e informadas respecto de los datos que comparte. Un estudio realizado en nombre de la GSMA demuestra que los usuarios móviles quieren opciones simples y claras para controlar el uso de su información. La GSMA y sus miembros trabajaron estrechamente para abordar proactivamente desafíos clave de la privacidad móvil y, como parte de ello, se encomendó una investigación global sobre más de 11.500 usuarios móviles (Brasil, Colombia, Indonesia, Malasia, Singapur, España y el Reino Unido). Los hallazgos determinan que los usuarios móviles de estos países comparten actitudes y preocupaciones similares respecto de su privacidad.[50] El estudio indicó que a más del 80 por ciento de los usuarios de Internet móvil les preocupa compartir sus datos personales al acceder a aplicaciones o servicios. Además, antes de instalar una aplicación, la mayoría (65 por ciento) de los usuarios intentan saber qué información quiere obtener la aplicación desde sus dispositivos, lo que demuestra un deseo de entender cómo se ve afectada la privacidad. La mayoría de los usuarios móviles (81 por ciento) también quieren que se les pida permiso antes de que terceros accedan a sus datos personales alojados en sus dispositivos móviles. También quieren tener más control sobre los tipos de datos a los que las empresas pueden acceder.

50 El documento "Mobile Privacy: Consumer research insights and considerations for policymakers" expone los principales hallazgos de la investigación y analiza las implicancias para los formuladores de políticas públicas. Para ver el informe, visite http://www.gsma.com/publicpolicy/mobile-privacy-consumer-research-insights-and-considerations-for-policymakers

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Tres de los nueve Principios de Privacidad Móvil elaborados por la GSMA tienen particular relevancia en la elección que el cliente haga respecto de su información personal:

- Elección y control del usuario: el usuario debe tener la oportunidad de realizar elecciones significativas y tener control de su información personal.
- Respeto por los derechos del usuario: el usuario debe recibir información sobre sus derechos en el uso de su información personal y tener una manera sencilla de ejercer tales derechos.
- Educación: el usuario debe recibir información sobre los problemas de privacidad y seguridad y las maneras de gestionar y proteger su privacidad.

Sin embargo, incluso cuando estos principios se cumplen plenamente, solo pueden ayudar un poco en la tarea de brindar al consumidor el nivel de elección requerido. Los operadores móviles no influyen sobre los términos y condiciones de privacidad que usan los proveedores de servicios en línea. Existe el riesgo de que nuevas leyes y regulaciones tengan el efecto no deseado de sobrecargar al usuario móvil y exacerbar la "fatiga de la privacidad" que puede generarse cuando se le pide al usuario aceptar condiciones que en realidad no leyó o no entendió.

En cuanto a los servicios que ofrecen, los operadores móviles deben procurar contar con políticas de privacidad claras y facilitar la comprensión y el control sobre el uso de los datos personales.

La GSMA se compromete a trabajar con las partes interesadas de toda la industria móvil para desarrollar una estrategia coherente para proteger la privacidad y promover la confianza en los servicios móviles.

Flujo transfronterizo de datos personales

El tercer aspecto de la privacidad del consumidor se relaciona con las jurisdicciones en las que se almacenan o donde se accede a los datos personales y las implicancias del flujo transfronterizo de datos. Por lo general, almacenar y procesar datos en ubicaciones centralizadas permite a los operadores móviles mejorar el desempeño y el aspecto económico en la provisión de servicios que podrían no ser viables si operaran en un solo país. Gracias a esto, el consumidor se beneficia de muchos servicios, innovaciones y soporte. Cuando los datos migran de un territorio a otro, se pueden plantear preguntas relativas a la jurisdicción legal adecuada. Los gobiernos pueden encontrar útiles a marcos y mecanismos de rendición de cuentas interoperables al momento de lidiar con desafíos jurisdiccionales y facilitar el flujo transfronterizo de datos.

Algunos marcos legales, como las Reglas de Privacidad Transfronteriza (CBPR) de APEC y las Normas Corporativas Vinculantes de la UE, establecen principios comunes internacionales, incluidos los mecanismos de rendición de cuentas, que rigen cómo deben gestionarse los datos al trasladarse entre distintos países. Sin embargo, el éxito de la adopción de estos principios se ve afectado por la implementación gubernamental de normas de "localización de datos" (también conocidas como "soberanía de datos") que imponen requerimientos locales de almacenamiento o uso de tecnología.[51] A menudo, los países imponen estos

51 Svantesson, D. (22-12-2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", Documentos de Economía Digital de la OCDE, N.° 301, OECD Publishing, París. http://dx.doi.org/10.1787/7fbaed62-en

requerimientos creyendo que es más fácil para las autoridades de supervisión inspeccionar los datos cuando se almacenan localmente.

Si bien algunas de estas normas procuran proteger la privacidad del individuo, también crean un conglomerado fragmentado de leyes y regulaciones que confunde y pone en riesgo los beneficios que ofrece una infraestructura de redes abierta. Estas normas de localización de datos también pueden tener un impacto negativo en el comercio digital y el crecimiento económico mundial. Por ejemplo,

la localización de datos causó un impacto negativo en el empleo y causó la pérdida de aproximadamente 205.000 puestos de trabajo en Brasil, 372.000 en Indonesia y 182.000 en Sudáfrica. El impacto adverso en las inversiones que causa el costo económico de las normas de localización de datos es aún más pronunciado: Brasil e Indonesia perdieron USD 5.000 millones y Sudáfrica, USD 4.000 millones.[52]

La privacidad y la seguridad en los flujos transfronterizos de datos

Las redes móviles generan grandes cantidades de datos. Para poder facturar a cada usuario por el servicio que usa, se registra y procesa cada llamada y transferencia de datos. Constantemente, se generan y almacenan datos sobre cargas de tráfico, registros de fallas o consultas del cliente (p. ej., cambio de tarifa, cambio de dirección). Como resultado, los operadores móviles dependen en gran medida de los servicios de centros de almacenamiento y procesamiento de datos.

Garantizar la integridad y la seguridad de esos datos es una tarea importante y requiere soluciones complejas. Para muchos operadores de redes móviles, en particular los que son subsidiarias de grupos internacionales o que eligen utilizar un proveedor externo, posiblemente la mejor solución sea alojar y procesar los datos de múltiples países en una única sede central. Así, pueden alcanzar economías de escala y crear una solución más robusta, con mejor funcionalidad, seguridad y más redundancia de la que sería posible en una estrategia fragmentada para un solo país. La centralización permite a los operadores desarrollar conocimientos técnicos más profundos e implementar soluciones de respaldo y redundancia que probablemente no serían económicamente viables, o ni siquiera posibles, para una única operación en un solo país.

Este tipo de soluciones implica transferir los datos del consumidor a los centros de datos multinacionales, que en muchos casos están ubicados en países distintos al del operador de red inicial.

Si bien los beneficios técnicos son evidentes, las implicancias legales son complejas. ¿De qué país son las normas de protección de datos que deberían aplicarse?: ¿las del país donde se procesan los datos, las del país del usuario final o las del país donde está ubicado el contralor de datos (p. ej., el operador móvil)?

Son varios los motivos por los cuales los países buscan imponer normas de localización de datos, entre ellos, la convicción de que las autoridades de supervisión pueden inspeccionar los datos almacenados localmente con mayor facilidad. Otro motivo común es el deseo de proteger la privacidad del individuo y asegurar que se cumplan las expectativas y los estándares de ese país: una forma obvia de hacerlo es exigir que los datos permanezcan en el país. No obstante, existen soluciones y principios que pueden mitigar estos riesgos sin restringir el flujo de datos y los beneficios que conlleva.

Las restricciones no necesariamente resultan en una mejor protección de los datos personales. La fragmentación genera una protección incoherente (p. ej., diferencias entre jurisdicciones y sectores respecto de lo que se puede almacenar y la duración de almacenamiento) y provoca confusión, afectando la gestión segura de los datos personales. La fragmentación que causa la localización también puede presentar obstáculos que hacen prohibitiva la inversión en la protección de la seguridad. En conjunto, esto puede socavar los esfuerzos de los operadores móviles por desarrollar tecnologías y servicios que mejoren la privacidad para proteger al consumidor.

52 Informe de la GSMA: Cross-Border Data Flows The impact of data localisation on IoT January 2021 https://www.gsma.com/publicpolicy/resources/cross-border-data-flows-the-impact-of-data-localisation-on-IoT

Es importante reiterar la distinción entre los datos personales, a los cuales tienen acceso y procesan los operadores móviles, y los datos personales recopilados y almacenados por proveedores de servicios en línea e intermediarios de Internet. Como se analiza en la sección sobre elección del consumidor, estos servicios son muy diferentes y el hecho de que sean operados desde fuera del país en el que se usan, en la mayoría de los casos, añade aún más complejidades legales. Aunque las inquietudes y cuestiones de privacidad son igual de relevantes, en este caso exceden el control de los operadores móviles, tanto en términos de datos transferidos por los usuarios como de la forma en que se puede acceder a ellos.

Un problema importante es que, en la actualidad, el flujo transfronterizo de datos está regulado por un mosaico de instrumentos y leyes internacionales, regionales y nacionales. Si bien todos los instrumentos adoptan principios comunes, no establecen un marco regulatorio interoperable que refleje la realidad, los desafíos y el potencial de un mundo conectado a escala global. Las normas de protección de datos deberían ser interoperables entre países y regiones en la mayor medida posible. La interoperabilidad crea una mayor seguridad y previsibilidad jurídica que facilita que las empresas desarrollen un marco escalable y responsable en materia de protección y privacidad de datos.

Los marcos de protección de datos interoperables ayudarían a fortalecer y promover mecanismos adecuados y eficaces para garantizar que en el manejo de los datos se protejan los derechos e intereses de los consumidores y los ciudadanos. Los marcos que incorporen mecanismos eficaces de rendición de cuentas pueden fortalecer y proteger derechos importantes que ayudan a las personas y las economías a prosperar. Por ejemplo, el trabajo para que el sistema CBPR de APEC y las Normas Corporativas Vinculantes de la UE sean interoperables puede traer beneficios para la industria, el comercio digital y los intereses y derechos de los consumidores.

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

El flujo internacional de datos cumple un papel importante en la innovación, la competencia y el desarrollo socioeconómico. Por lo tanto:

- Se debe minimizar toda restricción y condición impuesta sobre el flujo internacional de datos y aplicarse solamente en circunstancias excepcionales.
- Las normas de flujo transfronterizo de datos deben basarse en los riesgos y respaldar toda medida que asegure que el manejo de los datos se realice en base a salvaguardas adecuadas y proporcionales, a la vez que ayuden a materializar los potenciales beneficios socioeconómicos.
- Se deben promover y adoptar iniciativas regionales en materia de privacidad de datos en base a principios comunes. Tales iniciativas deben permitir los flujos de datos interregionales y ser interoperables con los trabajos de APEC y la UE y otros esfuerzos nacionales similares.
- Si los gobiernos necesitan analizar datos para fines sociales, deben hacerlo a través de medios lícitos y mecanismos intergubernamentales adecuados que no restrinjan el flujo de datos.

Los operadores móviles reconocen la preocupación relacionada con mantener la seguridad y la protección de los datos, y en ayudar a asegurar que los derechos de las personas no se vean perjudicados. También reconocen los desafíos más amplios que plantea la vigilancia nacional e internacional. Sin embargo:

- Los gobiernos deberían imponer medidas que restrinjan el flujo transfronterizo de datos solo cuando sea absolutamente necesario para lograr un objetivo legítimo de política pública.
- La aplicación de estas medidas debe ser proporcional, no arbitraria ni discriminatoria respecto de proveedores o servicios extranjeros.

La GSMA y sus miembros mantienen su compromiso de trabajar con todas las partes interesadas a fin de garantizar que el flujo transfronterizo de datos se maneje de forma tal que los datos personales y la privacidad de los individuos estén protegidos. Asimismo, la GSMA y sus miembros reconocen la importancia de afrontar toda cuestión relacionada con el flujo transfronterizo de datos, incluyendo cuestiones jurisdiccionales.

La industria móvil tiene la convicción de que los flujos transfronterizos de datos son esenciales para brindar beneficios a personas, organizaciones, gobiernos y a la economía, tanto a nivel nacional como internacional. Identificar los beneficios de la libre circulación de los datos no implica que sugerimos que esta área no debería estar regulada. Muchos formuladores de políticas públicas, organizaciones y la sociedad civil comparten la opinión de que una sólida regulación en materia de privacidad de datos puede facilitar los flujos de datos y proteger a los ciudadanos, haciendo que consumidores y formuladores de políticas públicas puedan confiar en los productos y servicios digitales. Para obtener los beneficios destacados en este documento, la GSMA motiva a que los gobiernos actúen en base a las siguientes recomendaciones[53]:

53 https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf

Recomendación 1: Comprometerse a facilitar los flujos transfronterizos de datos y eliminar medidas de localización innecesarias

Los gobiernos deberían asumir el compromiso de facilitar los flujos transfronterizos de datos y eliminar medidas de localización innecesarias para poder materializar los beneficios de su libre circulación, para las personas, los negocios y los gobiernos.

El compromiso del sector público, ya sea a nivel nacional o en el contexto de un organismo regional o multilateral, puede marcar el camino y la visión estratégica para estimular la economía digital nacional y motivar la armonización en toda la región. En los casos en que, aún así, las medidas de localización avancen, los gobiernos deberían consultar con las partes interesadas sobre cómo se interpretarán e implementarán tales medidas.

Recomendación 2: Garantizar que los marcos de privacidad sean adecuados para la era digital

Los formuladores de políticas públicas deberían garantizar que los marcos legales aborden de manera efectiva las preocupaciones de protección de datos en su país. Estos marcos deberían describir el derecho a la privacidad del ciudadano y las obligaciones impuestas a las organizaciones al momento de recopilar, analizar, procesar y almacenar los datos.

Para que sean adecuados para la era digital, los marcos de políticas públicas nacionales deberían basarse en "los principios básicos de la protección de datos que se encuentran en el centro de la mayoría de las leyes y los regímenes [de privacidad] nacionales"[54].

Estos enfoques deberían reflejar las preocupaciones del consumidor sobre la privacidad y la seguridad de los datos[55] y operar de forma neutral en sector y tecnología para que el consumidor tenga la garantía de que sus datos se procesan coherentemente. También deberían contemplar la creación y la provisión de recursos para una autoridad nacional de protección de datos. La regulación en materia de privacidad debería centrarse en los riesgos de daños al individuo e incorporar medidas para garantizar la rendición de cuentas de las organizaciones que recopilan datos y, a la vez, brindar la flexibilidad de implementación para que las organizaciones puedan innovar rápidamente, volverse escalables y reducir los costos de producción.

Recomendación 3: Revisar las normas de privacidad heredadas o de legado específicas del sector

Históricamente, los operadores han sido frecuentemente sujetos a restricciones de flujos internacionales de datos. Los operadores de telecomunicaciones tienen como propósito principal conectar a las personas independientemente de su ubicación y la distancia que las separe. Si bien las comunicaciones comenzaron con los telegramas y evolucionaron a llamadas de voz, mensajes de texto y correos electrónicos, ahora implican el intercambio de datos a gran escala, y la infraestructura y servicios de los operadores transportan esos datos. Considerando que los datos son un motor impulsor de la economía digital, ya no tiene sentido tener un trato diferente entre los datos de operadores de telecomunicaciones y aquellos generados por otros proveedores de comunicaciones electrónicas o, de hecho, por la economía digital en general. La adopción de un marco de privacidad nacional que sea apto para la era digital representa una oportunidad para revisar las normas heredadas del sector en materia de privacidad para evaluar si aún se necesitan.

54 UNCTAD, Normativa de protección de datos y flujos internacionales de datos: implicaciones para el comercio y el desarrollo, 2016. Consulte: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

55 Consulte la investigación publicada por la GSMA: https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf

Recomendación 4: Fomentar las iniciativas regionales en materia de privacidad de datos

Algunas organizaciones supranacionales, como APEC y la UE, ya han adoptado modelos regulatorios para la protección de los datos y la privacidad, mientras se garantiza que los datos puedan circular libremente en toda la región correspondiente. Estos modelos ofrecen una respuesta proporcional y eficaz para los formuladores de políticas públicas que desean proteger a la ciudadanía y los consumidores y, a la vez, apoyar el comercio internacional futuro de productos y servicios físicos y digitales.

Deberían incentivarse e implementarse iniciativas regionales de privacidad de datos basadas en principios comunes. Tales iniciativas deberían respaldar los flujos interregionales de datos y ser interoperables con los enfoques existentes de APEC y la UE[56] y otros enfoques nacionales semejantes. Deberían también desarrollar capacidad regulatoria en la privacidad de datos y el desarrollo de las mejores prácticas de la industria sobre procesamiento de datos. Así, se crearía confianza entre los países, se facilitaría el intercambio de mejores prácticas entre formuladores de políticas y se habilitaría a los reguladores de la privacidad a detectar y abordar más fácilmente los problemas de incumplimiento.

El abordaje regional de cuestiones de privacidad y seguridad nacional de los consumidores facilitará el flujo transfronterizo de datos y ofrecerá mecanismos de gobernanza de datos para garantizar la rendición de cuentas de la industria tanto a escala nacional como internacional.

Recomendación 5: Evitar la localización abordando con pragmatismo las cuestiones de vigilancia extranjera

Los gobiernos deberían considerar una gama de opciones disponibles para proteger los datos que se consideran sensibles, en lugar de imponer la localización. Entre estas se incluyen el cifrado, la anonimización y la agregación. En algunos casos, hasta podría considerarse la especificación de centros regionales para tipos de datos específicos.

Recomendación 6: Evitar la localización abordando con pragmatismo las cuestiones de aplicación de la ley y seguridad nacional

Los gobiernos deberían participar en iniciativas, como el Protocolo Adicional al Convenio sobre Ciberdelincuencia de Budapest, la ley CLOUD de EE. UU., y la propuesta eEvidence de la UE, para proporcionar marcos claros y predecibles que brinden certeza jurídica a las organizaciones, y un acceso más directo y oportuno a datos en el extranjero a las autoridades, eliminando la necesidad de medidas de localización.

Adoptar estas recomendaciones logrará lo siguiente:

- Permitir que la economía digital opere eficientemente y aporte beneficios socioeconómicos más rápidamente y en muchas naciones y regiones.
- Brindar a las personas acceso a una gama de servicios globales de buena calidad, superando las restricciones de los mercados nacionales, si las hubiere.
- Permitir que los negocios, incluidos los operadores de telecomunicaciones, adopten estrategias de transformación digital impulsada por datos para reducir costos y, consecuentemente, los precios de los productos digitales y físicos del mercado.

56 En especial, ser interoperables con las Reglas de Privacidad Transfronteriza (CBPR) de APEC, las Normas Corporativas Vinculantes (BCR) de la UE y el modelo de referencia en común establecido por un grupo de trabajo conjunto entre APEC y la UE.

04

Capítulo 4

Protección de la seguridad pública

Las redes móviles son fundamentales para la infraestructura crítica nacional y cumplen un papel importante en la protección del público general y la sociedad en su conjunto.

Protección de la seguridad pública

En línea con el objetivo general de proteger la seguridad pública, los operadores de redes móviles deben asumir responsabilidades adicionales y colaborar con las agencias de aplicación de la ley, conforme a las leyes, la regulación, las obligaciones relativas a las licencias y la legislación local. Es importante que los gobiernos garanticen la existencia de un marco legal proporcional que describa claramente las facultades de las que disponen las agencias nacionales de aplicación de la ley. Dicho marco legal debe garantizar también la necesidad y proporcionalidad de las solicitudes de asistencia, las cuales deben estar dirigidas al proveedor de tecnología o de servicios de comunicaciones más apropiado y ser compatibles con los principios de derechos humanos. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores cumplirán toda obligación, establecida por ley o por licencias, relacionada con temas de protección o seguridad pública en los países en los que operan, a la vez que darán su apoyo en cuestiones de derechos humanos. Además, colaborarán con las agencias de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- Working with the relevant agencies when specific situations require, to develop and implement appropriate solutions to achieve the end objective with minimal disruption to consumers and critical services.
- Building networks that have the functionality to address emergency and security situations, where appropriate.
- Being clear about the limit of action we can take over the value chain, and highlighting where others' actions should be undertaken.

or ejemplo, los servicios de emergencia que responden a acontecimientos graves dependen de las redes móviles para comunicarse entre sí, mientras que el público usa los dispositivos móviles para informar los incidentes que ocurren.

De conformidad con la legislación local y las obligaciones de licencias móviles, los operadores de redes móviles deben asistir a las agencias de aplicación de la ley en su labor de proteger la seguridad pública. Por ejemplo, como parte de una investigación penal, se puede otorgar una orden La

Declaración Universal de los Derechos Humanos (DUDH)[57] y el Pacto Internacional de Derechos Civiles y Políticos (PIDCP)[58] reconocen que todas las personas del mundo tienen derecho a comunicarse entre sí en privado y también a la libertad de expresión, dentro del ámbito, los límites y la moral

pública de cualquier Estado. Los instrumentos internacionales de derechos humanos también establecen que estos derechos pueden ser coartados solo en circunstancias muy acotadas y previamente definidas y que toda limitación debe ser siempre necesaria y proporcional a la amenaza percibida.

Pueden existir tensiones entre los objetivos de seguridad nacional y de aplicación de la ley para proteger la seguridad pública y los derechos a la privacidad, a la libertad de expresión y al acceso a la información. Estas necesidades potencialmente opuestas resultan en muchos países, en la postura comúnmente aceptada en la que las personas deben ser capaces de comunicarse libremente mientras que los bloqueos e intervenciones deben ser excepciones necesarias y proporcionales, sujetas al debido proceso legal. La mayoría de los países cuenta con salvaguardas para that individuals should be evitar el abuso y el uso excesivo de las facultades capaces de socavar la privacidad de la comunicación.

Esta sección destaca tres ejemplos típicos de intervenciones de la seguridad pública y los problemas que surgen entre las diferentes partes en la práctica:

- **Solicitudes de asistencia para la aplicación de la ley, con foco en la necesidad de transparencia y salvaguardas**
- **Restricción de servicio, con foco particular en el uso de inhibidores de señal móvil**
- **Registro de usuarios, con foco en el registro de usuarios de tarjetas SIM prepagas**

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y otras partes interesadas, las cuales también se describen más adelante en este capítulo.

Solicitudes de asistencia para la aplicación de la ley

Cumplimiento de las solicitudes de asistencia para la aplicación de la ley

Por lo general, las licencias otorgadas a operadores de redes móviles les imponen obligaciones para que colaboren con las actividades de aplicación de la ley y seguridad nacional del país que las emite. Cuando existen, esas leyes y obligaciones contenidas en las licencias suelen requerir que los operadores de redes móviles retengan datos[59] sobre el uso que el consumidor hace de los servicios móviles y los compartan con las agencias de aplicación de la ley, conforme a un requerimiento legal.

Además, deben tener la capacidad de interceptar las comunicaciones del consumidor en tiempo real, previa solicitud legal.

57 La Declaración Universal de los Derechos Humanos (DUDH) fue proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 como un ideal común para todos los pueblos y naciones. La Declaración establece, por primera vez, los derechos humanos fundamentales que deben protegerse en el mundo entero. El derecho a la privacidad se recoge en el Artículo 12 y el derecho a la libertad de expresión, en el Artículo 19. Consulte la DUDH en: http://www.un.org/en/universal-declaration-human-rights/

58 El Pacto Internacional de Derechos Civiles y Políticos (PIDCP) es un tratado multilateral adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966 y está en vigencia desde el 23 de marzo de 1976. El derecho a la privacidad se recoge en el Artículo 17 y el derecho a la libertad de expresión, en el Artículo 19. Consulte el PIDCP en: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en

59 En 2014, el Tribunal de Justicia de la Unión Europea (TJUE) declaró inválida la Directiva y dictaminó que la "conservación general de datos personales" según lo exige la Directiva sobre la Conservación de Datos de la UE violaba el derecho a la privacidad establecido en la Carta de los Derechos Fundamentales de la Unión Europea. En diciembre de 2016, el TJUE confirmó su posición y determinó que las leyes nacionales que se corresponden con la Directiva sobre la Conservación de Datos violan el acervo de la UE.

Usualmente, las leyes definen las condiciones y, en algunos casos, los procesos conforme a los cuales las agencias de aplicación de la ley pueden solicitar a un operador de redes que otorgue acceso o información sobre las comunicaciones llevadas a cabo en su red. También brindan un punto de referencia legal

que funciona como guía para los operadores móviles sobre cómo responder a estas solicitudes. En noviembre de 2016, el Reino Unido aprobó una nueva legislación[60] que aclara estos límites. Si bien existen diferentes posturas respecto de si las facultades que la nueva legislación otorga a los organismos de seguridad del Reino Unido son aceptables o no, lo importante es que las normas se debatieron y promulgaron públicamente. Es posible que en algunos países falte claridad en el marco legal para la regulación de la divulgación de datos o la interceptación legítima de las comunicaciones de los consumidores, lo cual plantea un desafío para la industria al momento de intentar proteger la privacidad de la información del consumidor y al mismo tiempo cumplir con las obligaciones de las licencias de asistir a las agencias de aplicación de la ley.

En los últimos años, se mantuvo un importante debate público a nivel global sobre el alcance, la necesidad y la legitimidad de los poderes legales que las autoridades de gobierno utilizan para acceder a las comunicaciones de las personas físicas. Las redes de telecomunicaciones y los proveedores de servicios trabajan hace más de diez años en las cuestiones de privacidad y libertad de expresión que surgen de este tipo de acceso. Por ejemplo, en 2011, un grupo de proveedores y operadores de redes móviles creó el espacio Diálogo de la Industria (ID) de las Telecomunicaciones y definió los principios que describen la responsabilidad de las empresas de telecomunicaciones en la protección de la libertad de expresión y la privacidad. Uno de los resultados del trabajo del ID fue que varias de las empresas miembro decidieron, cuando fuera posible, divulgar proactivamente información sobre la naturaleza y el volumen de las solicitudes de acceso a información que reciben de parte del gobierno de cada país en el que operan.[61] El ID se disolvió en 2017, cuando muchos de sus miembros se unieron a la Global Network Initiative.[62]

Por lo general, la legislación va atrasada respecto de los avances tecnológicos[63] y pueden surgir malentendidos sobre el nivel de capacidad técnica de los operadores de redes móviles para interceptar comunicaciones. Es técnicamente posible interceptar llamadas o mensajes de texto que realiza o recibe un usuario; hace décadas que los estándares móviles mundiales describen los requerimientos y las capacidades de interceptación lícita.

Sin embargo, las comunicaciones entre usuarios a través de una plataforma basada en Internet generalmente están fuera del alcance de los operadores de redes móviles, aun cuando dicho tráfico se transporte en sus redes. Algunos servicios populares, como WhatsApp, WeChat y Signal, están cifrados, sus mensajes no son almacenados por los operadores de redes móviles ni tienen a su disposición las claves de decodificación. Esto significa que, incluso si recibe una solicitud legítima, el operador de redes no puede acceder ni entregar el contenido de los mensajes (en la próxima sección, vea el ejemplo de restricción del servicio de WhatsApp en Brasil).

Los operadores de redes móviles reconocen la importancia de la soberanía y legitimidad de los gobiernos en la defensa de la seguridad de sus ciudadanos. De todas maneras, para lograrlo, la interceptación de las comunicaciones con fines de aplicación de la ley o de seguridad solo debe tener lugar dentro de un marco jurídico claro, compatible con los principios de derechos humanos de necesidad y proporcionalidad, y mediante procesos y autorizaciones formales, según lo especifique dicho marco.

Por último, la responsabilidad y, a menudo, los costos de las actividades emprendidas por los operadores de redes móviles para apoyar las necesidades de seguridad pública son asumidos, cada vez con más frecuencia, por los mismos operadores. El Salvador es un ejemplo extremo de ello, donde se aprobó un impuesto del 5 por ciento a los servicios de telecomunicaciones en noviembre de 2015 para financiar los planes de seguridad general del gobierno.[64] Si bien la política tributaria es un asunto que deben decidir los gobiernos, imponer impuestos a los operadores sobre la misma infraestructura de redes móviles que sustenta la seguridad es contraproducente, ya que desvía la financiación de una de las partes que ya está invirtiendo en la seguridad pública.

60 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

61 Sin embargo, muchos países prohíben explícitamente a los operadores de redes móviles la divulgación de detalles importantes sobre la naturaleza y el volumen de las solicitudes de interceptación que reciben.

62 Sobre la GNI: Global Network Initiative

63 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Acceso gubernamental

64 Telecompaper, 2016. El Salvador aprueba impuesto de 5% a las telecomunicaciones

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Los operadores de redes móviles tienen la responsabilidad de asegurarse de responder solamente a solicitudes legítimas (es decir, órdenes judiciales) que reciban de parte de organismos de gobierno legalmente autorizados y que hayan seguido el debido proceso, con los correspondientes mecanismos de protección. Por lo tanto, los gobiernos deben garantizar la existencia de un marco legal proporcional que describa claramente las facultades de vigilancia de las que disponen las agencias nacionales de aplicación de la ley.[65]

- Toda injerencia al derecho a la privacidad debe cumplir con la ley; es decir, tanto la retención como la revelación de datos y la interceptación de comunicaciones para fines de aplicación de la ley o de seguridad solo deben tener lugar a través de procesos y autorizaciones apropiados y especificados por dicho marco legal.[66]
- Los proveedores de telecomunicaciones deben contar con un proceso legal para oponerse a toda solicitud que consideren fuera del alcance de las leyes pertinentes.
- El marco debe ser transparente, proporcional, justificado y compatible con los principios de derechos humanos, incluidas las obligaciones resultantes de los tratados internacionales de derechos humanos aplicables, como el Pacto Internacional sobre Derechos Civiles y Políticos.
- Dada la constante expansión de la gama de servicios de comunicaciones, el marco legal debe contar con neutralidad tecnológica.[67]
- Los gobiernos deben proveer limitaciones de responsabilidad legal apropiadas o indemnizar a los proveedores de telecomunicaciones frente a demandas judiciales iniciadas respecto de su cumplimiento a las solicitudes y obligaciones para la retención, revelación e interceptación de comunicaciones y datos, así como la privación del acceso a redes y servicios.[68]
- Adicionalmente, los costos de cumplir todas las leyes que regulan la interceptación de las comunicaciones, la retención y revelación de datos, o la restricción del acceso a redes o servicios deben correr por cuenta de los gobiernos, como ocurre actualmente en algunos países. Esos costos y la base para calcularlos se deben acordar con antelación.[69]

La GSMA y sus miembros apoyan toda iniciativa que busque aumentar la transparencia del gobierno y la publicación gubernamental de las estadísticas relativas a las solicitudes de acceso a los datos de clientes[70] cuando sea posible.

65 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Acceso gubernamental
66 ibíd.
67 ibíd.
68 ibíd.
69 ibíd.
70 ibíd.

Informes de transparencia (divulgación de solicitudes de autoridades)

¿Por qué se informa?

El Diálogo de la Industria (ID) de las Telecomunicaciones fue fundado por un grupo de operadores y proveedores de telecomunicaciones que, en forma conjunta, se ocupa de los derechos de libertad de expresión y privacidad en el sector de las telecomunicaciones en el contexto de los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas.

Uno de los propósitos clave del ID era compartir aprendizajes y expandir la noción de transparencia. Los operadores del ID, incluidos AT&T, Millicom, Orange, Telenor Group, Telia Company, y Vodafone Group, fueron algunos de los primeros en publicar con frecuencia informes para difundir información sobre las solicitudes que recibían de las agencias de aplicación de la ley.

¿Qué se informa?

Generalmente, los objetivos de los informes de transparencia son los siguientes:

- Explicar los marcos legales y la capacidad de aplicación de la ley en sus mercados de operación.
- Explicar las políticas públicas y los procesos que se siguen al responder las exigencias de organismos y autoridades.
- Cuando sea posible, divulgar las estadísticas sobre la cantidad de solicitudes de datos de consumidores recibidas de parte de los organismos de seguridad en ciertos países o regiones.

¿Cuáles son las limitaciones?

A veces, la legislación en materia de aplicación de la ley y seguridad nacional incluye rigurosas restricciones que impiden a los operadores divulgar cualquier información relacionada con las exigencias que les imponen los organismos y las autoridades, incluida la divulgación de estadísticas agregadas. Muchos países también prohíben a los operadores suministrar información al público sobre los medios por los cuales se implementan esas exigencias. Estas restricciones pueden representar importantes obstáculos para que los operadores respondan a la petición del público de que brinden mayor transparencia.

No obstante, los operadores están convencidos de que medir la cantidad de solicitudes recibidas de las autoridades, con todas sus fallas, sigue siendo la medición más sensata disponible, sin ser demasiado compleja. Cabe destacar que solo los gobiernos que realizan estas solicitudes a los proveedores de comunicaciones son capaces de mostrar el panorama completo de la cantidad de solicitudes.

Desde el lanzamiento del ID en 2013, muchos operadores de redes móviles publican informes de transparencia. Access Now, una organización global de derechos digitales, se encarga de actualizar una base de datos, llamada Índice de Informes de Transparencia, que contiene enlaces a los informes de los operadores de redes móviles y otras empresas.[71]

71 https://www.accessnow.org/transparency-reporting-index/

Órdenes de restricción de servicio e inhibidores de señal

Órdenes de restricción de servicio

Además de las solicitudes de interceptación de comunicaciones, en ocasiones, los operadores de redes móviles reciben una orden, emitida por una autoridad de gobierno, de restringir servicios en sus redes ("órdenes de restricción de servicio" o SRO). Estas órdenes exigen que desconecten o restrinjan el acceso a su red móvil, a un servicio de red específico o a un servicio de terceros al cual se accede a través de su red. Las órdenes pueden exigir el bloqueo de un servicio o de un contenido móvil o de Internet específico, la restricción del ancho de banda de datos y la degradación de la calidad de los servicios de SMS o de voz. Además de estar obligados por ley, en algunos casos, los operadores de redes móviles podrían recibir sanciones penales (incluido el encarcelamiento del personal directivo) o perder su licencia, si divulgaran haber recibido una SRO o si se negaran a cumplir con tal orden.

Las SRO pueden tener varias consecuencias graves. Por ejemplo, puede verse afectada la seguridad nacional en caso de su uso indebido (p. ej., utilizar una restricción en la red para prevenir un ataque terrorista priva tanto a los ciudadanos como a los organismos de seguridad por igual de la oportunidad de utilizar las herramientas que ofrecen las comunicaciones para combatir el terrorismo). También puede ponerse en riesgo la seguridad pública si los servicios de emergencia y los ciudadanos no pueden comunicarse. Esto puede afectar la libertad de expresión, la libertad de asociación y la libertad de empresa, entre otros derechos humanos. Las órdenes de restricción de servicio pueden afectar el funcionamiento de la sociedad, la transferencia de fondos realizada por los usuarios a sus amigos y familias, y las transacciones y los pagos a proveedores y empleados de las empresas. Así, se puede generar un efecto dominó en los planes de crédito e inversiones, lo que, en definitiva, perjudicaría la reputación del país en cuanto al manejo de la economía y las inversiones extranjeras y desmotivaría a otros países a donar fondos u otros recursos.

Los operadores de redes móviles también se ven perjudicados. No solo sufren pérdidas financieras debido a la suspensión de los servicios y al daño en su reputación, sino que el personal local puede también quedar sometido a presiones por parte de las autoridades y, posiblemente, hasta sufrir represalias por parte del público.

En Brasil, por ejemplo, se dio una situación así, donde el servicio de mensajería WhatsApp supuestamente no brindó la asistencia necesaria a diferentes investigaciones penales.[72] Como respuesta, el gobierno exigió que los operadores de redes móviles dentro de Brasil restringieran el acceso a los servicios de WhatsApp en tres ocasiones distintas desde diciembre de 2015.[73] La principal consecuencia de este accionar fue impedir el uso de la aplicación de mensajería móvil más popular del país a los 100 millones de usuarios en Brasil. Se revocó cada uno de los fallos después de que se presentaran apelaciones ante tribunales superiores, dado que el impacto se consideró desproporcionado. WhatsApp y su sociedad controlante, Facebook, sostienen que la cooperación solicitada es técnicamente imposible, ya que no se almacena ninguna comunicación o, aun cuando se almacenaran, no se podría acceder a ellas debido al uso del cifrado de extremo a extremo. No obstante, muchos de los usuarios afectados generalmente culpan al operador de redes móviles por la interrupción del servicio.

En algunos países, hubo casos aún más extremos de bloqueo de redes, a veces, con el objetivo de limitar la capacidad de organización de la oposición política.[74] Como primera medida, los operadores de redes móviles instan a los gobiernos a ser transparentes con sus ciudadanos respecto de su rol

72 Financial Times, 2016: "WhatsApp ban ignites Brazil censorship fears"
73 The Guardian, 2016. "WhatsApp officially un-banned in Brazil after third block in eight months"
74 Puede ver algunos ejemplos de bloqueos en la base de datos retrospectiva de Internet & Jurisdiction en http://www.internetjurisdiction.net/publications/ retrospect#eyJ0byI6IjIwMTYtMTEifQ

en el bloqueo o la restricción de redes y servicios, como también de las justificaciones legales de dichas restricciones. Es importante agregar que las órdenes de bloqueo deberían permitir que las empresas notifiquen al consumidor de manera oportuna sobre aquellos servicios que hayan sido restringidos en virtud de la orden del gobierno.[75]

Uso de inhibidores de señal

Otra forma de restringir las comunicaciones móviles es el uso de inhibidores de señal, conocidos también como bloqueadores o "*jammers*".

Se trata de dispositivos que generan una interferencia que interrumpe, de forma intencional, los servicios de radiocomunicación entre el terminal móvil y la estación base.

Normalmente, estas herramientas rudimentarias se utilizan para impedir las comunicaciones en centros penitenciarios o entre terroristas o grupos políticos considerados subversivos, a menudo, en lugares de manifestaciones públicas masivas. Los inhibidores de señal también se utilizan como herramienta para

imposibilitar el uso de dispositivos móviles en áreas prohibidas. Por ejemplo, en América Latina, se emplean para evitar el uso ilícito de dispositivos móviles en lugares conflictivos, como las prisiones. Sin embargo, bloquear la señal no soluciona la causa del problema: el hecho de que los dispositivos móviles terminan en manos de los reclusos ilegalmente. Además, dada la naturaleza de las señales de radio, es prácticamente imposible garantizar que la interferencia generada por los inhibidores sea delimitada. Por lo tanto, la interferencia afecta a los ciudadanos, a los servicios y a las organizaciones de seguridad pública. Tiene un efecto dominó en muchos otros usuarios, especialmente aquellos que viven y trabajan en las inmediaciones de la prisión, que no pueden utilizar los servicios móviles. El costo de los bloqueadores, la pérdida de ingresos legítimos y, muchas veces, la mala reputación que genera la interrupción del servicio afecta negativamente a los operadores móviles.

Toda interrupción de las redes de comunicaciones, los servicios de red o Internet (como las redes sociales, los motores de búsqueda o los sitios de noticias) tiene el potencial de afectar la seguridad pública y restringir el acceso a servicios vitales de emergencia, pagos y salud. Por ejemplo, una restricción de servicio puede limitar la capacidad del usuario móvil de ponerse en contacto con los servicios de emergencia a través de números como el "112" o el "911" y puede interferir en el funcionamiento de las alarmas móviles conectadas o dispositivos médicos personales. Por estos motivos, las restricciones de servicios deben ser mínimas y se deben considerar los efectos colaterales negativos para todos los usuarios.

75 Declaración conjunta del Diálogo de la Industria de las Telecomunicaciones y la Global Network Initiative: http://www.telecomindustrydialogue.org/global-network-initiative- telecommunications-industry-dialogue-joint-statement-network-service-shutdowns/

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Si bien la GSMA comprende y apoya el uso adecuado de la interceptación legítima en pos de una mejor seguridad pública, también desaconseja el uso de las SRO y los inhibidores de señal.

Los gobiernos solo deberían recurrir a las SRO en circunstancias excepcionales y predeterminadas, únicamente en los casos en que sean estrictamente necesarias y proporcionales para alcanzar un objetivo específico y legítimo, conforme a las leyes pertinentes y los derechos humanos reconocidos internacionalmente.[76] También hay otras cuestiones que deben considerarse:

- A fin de promover la transparencia, toda SRO del gobierno debería ser emitida solo por escrito a los operadores, citar los fundamentos legales y establecer un claro mecanismo de auditoría que indique quién es la persona que autoriza dicha orden. También se debería informar a los ciudadanos que es el gobierno quien ordena la restricción del servicio y que fue aprobada por una autoridad judicial o cualquier otra que tenga competencia, de conformidad con los procedimientos administrativos establecidos por ley. Debe permitir que el operador de redes móviles investigue el impacto en sus redes y clientes y que se comunique libremente con estos últimos en relación con la orden. Si esta comunicación afectara la seguridad nacional al momento de la restricción, entonces se deberá informar a los ciudadanos a la mayor brevedad posible, con posterioridad al hecho.[77]
- Los gobiernos deben procurar evitar o mitigar los posibles efectos perjudiciales de las SRO minimizando la cantidad de exigencias, el alcance geográfico, la cantidad de personas y negocios potencialmente afectados, el alcance funcional y la duración de la restricción. Por ejemplo, en lugar de bloquear toda la red o toda una plataforma de redes sociales, la SRO podría apuntar a contenidos o usuarios específicos. En todo caso, la SRO debería siempre especificar una fecha de finalización. Se deben establecer mecanismos de supervisión independientes para garantizar el cumplimiento de estos principios.[78]
- Los operadores de redes móviles pueden desempeñar un papel importante en la concientización de los funcionarios de gobierno sobre el posible impacto de las SRO. También pueden estar preparados de forma tal que, si reciben una SRO, puedan trabajar con rapidez y eficiencia para determinar la legitimidad de la orden, comprobar si fue aprobada por una autoridad judicial, si es válida y vinculante, y si es apelable. Además, pueden trabajar con el gobierno para limitar el alcance y el impacto de la orden. Los procedimientos pueden incluir una guía sobre cómo el personal local debería gestionar una SRO (p. ej., escalar a representantes corporativos superiores).[79]
- En primer lugar, todas las decisiones deben tomarse teniendo en cuenta la seguridad y la protección de los clientes, las redes y el personal del operador móvil, con el objetivo de restablecer los servicios lo más rápidamente posible.[80]

76 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Órdenes de restricción de servicio
77 ibíd.
78 ibíd.
79 ibíd.
80 ibíd.

— La GSMA y sus miembros se comprometen a trabajar con los gobiernos y utilizar la tecnología como herramienta para mantener los dispositivos móviles fuera de áreas conflictivas, además de cooperar en los esfuerzos por detectar, rastrear e impedir el uso de dispositivos contrabandeados. No obstante, es esencial encontrar una solución práctica y a largo plazo que no afecte negativamente a los usuarios legítimos ni a las inversiones sustanciales que los operadores móviles realizan para mejorar su cobertura.[81]

— Los inhibidores de señal deberían utilizarse únicamente como último recurso o implementarse en coordinación con los operadores de redes móviles con licencia local. La coordinación debe continuar durante el tiempo que se utilicen los dispositivos para garantizar que la interferencia sea mínima en áreas adyacentes y que los usuarios de dispositivos móviles legítimos no se vean afectados.[82]

— Además, las autoridades regulatorias deben prohibir el uso de inhibidores de señal por parte de entidades privadas e imponer sanciones para aquellas que los utilicen o comercialicen sin el permiso de la autoridad correspondiente.[83]

— La importación y venta de inhibidores o bloqueadores debe limitarse a aquellas personas calificadas y autorizadas para hacerlo y su operación debe estar habilitada por el regulador nacional de telecomunicaciones. Asimismo, fortalecer la seguridad en áreas conflictivas, como las prisiones, para evitar el contrabando de dispositivos inalámbricos es la medida más efectiva contra el uso ilegal de dispositivos móviles en dichas áreas, porque no afectaría los derechos de los usuarios legítimos de servicios móviles que se encuentran en las inmediaciones.[84]

81 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Inhibidores de señal
82 ibíd.
83 ibíd.
84 ibíd.

En profundidad

Mitigación del impacto de las órdenes de restricción de servicio

En casos de emergencias en algunos países, las autoridades de gobierno tienen la facultad de exigir respuestas extremas a los operadores de redes, como la desconexión total o parcial de la red o de los servicios, durante cualquier período de tiempo. Cuando se alude a la seguridad nacional como fundamento para dichas solicitudes, es probable que se apliquen duras sanciones en caso de incumplimiento. Sin embargo, algunos operadores de redes trabajan con diligencia en estas solicitudes del gobierno para minimizar el potencial impacto en la libertad de expresión y la privacidad. **A continuación, se exponen tres ejemplos de lo anterior:**

1. El 1 de junio de 2014, en uno de sus mercados africanos, las autoridades de gobierno contactaron a Orange por teléfono y solicitaron la suspensión de los servicios de SMS en todo el país. Para verificar el fundamento legal de esta solicitud, Orange pidió que la orden se presentara por escrito. Al día siguiente, los cuatro operadores de telecomunicaciones del país recibieron una orden por escrito que citaba la ley pertinente y firmada por la autoridad competente e indicaba que el incumplimiento podía implicar sanciones.

   Luego, la orden se publicó en un periódico panafricano. Las empresas cumplieron la orden, lo cual provocó la suspensión de los servicios de SMS hasta el 24 de julio. Como resultado, la empresa aprendió varias lecciones, como la importancia de la cooperación entre pares al momento de responder a exigencias de gobierno que presentan irregularidades y que la transparencia puede ser útil para una empresa al responder a estas peticiones. (Diálogo de la Industria de Telecomunicaciones, 2016. “Aportes presentados al Relator de la ONU David Kaye”).

2. En AT&T, los empleados capacitados (incluidos los abogados de AT&T y, cuando corresponde, también el asesor legal local familiarizado con la legislación aplicable) evalúan este tipo de solicitudes para confirmar si las solicitudes fueron emitidas debidamente por la entidad competente, conforme a autoridad legal válida y en cumplimiento de los requerimientos aplicables. La empresa rechaza toda petición del gobierno que no cumpla con estos requisitos. Cuando corresponde, la empresa solicita una aclaración o modificación de la solicitud o presenta una objeción a la petición del gobierno o la orden judicial en el foro correspondiente. Estos esfuerzos ayudan a minimizar el posible impacto de las solicitudes de gobierno en la privacidad de los clientes de AT&T y en su capacidad de comunicarse y acceder a la información de su preferencia. (Diálogo de la Industria de Telecomunicaciones, 2016. “Aportes presentados al Relator de la ONU David Kaye”).

3. La situación de seguridad en las operaciones de América Central de Millicom fue todo un desafío en 2015. Desde el año anterior, las autoridades de Guatemala, El Salvador y Honduras habían aprobado leyes que obligan a todos los operadores de telecomunicaciones a desconectar servicios o reducir la capacidad de señal dentro y en los alrededores de las prisiones, ya que las autoridades sospechaban que las pandillas criminales seguían operando desde el encarcelamiento usando dispositivos móviles ingresados a las instalaciones como contrabando. Inicialmente, se solicitó a los operadores de telecomunicaciones que desconectaran las torres de las estaciones base que prestaban servicios a grandes zonas, lo cual también afectó a las poblaciones que viven en las inmediaciones de los establecimientos penitenciarios, además de interrumpir sus actividades diarias, como el uso de cajeros automáticos.

   La empresa trabajó de forma proactiva, tanto con las autoridades como con sus pares de la industria, centrándose en buscar soluciones alternativas que pudieran resolver el problema sin afectar a la población que vive en las inmediaciones de las prisiones. Las alternativas variaban: desde un nuevo diseño de cobertura de red alrededor de las prisiones y soluciones de terceros

similares a los bloqueadores para restringir la señal en una zona física específica hasta la reubicación de las prisiones a zonas no tan densamente pobladas.

Como resultado, a finales de 2015, todas las restricciones de señal a dispositivos móviles dentro de las prisiones de Guatemala y Honduras se implementaron de forma más específica, afectando solo el interior de los edificios de las prisiones. (Millicom, 2016. "Law Enforcement Disclosure Report 2016").

Registro obligatorio de tarjetas SIM prepagas

La tercera área de seguridad pública que ha sido objeto de mucho debate en los últimos años es el registro obligatorio de tarjetas SIM móviles prepagas, una política que varios gobiernos adoptaron en años recientes que requiere al consumidor mostrar un documento de identidad para poder activar una tarjeta SIM móvil prepaga. Muchos gobiernos siguen pensando que esta política es importante para abordar las preocupaciones de seguridad nacional, a pesar de la falta de publicación de pruebas empíricas que demuestren una conexión directa entre la adopción de tal política y la reducción de las actividades delictivas. Algunos gobiernos argumentaron que no registrar las tarjetas permite a los delincuentes aprovechar el anonimato para llevar a cabo diferentes actividades ilegales, como pedir rescate después de un secuestro o planear un ataque terrorista. Se cree que ese anonimato hace más difícil rastrear el uso de la tarjeta SIM móvil a un usuario real. En respuesta, varios gobiernos exigieron que los operadores de redes móviles registren a todos sus consumidores prepagos, tanto los existentes como los futuros.

Los gobiernos adoptan distintas estrategias para aplicar las políticas de prueba de identidad, lo que implica que los operadores de redes móviles con licencias locales están sujetos a diferentes requerimientos en los distintos países.

Para finales de 2020, el 72 por ciento de las suscripciones móviles eran prepagas[85] y ascendió a 157 la cantidad de países en los que son obligatorias las políticas de registro de tarjetas SIM prepagas. Cuando se implementan, estas políticas tienen una serie de consecuencias no deseadas, entre las que se incluyen las siguientes:

— La exclusión de usuarios que no cuentan con la documentación de identificación necesaria, generalmente aquellos en condiciones de pobreza y vulnerabilidad, lo cual les impide acceder a servicios móviles. Para aproximadamente mil millones de personas en todo el mundo sigue siendo difícil acceder a tarjetas SIM y a servicios móviles a su nombre porque no tienen los medios para probar su identidad. Esto sucede particularmente en los países en los que el registro de las SIM es obligatorio. Según el país y la disponibilidad de documentación de identidad estándar, este problema puede representar un impedimento mayor.[86]

— El registro fraudulento por parte de delincuentes que desean mantener su anonimato, causando un aumento del robo de dispositivos móviles y el surgimiento de un mercado clandestino de tarjetas SIM robadas.

— Una mayor preocupación del consumidor en relación con el acceso, la seguridad, el uso y la retención de sus datos personales, en particular ante la ausencia de leyes nacionales en materia de privacidad y libertad de expresión. Si bien muchos países que exigen el registro de las SIM cuentan con un marco de protección de datos o privacidad (64 por ciento), hay una porción significativa de países que están considerando la adopción de estos marcos o que no cuentan con marcos de ningún tipo.[87]

85 GSMA Intelligence, penetración de conexiones prepagas (conexiones prepagas, T3, 2020)

86 Informe de la GSMA "Access to Mobile Services and Proof of Identity 2021. Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19", abril de 2021 (https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf)

87 ibíd.

Caso de estudio

Colaboración de la industria

En 2020, muchos gobiernos flexibilizaron las regulaciones durante la pandemia de COVID-19 para facilitar la inclusión digital y financiera. Uno de los cambios en la regulación, la flexibilización de los procesos de *Know Your Customer* (conocer al cliente, KYC) y *onboarding* (proceso de suscripción de nuevos usuarios), fue el centro de la investigación del programa de Identidad Digital de la GSMA, debido a la conexión entre los requisitos de identificación y el acceso a los servicios móviles (p. ej., al dinero móvil) a través de billeteras móviles. La flexibilización de los procesos de KYC y *onboarding* tuvo como propósito motivar a que más personas utilicen los servicios financieros digitales en lugar de dinero en efectivo, lo que reduciría el contacto entre los usuarios de dinero móvil, los agentes y los comerciantes. La GSMA llevó a cabo una investigación exhaustiva con distintas partes interesadas de organizaciones que incluyeron operadores de redes móviles, bancos centrales y reguladores de telecomunicaciones de cinco países para entender cómo se produjeron estos cambios regulatorios y cuáles fueron los primeros impactos en las personas y el sector público y privado.

Algunos resultados fueron: en Colombia, se aceleraron los servicios financieros móviles existentes y los procesos de *onboarding* remotos en respuesta al virus COVID-19. En Jordania, la flexibilización de políticas puso de relieve la importancia de la digitalización y la adopción más rápida de servicios financieros digitales. Las plataformas en línea también se hicieron más robustas. Algunos operadores de redes móviles de Senegal dieron soporte al Programa Mundial de Alimentos (PMA) de la ONU para digitalizar la asistencia alimentaria, lo que logró que más de 40.000 familias recibieran ayuda en sus billeteras digitales.

Cada vez más gobiernos adoptan políticas de obligatoriedad de registro de usuarios de tarjetas SIM prepagas, principalmente como herramienta para luchar contra el terrorismo y mejorar la aplicación de la ley.[88] A enero de 2020, la investigación de la GSMA determinó que los gobiernos de 155 países impusieron políticas de registro de SIM.[89] Sin embargo, al día de la fecha, no ha habido evidencia empírica de que el registro obligatorio de SIM resulte en una reducción directa del delito.[90] A pesar de esta falta de pruebas empíricas, muchos gobiernos creen que el registro obligatorio de las SIM ayuda en la lucha contra el crimen y el terrorismo. Normalmente, si existe una obligación de registrar a los usuarios de SIM prepagas, el costo de implementación del proceso recae en los operadores de redes móviles. Dichos costos pueden ser significativos y afectar la capacidad de los operadores de invertir en la prestación de servicios a consumidores que gastan menos. Varios países, incluido el Reino Unido, examinaron minuciosamente[91] estos programas y concluyeron que los costos para la sociedad (traducidos en cargas burocráticas y bases de datos de registros) son mayores que los beneficios, por lo que decidieron no adoptar estas políticas. Estas decisiones se toman a nivel nacional y dependen de circunstancias nacionales. También pueden depender de los problemas que se procura resolver con el registro.[92]

El lado positivo de los registros de SIM es que facilitan el acceso del consumidor a servicios móviles y digitales de valor agregado, como dinero móvil, identidad digital y servicios de gobierno electrónico, a los cuales no hubieran podido acceder de no haber estado registrados. Para que estos beneficios estén disponibles para el consumidor y produzcan resultados valiosos para los clientes, los operadores de redes móviles y los gobiernos deben ofrecer servicios que incentiven al cliente a registrarse voluntariamente.

Es importante no confundir las consecuencias negativas no deseadas de una política de registro obligatorio en un país determinado con los beneficios potenciales que el consumidor podría obtener gracias al registro voluntario de su tarjeta SIM. Ninguno de

88 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Registro obligatorio de tarjetas SIM de prepago
89 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf
90 GSMA, 2016: Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice
91 Lord West de Spithead en respuesta a la pregunta parlamentaria del Vizconde Waverley sobre el registro obligatorio de los usuarios de tarjetas SIM: https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
92 GSMA, 2016. Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice

estos beneficios ni resultados positivos depende del mandato gubernamental de registro obligatorio de tarjetas SIM. Por el contrario, esos resultados se pueden obtener con el registro voluntario del cliente que decide registrar su tarjeta SIM prepaga para tener acceso a servicios que considera valiosos, como el dinero móvil, el comercio móvil o los servicios de gobierno electrónico. Cabe recordar que, aun así, el registro voluntario está sujeto a que el consumidor tenga acceso a un documento para comprobar su identidad.

Caso de estudio

Opciones alternativas al registro: México

En 2019, México introdujo el registro obligatorio de tarjetas SIM ("RENAUT") con el objetivo de combatir la actividad criminal.

Cuando las normas del "RENAUT" entraron en vigencia, la privacidad y la seguridad de los datos era una preocupación constante y había problemas para registrar, en un plazo de implementación muy breve, a gran parte de la población que no contaba con un documento de identificación oficial. Esta solución tampoco tuvo éxito en combatir la actividad criminal y, como resultado, se incrementó el robo de equipos.

Luego de consultas con la industria, la academia y ONG, el programa de registro RENAUT cesó sus operaciones en 2012. La base de datos fue desactivada y se dio por perdida la importante inversión financiera realizada por los operadores de redes móviles y las autoridades. Para abordar la situación específica del mercado mexicano, se incorporó un programa alternativo a la Ley de Telecomunicaciones y Radiodifusión, en vigencia desde 2014.

La nueva Ley de Telecomunicaciones y Radiodifusión, así como otras disposiciones regulatorias, no exige que el usuario proporcione detalles de registro para utilizar los servicios prepagos. En cambio, la ley aprovecha las diferentes obligaciones de los operadores de redes móviles (p. ej., interceptación legítima) para ayudar al gobierno y a los servicios de seguridad a combatir la actividad criminal.93

93 GSMA, 2016. Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice

Cuando el registro de tarjetas SIM sea obligatorio, se debe notificar a los clientes existentes sobre la necesidad de registrarlas, cómo hacerlo y las consecuencias de no hacerlo (p. ej., la posible desactivación de la tarjeta SIM). En este caso, el registro de la tarjeta SIM se debe implementar de forma pragmática, teniendo en cuenta las circunstancias del mercado local. Entre los factores relevantes del mercado local podemos mencionar si el acceso de los ciudadanos a un documento de identidad nacional es común en todo el país, si el gobierno mantiene buenos registros de la identidad de los ciudadanos y si los operadores de redes móviles tienen la posibilidad de verificar los documentos de identidad de sus clientes.

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Si bien el registro de usuarios de tarjetas SIM prepagas podría ofrecer valiosos beneficios a los ciudadanos y consumidores, no debería ser obligatorio. Si se toma la decisión de exigir el registro, el gobierno debería tener en cuenta las mejores prácticas internacionales y ofrecer mecanismos de registro flexibles, proporcionales y relevantes a su mercado específico, incluyendo el nivel de penetración de documentación de identidad oficial en el país.[94]

Si se cumplen estas condiciones, aumentarán las chances de que registrar las tarjetas SIM sea más eficaz y genere un registro de consumidores más preciso. Por otro lado, contar con un sólido sistema de verificación y autenticación de consumidores puede permitir a los operadores de redes móviles crear fácilmente soluciones de identidad digital que habiliten al usuario a acceder a una variedad de servicios móviles y no móviles. Dado el volumen de las bases de clientes existentes en todos los países, se debe considerar detenidamente la magnitud de la tarea y el tiempo que tomaría registrar a los usuarios para minimizar la carga del cliente y la posible interrupción de los servicios.

La GSMA insta a los gobiernos que están considerando incorporar o revisar el registro obligatorio de tarjetas SIM a seguir los siguientes pasos antes de concluir sus planes:

- Consultar a los operadores de redes móviles, colaborar y comunicarse con ellos, antes, durante y después de la implementación.
- Lograr un equilibrio entre las exigencias de seguridad nacional y la protección de los derechos de los ciudadanos, en particular en los casos en que el gobierno exija el registro obligatorio de tarjetas SIM por motivos de seguridad.
- Garantizar que existan salvaguardas de privacidad adecuadas y una supervisión legal eficaz para proteger los datos y la privacidad del cliente.
- Fijar plazos realistas para el diseño, la prueba y la implementación de los procesos de registro.
- Brindar certeza y claridad sobre los requisitos de registro antes de su implementación.
- Permitir o incentivar el almacenamiento de registros electrónicos y el diseño de procesos de registro “livianos” desde el punto de vista administrativo.
- Permitir o incentivar a los clientes que tengan una tarjeta SIM registrada a acceder a otros servicios móviles y digitales de valor agregado.
- Apoyar a los operadores de redes móviles en la implementación de programas de registro de tarjetas SIM, realizando aportes para actividades de comunicación conjunta y costos operativos.

94 Manual de políticas públicas de telecomunicaciones móviles de la GSMA: Registro obligatorio de tarjetas SIM de prepago

En profundidad

Asociaciones público-privadas para el registro en América Latina

Durante 2009 en Ecuador y diciembre de 2016 en Argentina, las Autoridades Regulatorias Nacionales (CONATEL y ENACOM, respectivamente) solicitaron la verificación cruzada y validación ante un organismo de registro de identidad nacional o privado del procedimiento de registro de tarjetas SIM de todos los consumidores. En ambos casos, Telefónica trabajó estrechamente con el gobierno para desplegar una solución adecuada para los consumidores, el gobierno y sus propias necesidades.

En Ecuador, Telefónica implementó un proceso de registro utilizando un sistema automatizado denominado "Respuesta de Voz Interactiva" (IVR). El servicio de voz representó una mejora ante el procedimiento anterior, que requería la verificación cruzada de la identidad del consumidor con el Registro Civil.

En Argentina, Telefónica desarrolló una aplicación que se activa al insertar una tarjeta SIM en el dispositivo móvil. La aplicación recopila la información de la tarjeta SIM, además de la identificación personal del usuario móvil. Este sistema digital se usa para crear una base de datos que captura la conexión única entre el propietario y la tarjeta SIM y entre la tarjeta SIM y el dispositivo móvil.

Gracias a estas experiencias de trabajo en colaboración con las autoridades nacionales pertinentes, Telefónica aprendió estas tres lecciones clave:

1. Existen varias formas de validar el proceso de registro de tarjetas SIM. Cada operador de redes móviles debe desarrollar la que considere más adecuada.
2. Contar con un cronograma predefinido es esencial para lograr una implementación exitosa. Por ejemplo, en Ecuador, los operadores de redes móviles y el regulador trabajaron en conjunto para implementar una "fase de estadística" que permitió evaluar las necesidades reales a fin de evitar el exceso de regulación
3. Para considerar alternativas de implementación y desarrollar la que mejor satisfaga las necesidades de todas las partes interesadas de forma equilibrada, se requiere una asociación público-privada estrecha y una colaboración sólida entre operadores de redes móviles y el gobierno.

05

Capítulo 5

Protección de la seguridad de las redes móviles y la integridad de los dispositivos

La seguridad y la resiliencia de la infraestructura de red apuntala el uso seguro de los servicios móviles.

Protección de la seguridad de las redes móviles y la integridad de los dispositivos

Los actores de la industria deben trabajar juntos y de forma coordinada con las agencias internacionales de aplicación de la ley y las autoridades nacionales de seguridad para compartir inteligencia sobre amenazas y así responder a ataques maliciosos a las redes y dispositivos móviles e identificar a los responsables. Esto se puede lograr con la participación de los equipos existentes de respuesta ante incidentes de seguridad y la creación de nuevos equipos, si fuese necesario, para contrarrestar cualquier deficiencia. Cuando sea necesario, la regulación debe aplicarse de manera coherente a todos los proveedores de la cadena de valor, con neutralidad respecto de los servicios y la tecnología, preservando al mismo tiempo el modelo de gobernanza de Internet de múltiples partes interesadas y permitiendo su evolución. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas para proteger la infraestructura subyacente y asegurar que se provea al cliente el servicio de comunicaciones más seguro y confiable posible, mediante las siguientes acciones:y:

- Tomar medidas para obtener equipos de red que cuenten con un diseño, un desarrollo y un soporte seguros, y garantizar la seguridad de la infraestructura de red que operan y controlan.
- Promover las asociaciones entre el sector público y el privado a través de estrategias globales y coordinadas para minimizar el riesgo de hackeo o uso de la red para fines maliciosos.
- Brindar claridad sobre qué parte de la infraestructura es responsabilidad de los operadores y dónde se encuentra la fronteras con otros servicios o infraestructuras.

Los operadores de redes móviles protegen la confidencialidad, integridad y disponibilidad de las comunicaciones en toda la red garantizando la seguridad de los activos críticos (hardware, software y datos) e impidiendo el acceso no autorizado o la intrusión a cualquier otro nodo o vínculo que sea parte de la red. Dado que el dispositivo móvil del usuario final es el primer punto de acceso a la red desde la perspectiva del usuario, proteger la integridad del dispositivo se convirtió recientemente en un requerimiento fundamental. Por necesidad, el acceso a las redes móviles está abierto a una gama muy amplia de usuarios, a través de diferentes dispositivos y protocolos de conexión. Las redes de comunicaciones también deben interconectarse con muchas otras en el mundo (fijas, móviles, proveedores de servicios de Internet y empresas) a fin de ofrecer la funcionalidad “en cualquier momento y lugar” de las redes modernas. Es por esto que, en la práctica, es sumamente complejo proteger las redes y los dispositivos.

La rápida evolución de las comunicaciones móviles de la última década no solo dio como resultado la convergencia de la conectividad de red móvil y fija, sino que también expuso a las redes móviles a nuevas interfaces que están fuera del control del operador de red. La tecnología 5G está marcando el inicio de una era en la que la conectividad es más fluida y flexible. Las redes 5G se adaptan a aplicaciones y

ajustan a medida su desempeño para satisfacer las necesidades de los usuarios.

Para 2030, la mayoría de los mercados tendrá al menos una red 5G y se espera que las conexiones 5G móviles excedan los 5.000 millones, lo que representará más de la mitad de las conexiones totales.[95] La industria móvil se encuentra trabajando en la mejora de la seguridad de la red y los servicios mediante el diseño de las funciones de red y sus estrategias de despliegue. Las nuevas capacidades de autenticación y la mejora en la protección de la identidad del suscriptor son mejoras significativas en materia de seguridad, en comparación con las generaciones anteriores. No obstante, es probable que las capacidades 5G deban coexistir con generaciones previas de infraestructura móvil durante algún tiempo, en cuyo caso se deberá garantizar la seguridad tanto de la infraestructura nueva como de la existente.

Diferentes tipos de amenazas (Figura 5) pueden socavar la integridad de las redes mediante la interceptación no autorizada, la suplantación de identidad o la interrupción de servicios. La principal respuesta de la industria móvil ante estas amenazas ha sido optimizar la solidez y salud de la seguridad, promoviendo un debate transparente sobre el equilibrio entre la conveniencia y la seguridad, e incorporando funcionalidades de seguridad cada vez más sofisticadas en las normas y protocolos técnicos, a medida que se desarrolla y despliega cada nueva generación de redes móviles.

Esta sección del informe aborda distintas cuestiones de seguridad que afectan a las redes y los dispositivos y que tienen el potencial de poner en peligro la integridad y protección necesarias en las comunicaciones del cliente:

- Seguridad de la red, que incluye la integridad física y la seguridad de señalización, interconexión y operación.
- Seguridad e integridad de los dispositivos móviles, que incluye el malware y software (tanto patentado como de código abierto).
- 5G, IoT y desarrollos futuros en redes, que incluyen la nube y la virtualización, así como también la cadena de suministro.

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y otras partes interesadas, las cuales son descriptas más adelante en este capítulo.

Figura 5
Protección de las redes

OBJETIVO DE LA PROTECCIÓN	DESCRIPCIÓN DE LA AMENAZA	POSIBLE ATAQUE
Integridad Evitar la alteración de datos	Adulteración no autorizada	**INTERCEPTACIÓN (*MAN IN THE MIDDLE*, MitM)** 
Confidencialidad Mantener la privacidad de los datos	Acceso no autorizado	**ESCUCHAS** 
Disponibilidad Mantener la disponibilidad de la red y los datos para usuarios legítimos	Destrucción, robo, eliminación o pérdida de datos o redes no disponibles	**DENEGACIÓN DE SERVICIOS (DOS)** 

95 Informe de la GSMA "5G in Context, Q4 2022 Data-driven insight into areas influential to the development of 5G" (marzo de 2022)

Infraestructura física de la red

La seguridad de las redes móviles comienza en su propia infraestructura física, como los emplazamientos de antenas, las redes de transmisión (*backhaul*) y los elementos del núcleo de red.

Por ejemplo, en la red existen funciones primordiales, como el registro de usuarios autorizados, cuya seguridad debe garantizarse ya que representan un punto único de vulnerabilidad a ataques maliciosos o fallas técnicas. Los operadores de redes móviles y proveedores de equipos continúan desarrollando y desplegando nuevas soluciones para que estas funciones sean más robustas y, hasta el momento, han tenido gran éxito. Sin embargo, esto requiere de inversión constante para el desarrollo y despliegue de nuevas funciones y prestaciones.

El uso de estaciones base móviles falsas o captadores de identidad internacional de suscriptor móvil (IMSI) es una vulnerabilidad causada por la ausencia de autenticación mutua en la tecnología 2G y de funcionalidades que permiten cambiar la configuración de los dispositivos 3G y 4G automáticamente para que utilicen una red 2G. Las estaciones base falsas engañan a los dispositivos móviles que se encuentran a su alcance para que se conecten a ellas en lugar de a la red real, a la que el operador de la estación base falsa retrasmite la llamada luego. Este ataque de intermediario, conocido como *man in the middle*, crea una serie de vulnerabilidades, como la interceptación, el rastreo de ubicación, la denegación de servicio y fraudes. Los formuladores de políticas, como el Comité de Supervisión y Reforma de Gobierno de EE. UU., se encuentran en proceso de elaborar recomendaciones para la protección contra el uso no autorizado de estos dispositivos. Los operadores de redes móviles pueden desplegar medidas de seguridad estándar para ayudar a mitigar este riesgo: la GSMA desarrolló directrices para asistirlos en esta labor.

Además de la infraestructura de telecomunicaciones, existe una variedad de servicios de IT corporativos que permiten hacer operaciones comerciales más amplias y software para dar soporte a los clientes, como sistemas de facturación, y sistemas y paneles de control para clientes empresariales.

Los sistemas corporativos internos incluyen la intranet, el correo electrónico, mensajería instantánea y sistemas de personal, como contabilidad y ventas. Distintos dispositivos para empleados tienen acceso a estos sistemas, los cuales cuentan con funciones variadas para el personal, incluidos administradores de sistema de la red operativa.

La tecnología que se usa dentro de las redes móviles se actualiza frecuentemente y de manera planificada con las mejoras más recientes. Los altos niveles de inversión contínua en nueva infraestructura han recorrido un largo camino en garantizar que la infraestructura de red sea lo más razonablemente robusta posible.

Para alcanzar un resultado exitoso, es cada vez más importante mantener la confianza en esta capacidad de inversión a medida que se modifican las leyes y las regulaciones en respuesta a las amenazas cambiantes.

Algunas redes heredadas 2G y 3G usan protocolos de señalización poco seguros, desarrollados hace muchos años, cuando las necesidades de seguridad eran menos urgentes. Como resultado, están expuestas a fraudes y amenazas de seguridad constantemente. El Grupo de Seguridad y Fraude de la GSMA encaró un importante trabajo para brindar asesoramiento a los operadores de red sobre cómo mitigar los riesgos de seguridad de señalización. El riesgo de que ocurran muchos ataques conocidos se vio mitigado gracias a las mejoras en materia de seguridad incorporadas en 4G y 5G. Se puede minimizar la explotación de las vulnerabilidades de las redes 4G garantizando que las capacidades de seguridad que son inherentes a los estándares se desplieguen y configuren correctamente. Sin embargo, debido a la retrocompatibilidad de 4G con 3G/2G, sus vulnerabilidades no desaparecerán hasta que deje de existir la tecnología legada o la retrocompatibilidad.

La tecnología 5G cuenta con controles de seguridad para lidiar con muchas de las amenazas a las que se enfrentan las redes 4G, 3G y 2G.

Algunos de los controles son: las nuevas capacidades de autenticación mutua, una mejor protección de la identidad del suscriptor y nuevos mecanismos de seguridad. Los *gateways* GSM (también conocidos como "SIM *boxes*") también pueden permitir que terceros no autorizados interfieran en el enrutamiento de llamadas a redes móviles y sus clientes, lo cual puede generar preocupaciones. Los *gateways* GSM generalmente no soportan la funcionalidad de identificación de llamada (CLI) y esta carencia tiene consecuencias en los servicios que dependen de la CLI (p. ej., recarga de cuentas de SIM prepagas) y para las obligaciones de interceptación lícita por parte de los operadores de red en cumplimiento de la aplicación de la ley.

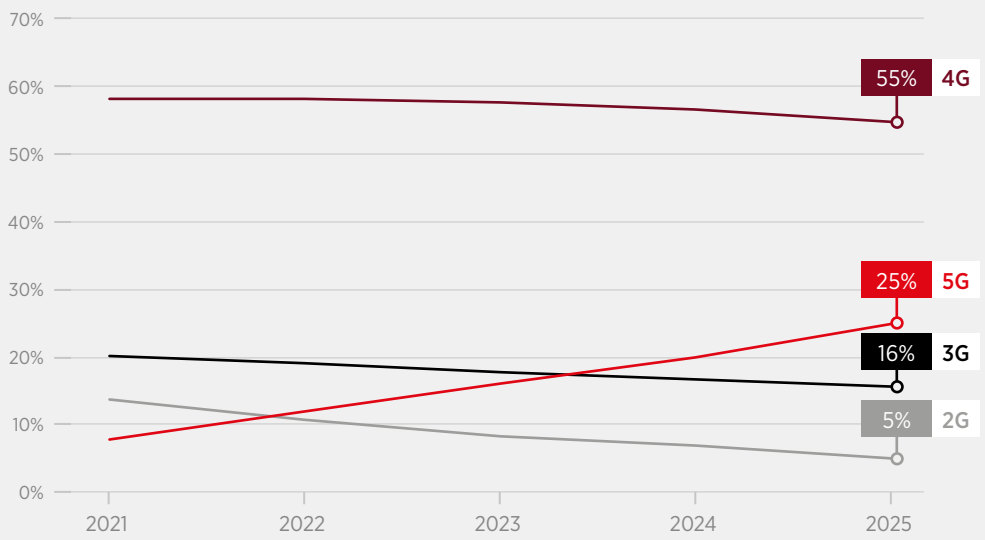
Si bien los operadores de redes móviles continúan mitigando las amenazas que enfrentan sus redes y consumidores, cabe destacar que lo mismo debería esperarse de los operadores de redes inalámbricas públicas, como los puntos de acceso Wi-Fi (*hotspots*) públicos. Los operadores de estas redes y sus clientes deberían implementar salvaguardas adecuadas (p. ej., redes privadas virtuales o VPN) para ayudar a garantizar la seguridad del ecosistema de comunicaciones en general.

Figura 6

Porcentaje de conexiones

Las conexiones 5G representarán un cuarto de las conexiones totales para 2025, más del triple que en 2021.

Porcentaje de conexiones (sin incluir IoT celular con licencia)



Fuente: GSMA Intelligence

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Si bien no se puede garantizar que una tecnología de seguridad sea infalible, los ataques a las redes y los servicios móviles no son tan frecuentes, dado que la mayoría requeriría considerables recursos, como equipos especializados, capacidad de procesamiento computacional y conocimientos técnicos que exceden las habilidades de la mayoría de las personas u organizaciones. Las barreras por derribar para comprometer la seguridad de las redes móviles han sido muy altas y la comprensión de las posibles vulnerabilidades ha sido mejorada sensiblemente, permitiendo una rápida respuesta de la industria ante nuevos problemas de seguridad. Sin embargo, el panorama tecnológico cambiante y el surgimiento de nuevas amenazas y fuentes de ataque requieren que la industria adopte un enfoque aún más proactivo para proteger las redes en el futuro:

- Es importante que la industria móvil asegure la implementación de mecanismos, herramientas y oportunidades adecuadas para facilitar el intercambio de información sobre amenazas y ataques, y garantizar la divulgación inmediata de la información en respuesta a incidentes. Esta iniciativa podría incluir a reguladores u otras autoridades de gobierno, como los Equipos de Respuesta ante Incidentes de Seguridad (CSIRT).
- Se necesita la acción conjunta de la industria a fin de proteger a las redes y los consumidores conectados mediante el desarrollo consistente y consensuado de estándares y el uso proporcionado de capacidades de monitoreo, detección y bloqueo.
- Garantizar la seguridad de las redes y los servicios móviles es una tarea compleja, ya que los operadores móviles y sus proveedores deben tomar múltiples decisiones en relación con la correcta implementación de normas de seguridad y el despliegue y configuración de una serie de funcionalidades. La GSMA ofrece asesoramiento y orientación a sus miembros sobre cómo alcanzar niveles de seguridad óptimos y también sigue trabajando en definir los requerimientos de seguridad básicos que deberían cumplir todos los operadores de redes móviles.
- Si bien el constante desafío que representa la seguridad será aún mayor con la evolución de la tecnología 5G, también constituirá una oportunidad de reconsiderar el concepto de seguridad y la forma en que se la puede proveer.
- Cuando sea necesario, la regulación debe aplicarse de manera coherente a todos los proveedores de la cadena de valor, con neutralidad respecto de los servicios y la tecnología, preservando al mismo tiempo el modelo de gobernanza de Internet de múltiples partes interesadas y permitiendo su evolución.

Seguridad e integridad de los dispositivos móviles

Para finales de 2021, alrededor de 5.300 millones de personas estaban suscritas a servicios móviles, lo cual representa el 67 por ciento de la población

mundial.[96] En el periodo hacia 2025, habrá cerca de 400 millones de suscriptores móviles nuevos, lo cual llevará la cifra total de suscriptores a 5.700 millones (70 por ciento de la población mundial).[97] Se espera que, para finales de 2030, haya 5.200 millones de conexiones 5G.[98]

Una llamada por teléfono celular o una trasmisión de datos recorre varias redes y, en su caso, los datos a menudo toman múltiples rutas como parte de una única comunicación. Como resultado, han surgido una gama de potenciales vulnerabilidades, que requieren que todos los operadores de red y el ecosistema de la industria móvil en general se mantengan atentos para poder responder a ellas. Los ataques de malware pueden afectar a varios blancos, como dispositivos móviles, aplicaciones de dispositivos e infraestructura. No obstante, con cada vez más acceso a banda ancha y la disponibilidad de variados malwares para dispositivos, la protección también debe abarcar los ataques de red basados en dispositivos (p. ej., los ataques o "tormentas" de señalización, los ataques de denegación de servicios (DoS), vulneraciones a la red desde la IoT).

Es probable que la amenaza más grave sea un ataque a gran escala, sistemático y premeditado, diseñado para inutilizar toda la red y afectar a todos los usuarios.

Existe el riesgo de que las vulneraciones a dispositivos móviles (p. ej., el malware enviado a través de correos electrónicos de *phishing*) puedan usarse como punto de entrada para propagarse a otros dispositivos conectados y así explotarlos para atacar redes basadas en IP.

Por ejemplo, el ataque del 21 de octubre de 2016 al importante controlador de infraestructura de sistema de nombres de dominio Dyn[99] se originó a partir del malware en una computadora, que luego se propagó a otros dispositivos y creó una red de *bots* que se usó para cometer un ataque de denegación de servicio distribuido (DDoS). A una escala mayor, se podría utilizar un método similar para inundar una red IP móvil con tráfico que provoque su saturación y la vuelva inutilizable. Para prevenir ese tipo de ataque, se necesita una estrecha cooperación entre los operadores de redes móviles y las agencias nacionales de aplicación de la ley, como parte de un plan de seguridad global, puesto que el ataque a las redes móviles es solo una de las posibles vías de ofensiva utilizadas por terceros hostiles.

La GSMA tuvo un papel central en la coordinación de actividades y la organización de iniciativas como el Esquema de Garantía de Seguridad de Equipos de Red (NESAS)[100], un marco de garantías de seguridad global que facilita las mejoras en los niveles de seguridad de toda la industria móvil para los proveedores de equipos de red. El esquema refleja las necesidades de seguridad del ecosistema entero, incluidos los gobiernos, los operadores de redes móviles y los reguladores, tal como lo definieron expertos de la industria mediante la GSMA y 3GPP.

Las amenazas de seguridad pueden tomar muchas formas. Los dispositivos móviles requieren de una SIM para conectarse a la red celular, ya sea en su formato tradicional de tarjeta UICC (SIM Card) o en su versión electrónica eUICC (eSIM). El cambio de SIM es un proceso comercial normal para la emisión y la provisión de nuevas SIM para los consumidores que necesiten reemplazarlas. El surgimiento del cambio fraudulento de SIM es un ejemplo en el que un servicio legítimo provisto por los operadores móviles para que sus clientes reemplacen su SIM vieja por una nueva permitió a estafadores obtener y usar la tarjeta SIM de reemplazo para acceder a las cuentas financieras y otros servicios del usuario legal. Los operadores móviles implementan continuamente las mejores prácticas para defenderse contra ataques como el mencionado. La eliminación gradual de métodos de autenticación antiguos (como el uso de información secreta y contraseñas seleccionadas por

96 https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf Mobile Economy Report 2022
97 ibíd.
98 5G in Context, Q1 2022 Data-driven insight into areas influential to the development of 5G. (mayo de 2022)
99 Dyn es un proveedor de sistemas de nombres de dominio (DSN) para proveedores de servicios de Internet, incluidos Twitter, Amazon, AirBnB y Spotify. La organización pudo restablecer sus servicios después de cada ataque, evitando a la vez una caída de todo el sistema, y mitigar un tercer ataque sin impactos para el consumidor.
100 https://www.gsma.com/security/nesas-network-equipment-vendors/

el usuario que deben ser expresadas verbalmente) es solo parte de la solución. Algunos operadores móviles ahora brindan API para servicios como bancos para poder conectarse y determinar si ha habido, recientemente, un cambio fraudulento de SIM.

Para el consumidor y las empresas, la oportunidad de utilizar estos servicios conlleva también el riesgo de que una gestión inadecuada de los dispositivos cree debilidades que vulneren las redes y afecten a un amplio conjunto usuarios. Un ataque a la seguridad representa una amenaza para todas las tecnologías, incluida la móvil. Los dispositivos móviles se convierten en el blanco por muchas razones. Por ejemplo, por su atractivo para los ladrones (debido a su valor relativamente alto y su tamaño reducido), el crimen organizado a menudo intenta cambiar el número de IMEI del dispositivo móvil robado para poder reactivarlo luego de haber sido reportado como robado. Otros criminales utilizan malware para ejecutar funciones que causan un daño al usuario, por lo general, mediante el robo de identidad y fraudes relacionados.

La GSMA colaboró en el desarrollo de mecanismos de protección, como los descritos en las Directrices para la eficiencia en la conexión de la Internet de las Cosas[101] de la GSMA, destinados a proteger las redes móviles contra la implementación masiva de dispositivos IoT ineficientes, inseguros o defectuosos. Además, la GSMA alienta a sus miembros a desplegar parches críticos de seguridad en dispositivos tan rápido como sea razonablemente posible.

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

Es esencial que los proveedores de la industria adopten buenas prácticas y políticas de seguridad. Programas como el Esquema de Acreditación de Seguridad de la GSMA ofrecen una certificación de proveedores de SIM, y aseguran que se promueva y se pueda demostrar el compromiso con los niveles de seguridad. Ya hace algún tiempo, la GSMA se ha encargado de garantizar la seguridad de los proveedores y sus productos a través del Esquema de Acreditación de Seguridad para proveedores de tarjetas SIM y del Esquema de Garantía de Seguridad de Equipos de Red (NESAS) para los proveedores de productos de infraestructura de red.

La GSMA también busca apoyar a los proveedores de servicios de Internet y desarrolladores de aplicaciones que operan en la red, quienes tienen la responsabilidad de evitar ser utilizados como canal para violar la integridad de la red móvil.

La GSMA apoya las normas de seguridad internacionales para servicios emergentes y reconoce el rol que pueden desempeñar los elementos de seguridad basados en tarjeta SIM, como alternativa a la incorporación de la seguridad integrada en el propio dispositivo móvil o en una tarjeta digital externa (microSD), dado que la tarjeta SIM demostró su resiliencia ante ataques.

101 https://www.gsma.com/newsroom/wp-content/uploads//TS.34-v8.pdf

5G, IoT y desarrollos futuros de la red

La tecnología 5G supone para la industria móvil una oportunidad sin precedentes de incrementar el nivel de seguridad de los servicios y la red. La GSMA explora con regularidad una gama de consideraciones de seguridad, incluyendo la seguridad por diseño, los modelos de despliegue de 5G y actividades de seguridad de 5G. Este análisis se incorpora a la Base de Conocimientos de Ciberseguridad 5G de la GSMA para brindar una orientación útil sobre diferentes riesgos de seguridad en 5G y medidas para mitigarlos.

El Grupo de Trabajo de Seguridad de 5G (5GSTF) de la GSMA se encarga de monitorear las labores en materia de seguridad de 5G dentro de la GSMA, en toda la industria en general y en la comunidad de desarrollo de estándares; para asegurar que estén disponibles todas las herramientas necesarias para brindar redes operativas seguras y resilientes. Particularmente, este grupo de trabajo se centra en las posibles disparidades entre los estándares y las implementaciones operativas y en cómo resolverlas.

Con la implementación de 5G viene también la migración a la computación en la nube, lo que plantea consideraciones de seguridad que, en su momento, eran responsabilidad del proveedor de equipos de red y que ahora recaen cada vez más en los operadores. Las redes virtualizadas brindan distintas oportunidades y beneficios, incluyendo la partición de la red, la escalabilidad de la red y una mayor flexibilidad de elección de proveedores. Dicho esto, también acarrean posibles amenazas a la seguridad. El traslado a la nube de los entornos de red de operadores provoca cambios significativos en las operaciones de seguridad y la gestión de esas redes, así como también en el tipo y las capacidades de los controles de seguridad. Los activos ya no se encuentran en un lugar fijo (caja física) con una capacidad planificada y una larga vida útil. En cambio, la pila de soluciones cambia de manera dinámica y, con ella, el tráfico de red en los interruptores físicos y virtuales. Esto aumenta la complejidad del monitoreo de las propiedades de procesamiento, almacenamiento y conectividad de cada componente, dado que ya no están unidos de manera estática.

Además, el ciclo vital de estas entidades se vuelve más corto para prestar servicios a una carga de trabajo durante unos minutos y luego quedar desactivadas. En caso de que se vean comprometidos, es necesario rastrear no solo las alineaciones de los activos virtuales/físicos, sino también la relación entre los activos, y el historial de cómo fueron asignados a medida que se movían dentro de la plataforma.

La tecnología 5G es necesaria para aprovechar la gran oportunidad que presenta la IoT. A medida que crece el ecosistema, se esperará que la industria móvil dé soporte a servicios personalizados en todos los verticales de la industria, donde se intercambian datos y se toman decisiones concienzudas usando IA. Según la última actualización del mercado IoT de GSMA Intelligence, la cantidad total de conexiones IoT se duplicará con creces para 2030 y ascenderá a 37.400 millones. Las conexiones de IoT de consumidores serán casi el doble entre 2020 y 2030 y alcanzarán los 13.800 millones.

Los servicios de IoT plantean desafíos de seguridad, no solo debido a la escala y la amplitud de los servicios, sino también a la funcionalidad crítica que brindan y la información privada que utilizan. Estos factores hacen de los servicios IoT blancos de alto valor para posibles atacantes que desean explotar estos servicios para, por ejemplo, lanzar ataques de DDoS o extraer datos sensibles. Además, hay un conjunto relativamente grande de dispositivos IoT legados con protecciones de seguridad integrada limitadas. La GSMA elaboró directrices de seguridad de la IoT y un esquema de autoevaluación de seguridad para distintos actores del ecosistema. Las directrices de seguridad de la IoT de la GSMA son una guía exhaustiva para los proveedores de servicios de IoT.

A medida que la industria se traslada de métodos tradicionales con hardware específico a métodos orientados en la nube, crece la cantidad de opciones de infraestructura. La clasificación típica de las opciones de infraestructura moderna se divide en cuatro grupos: software como servicio (SaaS), infraestructura como servicio (IaaS), plataforma como servicio (PaaS), e infraestructura en el sitio.

La mudanza desde el método tradicional de hardware especializado hacia uno orientado a la nube propone una serie de oportunidades y beneficios, como la partición de la red, la escalabilidad de la red y una mayor flexibilidad de elección de proveedores. El software de computación en la nube puede funcionar en varias plataformas no propietarias, abarcando desde el alojamiento de todo el producto en la nube hasta todo elemento bajo propiedad y gestión del operador. El Análisis de Amenazas a la Virtualización de las Funciones de Red (FS.33)[102] de la GSMA expone una descripción integral de las amenazas relacionadas con la virtualización de las funciones de red (NFV) y la infraestructura subyacente y plataformas que alojan la NFV. También incluye orientación exhaustiva sobre los controles de riesgos adecuados.

La infraestructura virtualizada y las interfaces más abiertas traen grandes beneficios, pero también

complejizan y pluralizan la cadena de suministro de 5G en comparación con 4G y generaciones anteriores. Así, aunque se da paso a la flexibilidad, escalabilidad y ahorro en costos potenciales, también se complica la cadena de suministro. La necesidad de contar con una mayor resiliencia en la infraestructura de red hizo que muchos reguladores impongan requisitos a los operadores para que estos aumenten los niveles de diversidad, seguridad y control.

La GSMA alienta a los proveedores a participar de los esquemas de garantía de seguridad reconocidos por la industria, como el Esquema de Garantía de Seguridad de Equipos de Red (NESAS)[103] de la GSMA y motiva a los operadores a comprar equipos a proveedores que participen en estos esquemas. La Herramienta de Cadena de Suministro de la GSMA expone una serie de servicios y lineamientos para ayudar a que los operadores y sus proveedores comprendan mejor la seguridad e implementen las mejores prácticas.

102 https://www.gsma.com/security/resources/fs-33-network-function-virtualisation-nfv-threats-analysis/
103 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Implicancias clave para los gobiernos, la industria y otras partes interesadas relevantes

La GSMA apunta a tener un rol significativo en ayudar a moldear el desarrollo estratégico, comercial y normativo del ecosistema de seguridad de la IoT y 5G.

— La GSMA reconoce que tiene un papel clave en reunir y priorizar los requerimientos de seguridad de 5G para su estandarización. La GSMA y sus miembros invitan a otros expertos en el tema y a agencias de aplicación de la ley a participar para asegurar que se comprendan claramente todas las necesidades.

— El gobierno debería apoyar la naturaleza global de los futuros mercados de redes y la gran variedad de dispositivos que se conectarán a Internet en el futuro. Debería trabajar en todas las jurisdicciones para garantizar la coherencia y la claridad de la regulación y las obligaciones de seguridad de la red para todos los actores que forman parte de esta cambiante y compleja área.

— La industria móvil continuará interactuando con el ecosistema en general y fomentando las inversiones necesarias, de manera directa o a través de proveedores y socios del ecosistema, para garantizar la seguridad de las redes y los dispositivos a medida que evoluciona la tecnología, en especial cuando se trata de la transición a la virtualización de las funciones de red y la tecnología 5G.

La GSMA también llevó a cabo un análisis integral de amenazas junto a expertos de la industria de todo el ecosistema, reguladores y también fuentes públicas como 3GPP, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Instituto Nacional de Estándares y Tecnología (NIST). Las amenazas se asignaron a controles de seguridad adecuados y eficaces, y el análisis se incorporó a la Base de Conocimientos de Ciberseguridad 5G, brindando orientación útil sobre una gama de riesgos de seguridad 5G y de medidas de mitigación.

La Base de Conocimientos de Ciberseguridad 5G pone a disposición el conocimiento conjunto del ecosistema 5G para incrementar la confianza en las redes 5G y hacer que el mundo interconectado sea lo más seguro posible. La GSMA monitorea las actividades de grupos de hackers constantemente, al igual que de investigadores, innovadores y otras partes interesadas de la industria, para mejorar la seguridad de las redes de una generación a otra.

Iniciativas de seguridad de la GSMA

La GSMA organiza una serie de iniciativas a nivel industria (Figura 7) para concientizar a los operadores acerca de los riesgos y las opciones de mitigación disponibles para proteger sus redes y clientes. Los reguladores de todo el mundo reconocen este trabajo como suficiente para eliminar la necesidad de regulación formal de varios problemas de seguridad.

Figura 7
Servicios de seguridad y fraude de la GSMA

Divulgación Coordinada de Vulnerabilidades (CVD)
Un recurso para que los investigadores revelen las vulnerabilidades que podrían afectar al ecosistema móvil

GSMA Device Check™
Protección contra riesgos de manejo de dispositivos robados o fraudulentos mediante este servicio de búsqueda instantánea

Registro de Dispositivos de la GSMA
Disuadir los crímenes relacionados con dispositivos mejorando la información de

Garantía de Seguridad de eUICC (eSA) de la GSMA
Generar confianza en que los chips de eUICC cumplen rigurosos estándares de seguridad de la industria

Esquema de Garantía de Seguridad de Equipos de Red (NESAS) de la GSMA
Evaluación de seguridad de los procesos de desarrollo de productos, vida útil y productos de infraestructura de los

Esquema de Acreditación de Seguridad (SAS) de la GSMA
Auditorías de seguridad y certificación de la producción de SIM/eSIM y los sitios de gestión de suscripciones

Servicios exclusivos para los miembros de la GSMA:

GSMA (FASG)
Intercambio de inteligencia sobre amenazas en un foro confidencial y colaboración para mantener la seguridad de los activos de los operadores y sus clientes

Centro de Análisis e Intercambio de Información de las Telecomunicaciones (T-ISAC) de la GSMA
Intercambio oportuno de información procesable sobre amenazas de ciberseguridad en un entorno de confianza

Anexo:
Principios de la industria móvil

Como parte de su continuo trabajo en los temas de seguridad, privacidad y protección identificados en este informe, la GSMA y sus operadores miembros reconocen la necesidad de contar con un enfoque flexible y dinámico para encontrar un equilibrio entre los derechos del consumidor/ciudadano, las necesidades de seguridad pública y el rol de los operadores de redes móviles en su respaldo a ambos. Si bien la respuesta más apropiada será la que mejor se acomode a las necesidades y variaciones de cada mercado local en vez de solo seguir lo que se pudo haber hecho en otro lugar, queda claro que, aun así, los diferentes grupos regionales deben colaborar y compartir sus aprendizajes.

La GSMA y sus organizaciones miembros establecieron los siguientes principios, que demuestran cómo continúan desarrollando soluciones para las cuestiones planteadas en este informe.

Protección del consumidor

Para promover el uso seguro y responsable de los servicios y dispositivos móviles en línea, es indispensable contar con los esfuerzos de las múltiples partes interesadas. En particular, los gobiernos y sus agencias de aplicación de la ley deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar conductas delictivas. A menudo, esto requerirá de una cooperación global. Otros actores del ecosistema de la industria, como los fabricantes de dispositivos y los proveedores de servicios móviles, deberían participar en las iniciativas destinadas a proteger al consumidor al momento de usar servicios y dispositivos móviles, y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios de forma segura. Los operadores pueden desempeñar un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, y en alentarlo a utilizar todo el conjunto de medidas de seguridad disponibles. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para tratar las cuestiones relacionadas con la protección del consumidor y las actividades ilegales y perjudiciales vinculadas al uso de teléfonos celulares o facilitadas por estos, mediante los siguientes esfuerzos:

— Trabajar en colaboración con otros organismos en pos de brindar soluciones multilaterales adecuadas.

— Implementar soluciones diseñadas con el objetivo de prevenir el uso de las redes para la comisión de fraudes y actividades delictivas y el uso de los dispositivos para perjudicar al consumidor.

— Educar al consumidor acerca de las conductas seguras relacionadas con el uso de aplicaciones y servicios móviles para así aumentar su confianza.

Protección de la privacidad del consumidor

El objetivo principal de la protección de la privacidad es generar confianza en que los datos privados son protegidos de forma adecuada y conforme con la regulación y los requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia en todos los servicios, sectores y geografías. Los gobiernos pueden ayudar a garantizar este resultado, y a la vez ofrecer la flexibilidad necesaria para la innovación, mediante la adopción de marcos legales basados en riesgos para así salvaguardar los datos privados y promover prácticas de gobernanza digital responsables que estén alineadas con la regulación local. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas proactivas para proteger y respetar los intereses de privacidad del consumidor y facilitar la toma de decisiones informadas sobre qué datos personales se recopilan y cómo se utilizan, mediante la implementación de políticas que promuevan lo siguiente:

— El almacenamiento y procesamiento seguro de toda la información personal y privada, conforme a los requisitos legales, cuando corresponda.

— La transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y el pleno cumplimiento de las exigencias legales.

— La entrega de información y herramientas para que el consumidor pueda tomar decisiones simples y significativas sobre su privacidad.

Protección de la seguridad pública

En línea con el objetivo general de proteger la seguridad pública, los operadores de redes móviles deben asumir responsabilidades adicionales y colaborar con las agencias de aplicación de la ley, conforme a las leyes, la regulación, las obligaciones relativas a las licencias y la legislación local.

Es importante que los gobiernos garanticen la existencia de un marco legal proporcional que describa claramente las facultades de las que disponen las agencias nacionales de aplicación de la ley. Dicho marco legal debe garantizar también que las solicitudes de asistencia sean efectivamente necesarias y proporcionadas, que estén al proveedor de tecnología o de servicios de comunicaciones más apropiado y que respeten los principios de derechos humanos. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores cumplirán toda obligación, establecida por ley o por licencias, relacionadas con temas de protección o seguridad pública en los países en los que operan, a la vez que darán su apoyo en cuestiones de derechos humanos.

Además, colaborarán con las agencias de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- Trabajar con las agencias pertinentes cuando la situación particular así lo requiera, a fin de desarrollar e implementar soluciones adecuadas para lograr el objetivo final con mínimas molestias al consumidor y los servicios críticos.
- Construir redes que tengan la funcionalidad de abordar situaciones de emergencia y seguridad, cuando corresponda.
- Brindar claridad sobre las limitaciones de las acciones que se pueden tomar en la cadena de valor e indicar cuándo se deben implementar acciones por parte de terceros.

Protección de la seguridad de las redes y la integridad de los dispositivos

Los actores de la industria deben trabajar en conjunto y coordinar con las agencias internacionales de aplicación de la ley para compartir inteligencia sobre amenazas para así responder a ataques maliciosos a las redes y dispositivos móviles e identificar a los responsables. Esto se puede lograr a través de la participación de los equipos de respuesta ante incidentes de seguridad existentes y la creación de nuevos equipos, si fuese necesario, para contrarrestar cualquier deficiencia. Cuando se necesite, la regulación debería aplicarse de manera coherente a todos los proveedores de la cadena de valor, con neutralidad respecto de los servicios y la tecnología. Preservando al mismo tiempo el modelo de gobernanza de Internet de múltiples partes interesadas y permitiendo su evolución. Con esto en mente, la GSMA y sus operadores de redes móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas para proteger la infraestructura subyacente y asegurar que se provea al cliente el servicio de comunicaciones más seguro y confiable posible, mediante las siguientes acciones:

- Tomar medidas para garantizar la seguridad de la infraestructura de red que operan y controlan.
- Promover las asociaciones entre el sector público y el privado a través de estrategias globales y coordinadas para minimizar el riesgo de hackeo o uso de la red para fines maliciosos.
- Brindar claridad sobre qué parte de la infraestructura es responsabilidad de los operadores y dónde se encuentran las fronteras con otros servicios o infraestructuras.

Oficina Central de la GSMA
One Angel Lane
London, U.K.
EC4R 3AB
Reino Unido
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601