Seguridad, privacidad y protección del ecosistema móvil

Cuestiones clave e implicancias de las políticas públicas

La GSMA representa los intereses de los operadores móviles de todo el mundo, reuniendo a casi 800 operadores con unas 300 compañías del amplio ecosistema móvil. Estas empresas incluyen fabricantes de teléfonos y dispositivos móviles, empresas de software, proveedores de equipamiento y empresas de internet, así como también organizaciones de sectores adyacentes de la industria. La GSMA también organiza eventos líderes de la industria como el Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas y la serie de conferencias Mobile 360.

Para más información, visite el sitio web corporativo de la GSMA en **www.gsma.com**

Siga a la GSMA en **Twitter: @GSMA y @GSMALatam**

Para mayor información o consultar sobre este informe, envíe un correo electrónico a **publicpolicy@gsma.com**

A.T. Kearney es una consultora líder de alta dirección a nivel global, con oficinas en más de 40 países. Desde 1926, hemos sido asesores de confianza de las empresas más destacadas del mundo. A.T. Kearney es una firma propiedad de sus socios, con el compromiso de ayudar a sus clientes a lograr una clara ventaja competitiva en los temas más cruciales para su trabajo.

Para más información, visite **www.atkearney.com**

Tabla de Contenidos

1 Resumen ejecutivo

En las últimas tres décadas, el mercado de servicios de telecomunicaciones móviles creció hasta representar más de 7600 millones de conexiones móviles,[1] brindándole servicios a 4700 millones de suscriptores móviles únicos a nivel mundial.[2] Se estima que este crecimiento continuará y se prevé que para el año 2020, casi tres cuartas partes de la población mundial podrán disfrutar los beneficios que ofrece una suscripción móvil.[3]

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 novedosas y, a menudo, inesperadas. Además, los consumidores de todo el mundo muestran un apetito voraz por adoptar nuevas tecnologías. En muchas economías en desarrollo, la ubicuidad de los servicios móviles y los *smartphones* ha hecho posible la aparición de modelos de negocios completamente nuevos que soportan nuevas formas de interacción, tanto personal como comercial, y permiten que el ecosistema móvil más amplio aporte USD 3,1 billones en valor económico agregado.[4]

Dada la creciente relevancia de internet a nivel económico y social, en general, y del uso de internet móvil, en particular, surge la consiguiente necesidad de proteger a los consumidores que utilizan estos servicios y garantizar que puedan seguir haciéndolo en forma segura. Sin esa protección, se corre el riesgo de que los beneficios que ofrecen las comunicaciones modernas se vean socavados. Si el consumidor no confía en la integridad del servicio de comercio electrónico o se preocupa por la posible interceptación de datos privados y sensibles cuando utiliza un servicio de comunicaciones, la probabilidad de que utilice dicho servicio disminuirá, debiendo recurrir a canales de comunicación más costosos y menos efectivos como resultado. En casos más extremos, un servicio podría ser sujeto de abuso y así poner en riesgo estas necesidades fundamentales, como en la década de los 90, cuando este tipo de servicios se promocionaba como proveedor de seguridad (a conductores de automóviles o personas en situación de vulnerabilidad que viajaban solas) y privacidad (llamadas desde un dispositivo personal en lugar de una línea fija en el living de una casa).

La industria móvil se esforzó por educar a los consumidores y desarrolló nuevas funcionalidades que aumentaron la confianza en sus servicios. Con cada iteración tecnológica adicional, se introdujeron nuevos servicios, tales como la encriptación y la validación de la identificación del usuario, que aumentaron cada vez más la seguridad de los servicios móviles y minimizaron el potencial de fraude, robo de identidad y muchas otras posibles amenazas.

La confianza que sustenta estos servicios y permite que todas las personas del mundo puedan comunicarse, conducir sus negocios, compartir ideas e interactuar, no puede darse por sentada. A medida que se desarrollan servicios más avanzados y complejos, también 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, la capacidad de los criminales de interceptar comunicaciones aumenta con frecuencia y va desde el robo de grandes cantidades de datos hasta el hackeo y la divulgación de comunicaciones privadas durante las elecciones estadounidenses en 2016. Aunque con perfil más bajo, la prevalencia de estafas relacionadas con *phishing*, *ransomware* y fraude de dinero son igual de perjudiciales para el individuo. Dado que el objetivo de estas estafas son las comunicaciones en general y no solo las de un dispositivo móvil, 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, es importante que el objetivo de cualquier intervención sea 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 los organismos de seguridad que, en ocasiones, deben interceptar ciertas comunicaciones para proteger el bien público. Además, se debe tener 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 "chat" de mensajería, en realidad, están

1. Incluye las conexiones máquina a máquina (M2M)
2. GSMA, 2016. "La Economía Móvil: 2016"
3. Ibídem.
4. Ibídem.

1

utilizando dos dispositivos diferentes, posiblemente dos sistemas operativos y aplicaciones de interfaces diferentes y múltiples redes para conectarse a través de una plataforma de mensajería, 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 interceptación y abuso hasta hackeo y software malicioso. El esfuerzo por proteger al consumidor puede desviarse si se enfoca en una única posible debilidad, sin considerar todas las demás. Por lo general, toda actividad 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 del uso seguro de sus servicios, a la vez que también intenta proteger la privacidad de sus clientes en la mayor medida de lo posible. Está claro que estos esfuerzos se enmarcan dentro de una dimensión tecnológica: estándares en constante mejora, implementación de mejores versiones de la tecnología, pruebas de redes para identificar debilidades y desarrollo de la capacidad de detectar e impedir ataques maliciosos. La GSMA desempeña un papel clave en la coordinación de actividades y en el liderazgo de iniciativas tales como el IMEI (códigos identificadores destinados a combatir el robo de dispositivos móviles) o los esquemas de Acreditación de Seguridad para componentes de infraestructura crítica. Además, varios 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; la tendencia natural es esperar que los operadores de redes resuelvan el tema. Sin embargo, las consideraciones sobre tecnología y defensa de la competencia dificultan mucho (y, en ocasiones, hasta impiden) la intervención del operador de redes móviles en los intercambios que tienen lugar entre el proveedor de servicios en línea y el usuario. Asimismo, dada la gran diferencia entre el estándar de protección de datos que se aplica en distintas jurisdicciones y, especialmente, entre el sector de telecomunicaciones versus el de los proveedores de servicios en línea, un operador de redes móviles solo puede comprometerse a proteger los datos de su usuario directo y a concientizar al usuario final de que posiblemente esté compartiendo demasiados datos con organizaciones que exceden el control del operador. La colaboración entre los gobiernos y el ecosistema móvil más amplio es importante 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, financiados a través de 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 comunicaciones bajo 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 focaliza en

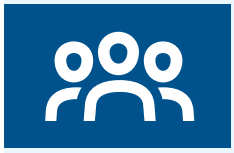
establecer principios comunes y en educar a todas las partes sobre las mejores prácticas. Los operadores de redes móviles enfrentan otros dos desafíos adicionales: son la primera línea de ataque cuando los gobiernos intentan poner en tela de juicio a las compañías internacionales de internet, sobre las 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.

Acciones de los gobiernos, la industria y otros interesados

El presente reporte trata, una a una, las principales problemáticas de 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. Estas cuestiones son tan importantes que los operadores móviles miembros de la GSMA han concluido que deben trabajar más estrechamente, tanto a nivel nacional como internacional, para poder garantizar una respuesta más efectiva. Ninguna de estas cuestiones multidimensionales puede "resolverse" en forma simple ni mediante las acciones aisladas de una organización o un sector. A fin de obtener los mejores resultados, tanto para los usuarios móviles como para la sociedad en general, también se debe contar con el compromiso y la acción de los gobiernos, los organismos de seguridad, las organizaciones multilaterales y no gubernamentales además de las empresas de todo el ecosistema digital, así como los esfuerzos personales de los mismos 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 una cooperación más estrecha entre las múltiples partes que prestan servicios al usuario final es común a todos los temas y geografías, a fin de garantizar la maximización de la seguridad y la confianza como también el desarrollo e implementación de soluciones que brinden un beneficio mayor y generalizado para toda la sociedad. La naturaleza global de los sistemas de comunicaciones modernos, desde las normas 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.

El reporte incluye el conjunto de principios que los operadores móviles miembros de la GSMA sostienen en la orientación de sus acciones en pos de proteger al consumidor y la seguridad de las redes de comunicaciones móviles. También hace un llamado a los formuladores de políticas y reguladores para que adopten una amplia visión sobre las cuestiones en juego y así colaboren en el desarrollo de soluciones (elaboradas por todas las partes interesadas) que protejan mejor los intereses generales de los consumidores, las empresas y la sociedad civil. Este claro compromiso con la seguridad, privacidad y 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 inmediato, enriqueciendo la vida de las personas y la sociedad con el máximo potencial de estas apasionantes y dinámicas tecnologías.

1



Protección del consumidor

Para promover el uso seguro y responsable de los servicios y dispositivos móviles en línea, es necesario contar con el esfuerzo de las múltiples partes interesadas. En particular, los gobiernos y sus organismos de seguridad deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar conductas delictivas. A menudo, esto requerirá de la cooperación global. Asimismo, otros actores del ecosistema de la industria, como fabricantes de dispositivos y proveedores de servicios móviles, deberían participar en las iniciativas destinadas a proteger al consumidor en relación al uso de servicios y dispositivos móviles y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios en forma segura. Los operadores juegan un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, además de 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 móviles o facilitadas por estos, mediante los siguientes esfuerzos:

- **Trabajar en colaboración con otros organismos en pos de encontrar soluciones multilaterales adecuadas**
- **Implementar soluciones diseñadas con el objeto 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**
- **Enseñarle al consumidor 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 están protegidos de forma adecuada y conforme con las reglamentaciones y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia a través de 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 responsables de gobierno digital que se encuentren alineadas con las reglamentaciones locales. 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 recolectan y cómo se utilizan, mediante la implementación de políticas tales como:

- **Almacenamiento y tratamiento seguro de toda información personal y privada, conforme a los requisitos legales, cuando corresponda**
- **Transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y el pleno cumplimiento con los requisitos 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 los organismos de seguridad, conforme a las leyes y reglamentaciones, las obligaciones contenidas en las licencias y la legislación local. Es importante que el gobierno garantice la existencia de un marco legal adecuado que describa claramente las facultades de los organismos nacionales de seguridad. Asimismo, este marco debe garantizar 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 con toda obligación, establecida por ley o por sus licencias, relacionadas con temas de protección o seguridad pública en los países en los que operan, a la vez que cumplen con los principios de derechos humanos. Los operadores colaborarán con los organismos de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- **Trabajar con los organismos pertinentes cuando la situación particular así lo requiera, a fin de desarrollar e implementar soluciones adecuadas para alcanzar el objetivo final con el mínimo trastorno al consumidor y los servicios críticos**
- **Construir redes que tengan la funcionalidad de enfrentar situaciones de emergencia y seguridad, cuando corresponda**
- **Ser claros sobre las limitaciones de las acciones que se pueden tomar en relación con 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 dispositivos

Los actores de la industria deben trabajar codo a codo y en forma coordinada con los organismos internacionales de seguridad para compartir inteligencia sobre amenazas a fin de responder a ataques maliciosos en las redes y dispositivos móviles e identificar a los autores. Esto se puede lograr con la participación de los equipos de respuesta ante incidentes de seguridad y la creación de nuevos equipos, si fuese necesario, para resolver cualquier deficiencia. Cuando sea necesario, la regulación debe aplicarse de manera consistente a todos los proveedores de la cadena de valor, en forma neutral 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 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 público-privadas para minimizar el riesgo de *hackeo* o uso de la red para fines maliciosos a través de estrategias globales y coordinadas**
- **Ser claros sobre qué parte de la infraestructura es responsabilidad del operador y dónde se encuentra la demarcación con otros servicios o infraestructura**

2 Introducción

En todas las regiones del mundo, se observa un aumento en las amenazas, ya sean reales o percibidas, a la seguridad nacional, la seguridad pública y la privacidad del individuo. Las redes móviles desempeñan un importante papel en la protección de la seguridad pública, tal como cuando los organismos de seguridad, siguiendo su mandato, realizan investigaciones criminales en base a información sobre llamadas e interceptación de comunicaciones. Las redes también son esenciales para el soporte de comunicaciones sobre incidentes importantes o el rastreo de la propagación de amenazas a la salubridad. A nivel personal, hay casos de fraude, robo de identidad, ciberacoso y otras actividades ilegales que se realizan tanto a través de redes móviles como de servicios digitales o en línea a los cuales se accede a través de las redes fijas. Acontecimiento recientes, como los casos de violaciones de datos que tuvieron un alto perfil, han también generado intranquilidad en un gran número de consumidores sobre la protección de la seguridad y privacidad de los detalles de su vida personal, por ejemplo.

En este contexto, los operadores de redes móviles enfrentan el permanente desafío de brindar a sus clientes una experiencia móvil segura, cumpliendo al mismo tiempo con las obligaciones de proteger la seguridad pública. La GSMA y sus operadores miembros ya están trabajando para enfrentar y solucionar las cuestiones de privacidad y seguridad, así como para promover el uso seguro y fructuoso de los servicios móviles y la gran variedad de aplicaciones que soportan.

El objetivo de este reporte es explicar las cuestiones y desafíos más importantes en torno a la seguridad y privacidad en el ámbito móvil, destacando tanto las complejidades como las concesiones y mostrando las iniciativas y acciones de la industria que ya se encuentran en curso. En aquellos casos donde existe la posibilidad de hacer aún más, el reporte 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 el informe trata cada cuestión individualmente, también reconoce las diferentes interdependencias y superposiciones entre las mismas.

Estructura

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

Figura 1

Marco de seguridad y privacidad

Las cuatro secciones siguientes del presente reporte tratan cada área en forma individual, o sea:

1. **Protección del consumidor** – promover el uso seguro de los servicios móviles
2. **Protección de privacidad y datos** – proteger la privacidad del consumidor y el almacenamiento y tratamiento seguros de los datos personales del individuo
3. **Protección de la seguridad pública** – definir el rol y las responsabilidades de los operadores móviles respecto de 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 las mismas

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

Tal como demostrará el reporte, la naturaleza de estas cuestiones requiere de una acción coordinada en todas las geografías y los segmentos de la industria. Si bien la industria móvil lidera los esfuerzos de abordar estas cuestiones, existen varios otros grupos activos en este espacio, desde organismos de normalización como el 3GPP, IETF y oneM2M, hasta entes internacionales, tales como la UIT, el Diálogo de la Industria [Industry Dialogue, ID] de las Telecomunicaciones, la Iniciativa de Red Global [Global Network Initiative, GNI] y UNICEF. A todos ellos les toca desempeñar un valioso e importante papel en encauzar el debate y desarrollar soluciones. La GSMA recibe con gusto toda colaboración y compromiso adicional del ecosistema móvil y de la industria de las TIC más amplia en todos estos temas.

3 Protección del consumidor

A medida que los servicios móviles adquieren mayor importancia y alcance, se están gestando cambios fundamentales en la forma de conectarse e interactuar de las personas, entre sí y con las empresas. Dada la masividad del uso de la tecnología móvil, probablemente no se pueda evitar que algunas personas intenten utilizarla para perjudicar a otras.

Para que los consumidores en todo el mundo sigan disfrutando los diferentes beneficios que ofrece la tecnología móvil, es importante que estos servicios puedan utilizarse en forma segura y confiable. Esta sección está dedicada a las cuestiones que afectan, en forma directa, la seguridad y el bienestar del consumidor de los servicios móviles y, especialmente, los casos en los que el usuario de dispositivos y servicios móviles está expuesto a las amenazas generadas por comportamientos ilícitos, criminales o antisociales, tales como:

- Protección de la infancia y personas vulnerables
- Robo y comercialización de dispositivos robados y venta y uso de dispositivos falsificados
- Fraude y seguridad de los dispositivos móviles

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y otros interesados. Más adelante, en este capítulo, se describen en forma detallada.

3

Protección del consumidor

Para promover el uso seguro y responsable de los servicios y dispositivos móviles en línea, es necesario contar con el esfuerzo de las múltiples partes interesadas. En particular, los gobiernos y sus organismos de seguridad deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar conductas delictivas. A menudo, esto requerirá de la cooperación global. Asimismo, otros actores del ecosistema de la industria, como fabricantes de dispositivos y proveedores de servicios móviles, deberían participar en las iniciativas destinadas a proteger al consumidor en relación al uso de servicios y dispositivos móviles y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios en forma segura. Los operadores juegan un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, además de 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 móviles o facilitadas por estos, mediante los siguientes esfuerzos:

- **Trabajar en colaboración con otros organismos en pos de encontrar 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**
- **Enseñarle al consumidor conductas seguras relacionadas con el uso de aplicaciones y servicios móviles, para así aumentar su confianza**

Infancia y personas vulnerables

Los servicios móviles ofrecen un sinnúmero de beneficios a los grupos de usuarios potencialmente vulnerables, incluidos los niños y ciertos grupos de mujeres, entre otros. Estos servicios pueden ayudarlos a estar más conectados, ser más independientes y mantenerse más seguros. No obstante, tanto los niños como las personas vulnerables, también corren el riesgo de estar expuestos a conductas negativas. Por ejemplo, un estudio de la GSMA analizó la brecha de género en términos de propiedad y uso de dispositivos móviles e identificó que el 68% de las mujeres tienden a percibir el tema de seguridad y el acoso de extraños como una barrera a la propiedad y uso de dispositivos móviles.[5] Las cuestiones relacionadas con "seguridad y acoso" surgieron como una de las cinco principales barreras para la propiedad y el uso de teléfonos móviles por parte de las mujeres.[6] 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 las mayores probabilidades de obtener beneficios con el uso de los servicios móviles.

El consumidor debe familiarizarse con el uso seguro de las funcionalidades de los dispositivos (por ejemplo, las cámaras) y los servicios móviles. Esta necesidad se incrementa aún más cuando se trata de dispositivos móviles más poderosos, que pueden ser usados, cada vez más, para realizar tareas comunes, incluso para el acceso a aplicaciones de educación formal y aprendizaje informal, banca y salud electrónica. A medida que el consumidor aprende a aceptar estos diversos beneficios, se presenta una oportunidad para ampliar proactivamente sus aptitudes digitales, ya en constante evolución, para 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 los aportes de las diferentes partes interesadas. Es importante que los operadores de redes móviles participen en el diseño de estos programas para asegurarse de que se enfoquen en las necesidades de una industria en rápida evolución y aclaren el rol de los diferentes actores del ecosistema de las TIC. Los operadores de redes móviles ya juegan un papel importante en la promoción de los beneficios de la tecnología móvil, al tiempo que enseñan a los potenciales grupos vulnerables a desarrollar una resiliencia digital, a utilizar los servicios en forma segura y a responder y denunciar cualquier abuso, cuando corresponda.

Apoyo a la inclusión y seguridad de las mujeres

En promedio, la probabilidad de que las mujeres tengan un dispositivo móvil es 14% menor que la de los hombres. Esta brecha de género llega hasta 38% en algunas regiones.[8] En total, más de 1700 millones de mujeres en países de ingresos bajos y medios no poseen dispositivos móviles.[9] Si bien los motivos son diversos, el programa Connected Women de la GSMA trabaja para identificarlos y solucionarlos. La preocupación por la seguridad y el acoso surgieron como importantes barreras para la adopción de dispositivos móviles por parte de algunas mujeres, especialmente en países de bajos ingresos. [10] En la actualidad, la GSMA, junto con las organizaciones que forman parte de la misma, está lanzando una iniciativa que expande aún más el trabajo del programa Connected Women, concentrándose específicamente en cuestiones de seguridad y acoso.

Los operadores de redes móviles reconocen que, al utilizar los servicios móviles de seguridad, las mujeres pueden seguir disfrutando la seguridad que ofrece la conectividad al tiempo que se reduce la posibilidad 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 propietarios de teléfonos básicos, tales como 'Banglalink Emergency' [Emergencia Banglalink], que envían automáticamente una alerta por SMS a tres contactos previamente registrados cuando el usuario marca un número corto. La ubicación del usuario también es enviada a esos contactos,[11] mejorando así su nivel de seguridad.

5. GSMA, 2015. "Connected Women - Cerrando la Brecha de Género: Uso y acceso móvil en países de ingresos bajos y medio"
6. Ibídem.
7. Ibídem.
8. Ibídem.
9. Ibídem.
10. Ibídem.
11. Banglalink Emergency: https://www.banglalink.net/en/personal/digital-services/messaging-and-utility-services/bl-emergency-alert

Salvaguarda de usuarios jóvenes y protección de la infancia en línea

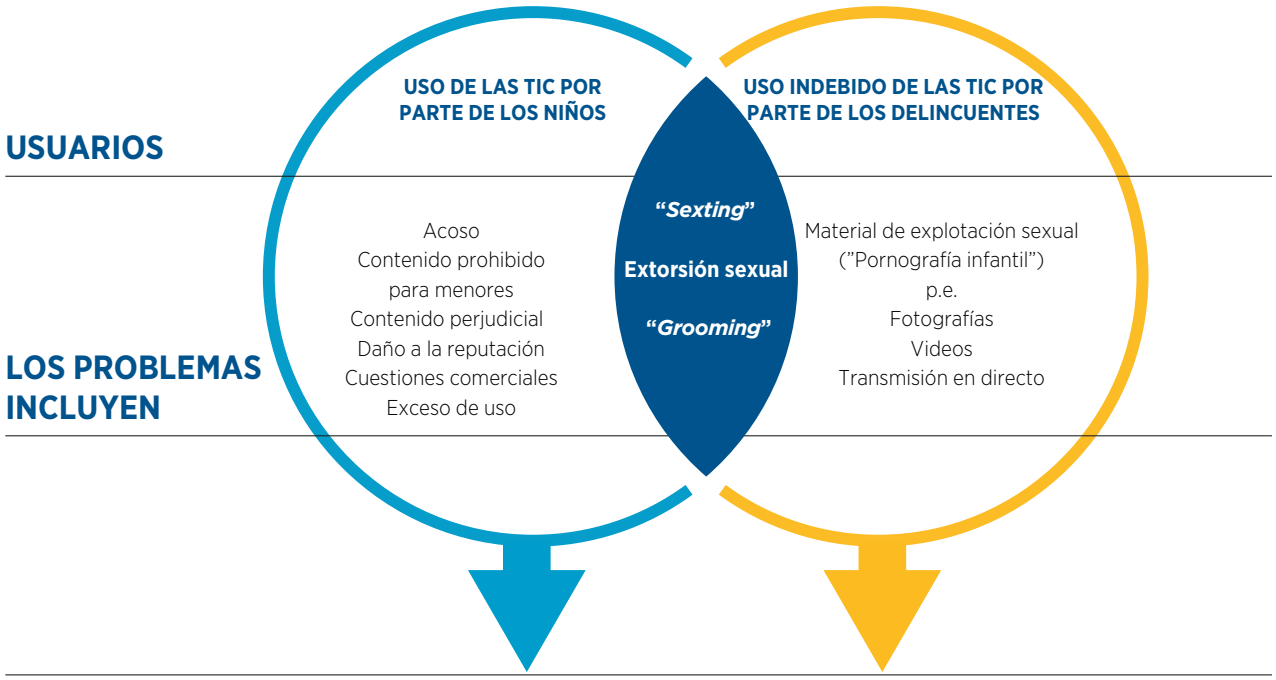
Los niños son el segundo grupo de usuarios de servicios móviles potencialmente vulnerables. Para comprender el tema de la protección infantil en línea, es importante distinguir dos distintas cuestiones:

1. Estimular el uso seguro y responsable de los servicios móviles por parte de los niños
2. Combatir el uso indebido de los servicios móviles por parte de adultos/delincuentes, por ejemplo, para elaborar, 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.

Figura 2

Protección de la infancia en línea – problemas y usuarios



El elemento clave para que los niños y jóvenes lleven una vida digital más segura es el fomento de conductas positivas en línea, así como la enseñanza de los riesgos potenciales y el empoderamiento para navegar la red de internet con mayor seguridad y confianza. Junto a otros interesados, tales 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 proveer controles parentales.

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 lucro, requiere de una serie de acciones por parte de las diferentes partes interesadas. Los gobiernos deben contar con la legislación correspondiente, los organismos de seguridad deben estar equipados y facultados para investigar todos los aspectos de abuso sexual infantil (desde la captación de niños y jóvenes con fines sexuales o "*grooming*" hasta la distribución de material de explotación sexual infantil) y deben implementarse líneas nacionales de atención telefónica para denunciar el abuso sexual infantil en línea. Posteriormente, la industria puede colaborar con esta acción colectiva, por ejemplo, trabajando codo a codo con las líneas nacionales de atención telefónica para eliminar el material de explotación sexual infantil de sus servicios en cuanto sea de su conocimiento y, con el gobierno, en toda circunstancia relevante en la que haya un proceso legal.

Las áreas en las que existe superposición, tal como ilustra la Figura 2, requieren ambos tipos de respuestas. Por ejemplo, para mitigar el riesgo de que los jóvenes compartan imágenes sexuales propias generadas por ellos mismos ("*sexting*"), esos niños deben entender cuáles son las posibles consecuencias de compartir dichas imágenes y no tener el control sobre las mismas. Cuando un delincuente obtiene y comparte este material sexual autogenerado, se debe iniciar un proceso para remover dicho material (tema que se describirá en mayor detalle en la subsección relativa a material de explotación sexual infantil), además de investigar y procesar al delincuente.

Estimular el uso seguro y responsable de la tecnología y los servicios móviles por parte de los niños

La industria móvil, junto a otros interesados, ha tomado medidas proactivas para fomentar el uso más seguro de los servicios móviles por parte de los niños y los jóvenes.

En cooperación con interesados de todo el ecosistema móvil, así como las ONG y las organizaciones de gobierno, el programa mYouth[12] de la GSMA se dedica a ayudar a los jóvenes a aprovechar al máximo su experiencia móvil. Entre otras iniciativas, el programa mYouth se concentra en distribuir información sobre estrategias que se pueden utilizar para promover el uso seguro y responsable de los dispositivos móviles. Las directrices de los operadores móviles incluyen programas de educación y concientización de amplio alcance, además de la provisión de soluciones técnicas tales como los servicios de control parental. Gracias a su asociación con Child Helpline International, la GSMA ha desarrollado directrices para un internet más seguro, a fin de apoyar a la comunidad de líneas de ayuda telefónica para la infancia, a fin de que el niño que encuentre algún problema en línea pueda ser derivado a una línea de ayuda infantial en la que un consejero pueda brindarle el apoyo necesario.[13]

Cuando se trata de proteger los derechos de los niños en línea, tanto las empresas como las demás partes interesadas, deben lograr un delicado equilibrio entre el derecho a la protección de la infancia y el derecho al acceso a información y libertad de expresión de los niños. Por lo tanto, las empresas deben garantizar que las medidas de protección de la infancia en línea sean específicas y no indebidamente restrictivas para el niño ni para otros usuarios. Las Directrices de la UIT y UNICEF para la Industria sobre Protección de la Infancia en Línea describen las medidas que se pueden tomar para ayudar a proteger y promover los derechos de los niños en el mundo digital.[14]

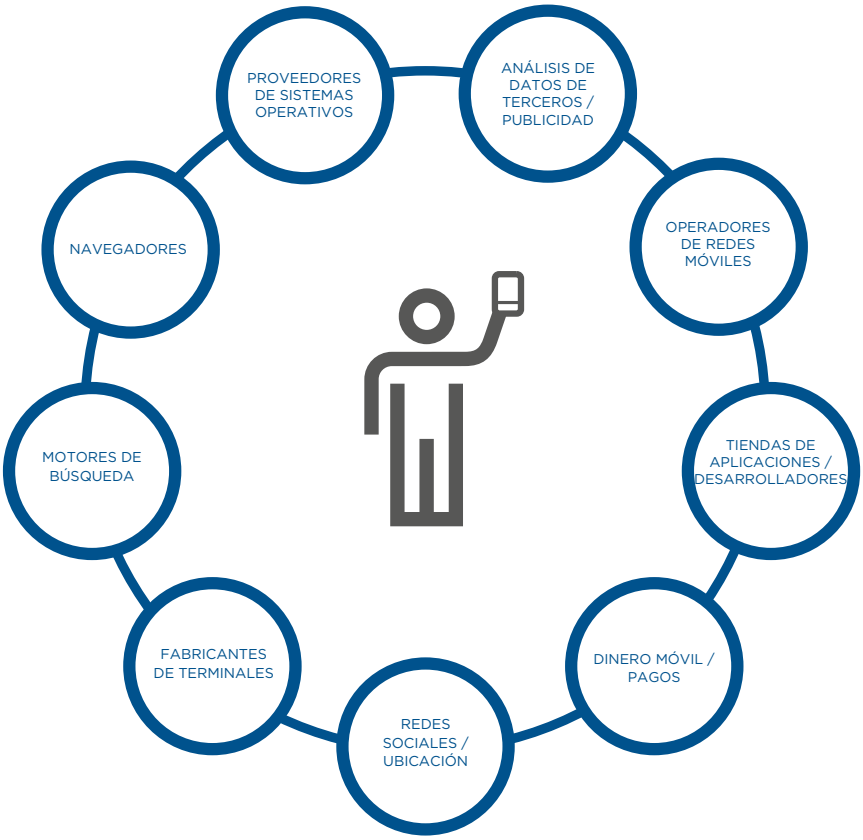
La rápida evolución del ecosistema móvil agrega complejidad a este entorno. El modelo en el cual el operador era responsable por el contenido de sus servicios ha evolucionado; en la actualidad, los usuarios cuentan con diversos medios para acceder a la gran variedad de contenido digital a través de sus dispositivos móviles. Como ilustra la Figura 3, muchos actores desempeñan un papel clave en la entrega de esta capacidad, incluidos los operadores de redes móviles.

Las distinciones tradicionales entre las diferentes partes del sector de las telecomunicaciones y las compañías de radiodifusión y de internet están rápidamente

12. La misión del programa mYouth de la GSMA es promover el uso positivo, seguro y responsable de los servicios móviles por parte de los jóvenes. Esta iniciativa de múltiples interesados incluye asociaciones con Child Helpline International y UNICEF. Para más información, consultar: http://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/myouth
13. Para ver las directrices, consultar: http://www.childhelplineinternational.org/resources/manuals-toolkits/internet-safety-guides/
14. UIT y UNICEF, 2014. "Directrices de protección de la infancia en línea para la Industria"

Figura 3

El ecosistema móvil



desapareciendo o volviéndose irrelevantes. El gobierno, el sector privado, los formuladores de políticas, los docentes, la sociedad civil y los padres desempeñan un papel esencial en estimular el uso más seguro de los servicios móviles por parte de niños y jóvenes.[15] La cooperación y la asociación entre estas partes son la clave para establecer las bases para un uso más seguro del internet y de las tecnologías asociadas.

La GSMA desempeña un rol protagónico en las iniciativas de autorregulación de la industria móvil y sus aportes a las "Directrices de protección de la infancia en línea para la industria" de la UIT y UNICEF han sido fundamentales. La GSMA trabaja en forma proactiva con gobiernos y reguladores, formuladores de políticas, organismos de seguridad y la industria para facilitar el desarrollo de estrategias colaborativas destinadas a promover el uso seguro y responsable de internet.

15. ITU y UNICEF, 2014. "Guidelines for Industry on Child Online Protection"

Cavando hondo

Directrices de protección de la infancia en línea para la Industria - UIT y UNICEF

El objetivo de las "Directrices de protección de la infancia en línea para la Industria" es sentar las bases para un uso más seguro de los servicios basados en internet y las tecnologías asociadas para los niños de hoy y de las futuras generaciones.

Estas directrices son el resultado del diálogo con miembros de la Iniciativa de Protección de la Infancia en Línea, y de una consulta más amplia y abierta que invitó a los miembros de la sociedad civil, las empresas, la academia, los gobiernos, los medios, las organizaciones internacionales y los jóvenes, a presentar sus comentarios a dichas directrices.

La cooperación y las alianzas son clave para establecer los fundamentos de un uso más seguro de internet y tecnologías asociadas. El gobierno, el sector privado, los formuladores de políticas, los docentes, la sociedad civil, los padres y los encargados de cuidar a los niños, desempeñan un rol fundamental en alcanzar esta meta. Las iniciativas de autorregulación de la industria pueden actuar en cinco áreas fundamentales:

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

Estimular el uso seguro y responsable de la tecnología y los servicios móviles por parte de los niños

Si bien las leyes relativas al contenido ilegal varían sustancialmente de país en país, casi todo el mundo considera que el el material de explotación sexual infantil es ilegal. Sin lugar a dudas, es universal el consenso de que es inaceptable la explotación sexual de niños por parte de personas u organizaciones que consumen, distribuyen o lucran con este tipo de material.

Como se analizó anteriormente, combatir el uso indebido de la tecnología en relación con el material de explotación sexual infantil [child sexual abuse content o CSAC, por sus siglas en inglés] requiere que los gobiernos cuenten con la legislación apropiada, que los organismos de seguridad estén equipados y facultados para llevar a cabo investigaciones y que se implementen líneas nacionales de atención telefónica para denunciar los casos de explotación sexual infantil en línea. Tanto los proveedores de servicios de internet como los operadores de redes móviles pueden desempeñar un papel clave en la prevención de la revictimización de un niño que ha sufrido abuso sexual infantil a través de medidas enfocadas en la restricción del acceso a dicho material. Por ejemplo, el trabajo de los miembros de la "Alianza móvil contra contenidos de abuso sexual infantil" de la GSMA[16] es bloquear el uso de servicios móviles de personas u organizaciones que pretenden consumir o lucrar con material de explotación sexual infantil, mediante colaboración, intercambio de información y trabajo conjunto con las líneas nacionales de atención telefónica de denuncias en internet, implementación de procesos de 'notificación y retirada' y restricción del acceso a los URL o sitios web en los que una autoridad competente haya identificado la existencia de material de explotación sexual infantil. Es importante que sea una autoridad competente (como INTERPOL, una línea nacional de atención telefónica o un organismo de seguridad) la que determine qué URL o dominio debe ser bloqueado, para que así los operadores móviles solo deban consultar esta lista y asegurar la implementación de dicha restricción, sin necesidad de juzgar la legalidad del contenido en cuestión.

El compromiso de los miembros de la Alianza Móvil de la GSMA es monitorear las nuevas tendencias que afectan esta área e implementar respuestas adecuadas. Por ejemplo, la Alianza Móvil de la GSMA ya comenzó a trabajar con sus socios externos para entender, monitorear y, cuando corresponda, abordar, el potencial impacto de la encriptación en la restricción del acceso a material conocido de explotación sexual infantil.

16. Para más información sobre la Alianza Móvil, consultar: http://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

Análisis más profundo

Alianza móvil contra contenidos de abuso sexual infantil de la GSMA

La "Alianza móvil contra contenidos de abuso sexual infantil" (Alianza Móvil) fue fundada por un grupo internacional de operadores móviles, dentro de la GSMA, con el fin de trabajar conjuntamente en pos de evitar que diferentes personas y organizaciones utilicen el entorno móvil para consumir o lucrar con contenido de abuso sexual infantil.

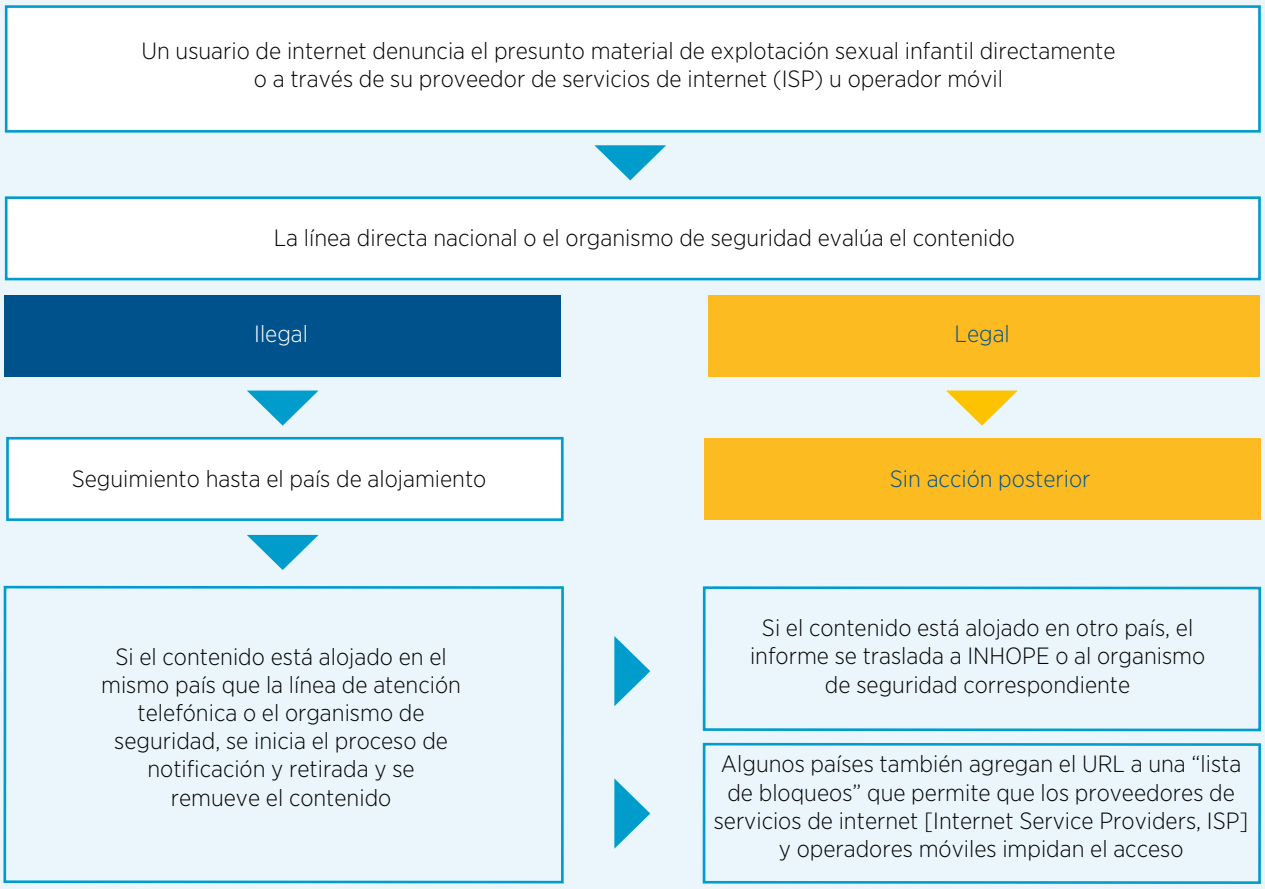
Los miembros de la Alianza se comprometieron a:

- **Implementar mecanismos técnicos para restringir el acceso a los URL o sitios web en los que un organismo competente e internacionalmente reconocido ha identificado que se aloja material de explotación sexual infantil**
- **Implementar procesos de 'notificación y retirada' para remover todo material de explotación sexual infantil publicado en sus propios servicios**
- **Apoyar y promover las líneas de atención telefónica como también otros mecanismos para que los consumidores denuncien todo material de explotación sexual infantil descubierto en internet o en los servicios de contenidos móviles**

A través de una combinación de medidas técnicas, cooperación e intercambio de información, la Alianza Móvil trabaja para detener y, en última instancia, revertir el aumento del material de explotación sexual infantil en línea en todo el mundo.

Además, la Alianza Móvil colabora con los esfuerzos más amplios de erradicar el contenido de abuso sexual infantil en línea publicando directrices y herramientas para uso de toda la industria móvil. Algunos ejemplos son la guía para establecer y administrar una línea de atención telefónica en colaboración con INHOPE, la organización que nuclea dichas entidades, y una guía para los procesos de Notificación y Retirada, en colaboración con UNICEF. La Alianza Móvil también coopera con la Coalición Financiera Europea [European Financial Coalition] y la Coalición Financiera contra la Pornografía Infantil [Financial Coalition Against Child Pornography].

Ejemplo de gestión de denuncia de explotación sexual infantil por una línea de atención telefónica y sus socios



Implicancias clave para los gobiernos, la industria y otros interesados relevantes

Los dispositivos y los servicios móviles mejoran la vida de los jóvenes. Todos los interesados deben adoptar, promover y entender mejor esta perspectiva para asegurar que los jóvenes aprovechen al máximo los beneficios que ofrece la tecnología móvil. La mejor forma de abordar la protección de la infancia en línea es a través del esfuerzo conjunto de las diversas partes para promover, en los niños y los jóvenes, el uso seguro y responsable de los servicios en línea y los dispositivos de internet, y empoderar a los padres y cuidadores para que participen en la protección de sus hijos en el mundo digital y colaboren con la misma.[17]

3

Asimismo, el conjunto completo de respuestas para afrontar y combatir el material de explotación sexual infantil incluye legislación, líneas de atención telefónica de denuncias, compromiso de los organismos de seguridad, apoyo a las víctimas, además de las medidas y procesos técnicos necesarios para sustentar estos servicios. Si bien los operadores móviles desean desempeñar un papel protagónico en ayudar a enfrentar este problema, tal como lo han hecho, por ejemplo, a través de la Alianza Móvil, necesitan el apoyo, liderazgo y el compromiso de todos los demás organismos y agencias relevantes para tener un impacto real.

La industria móvil repudia el uso indebido de sus servicios para la distribución de material de explotación sexual infantil.

- La "Alianza móvil contra contenidos de abuso sexual infantil" de la GSMA ofrece liderazgo en este ámbito y trabaja en forma proactiva para combatir el uso indebido de las redes y los servicios móviles por parte de criminales que pretenden tener acceso o distribuir contenido de abuso sexual infantil[18]
- Los operadores de redes móviles utilizan términos y condiciones, procesos de "notificación y retirada" (*notice & take-down*) y mecanismos de denuncia para mantener a sus servicios libres de este tipo de contenido[19]
- La industria móvil se compromete a trabajar con los organismos de seguridad y las autoridades correspondientes para facilitar la inmediata eliminación o deshabilitación de toda instancia de contenido ilegal cuyo alojamiento en un servicio móvil haya sido confirmado,[20] incluído todo material de explotación sexual infantil

La actitud de los gobiernos nacionales debe ser abierta y transparente respecto del contenido ilegal que existe en su país, antes de trasladar la responsabilidad de la aplicación de la ley a las líneas de atención telefónica, los organismos de seguridad y la industria, sujeto al proceso legal correspondiente.[21] No obstante, estas iniciativas proactivas no deben extenderse a acciones que estén en violación de los tratados internacionales de derechos humanos o a 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 comprometerse con iniciativas tales como la Alianza Mundial WePROTECT y consultar su marco nacional de respuestas modelo como herramienta útil para orientar su lucha contra el material de explotación sexual infantil en línea.[22]

17. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicaciones Móviles: Los niños y la tecnología móvil"
18. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicaciones Móviles: Contenido ilegal"
19. Ibídem.
20. Ibídem.
21. Ibídem.
22. Para más información, consultar: http://www.weprotect.org/the-model-national-response/

Dispositivos robados y falsificados

Robo y comercialización de dispositivos móviles

Desafortunadamente, los dispositivos móviles tienen un atractivo especial para los delincuentes dado que son pequeños, portátiles, de alto valor y contienen información importante. En consecuencia, se ha creado un mercado negro internacional de dispositivos móviles robados. En muchos países, los formuladores de políticas están cada vez más preocupados por los casos de robo de dispositivos móviles, así como por la participación del crimen organizado en la exportación y comercialización por volumen de los dispositivos móviles robados.

Barreras contra el robo y la comercialización de dispositivos móviles

La GSMA asigna un identificador único, conocido como el International Mobile Equipment Identifiers (IMEI) [identificador internacional de equipo móvil] a los fabricantes cuyos dispositivos se fabrican conforme al Proyecto de Asociación de Tercera Generación [3rd Generation Partnership Project o 3GPP, por sus siglas en inglés][23]. En su Base de Datos de IMEI, la GSMA registra los rangos asignados y toda la información relacionada con el modelo del dispositivo al cual fue asignado, incluidos el nombre del fabricante y del modelo del dispositivo, como también las principales funcionalidades de red (por ejemplo, bandas de frecuencia, interfaces de radio y tipos de dispositivos).

En 1996, la GSMA lanzó una iniciativa cuyo objetivo es bloquear todo dispositivo móvil robado denunciado como perdido o robado por el usuario ante un operador miembro de la GSMA, mediante el intercambio de información a través de una base de datos que contiene los identificadores únicos de dichos dispositivos móviles. Todos los miembros de la GSMA conectados a la Base de Datos de IMEI para compartir información sobre dispositivos robados tienen acceso a esa lista central, comúnmente conocida como la "lista negra". Cuando los operadores de redes móviles detectan que un dispositivo registrado en la lista negra se conecta a su red, pueden bloquear su uso.

Cuando un ladrón se da cuenta de que la probabilidad de que un consumidor compre un dispositivo robado es baja, dado que posiblemente haya quedado deshabilitado inmediatamente después de haber sido extraído, el robo de dispositivos perderá su atractivo. En este sentido, la GSMA alienta a sus miembros a implementar, sobre la base de ciertos estándares, un Registro de Identidad de Equipos [Equipment Identity Register, EIR] en sus redes para bloquear la conexión de todo dispositivo robado en base al identificador IMEI. Si bien el bloqueo de IMEI en base a la lista negra tuvo un impacto positivo en muchos países, para que una campaña antirrobo sea totalmente efectiva se deben implementar otras medidas adicionales. El robo y la venta de dispositivos es un problema internacional. Aun cuando todos los operadores de redes móviles de una región bloqueen un IMEI, el dispositivo móvil puede ser utilizado en cualquier otra región en la que los operadores de redes móviles no estén conectados a la Base de Datos de IMEI de la GSMA.

Los esfuerzos de la GSMA se han concentrado en conectar la mayor cantidad de operadores de redes móviles posible a la Base de Datos de IMEI. Hasta fines de 2016, la lista negra de la Base de Datos de la GSMA era utilizada por más de 140 operadores de redes móviles en más de 40 países del mundo para compartir diariamente información sobre dispositivos robados. En América Latina, donde la incidencia de este problema es altísima, son 18 los países conectados a la Base de Datos de IMEI, con la participación activa de la mayoría de los operadores de redes móviles de la región. A fin de empoderar y ayudar aún más al consumidor y los negocios minoristas, en algunos mercados se encuentra disponible un servicio público de Verificación de IMEI de Dispositivos que permite verificar el estado del dispositivo que se encuentra a la venta. Estos servicios se implementaron como parte de la campaña "Nos Importa",[24] a cargo de la GSMA, con más de 1,5 millones de búsquedas realizadas hacia fines de 2016.

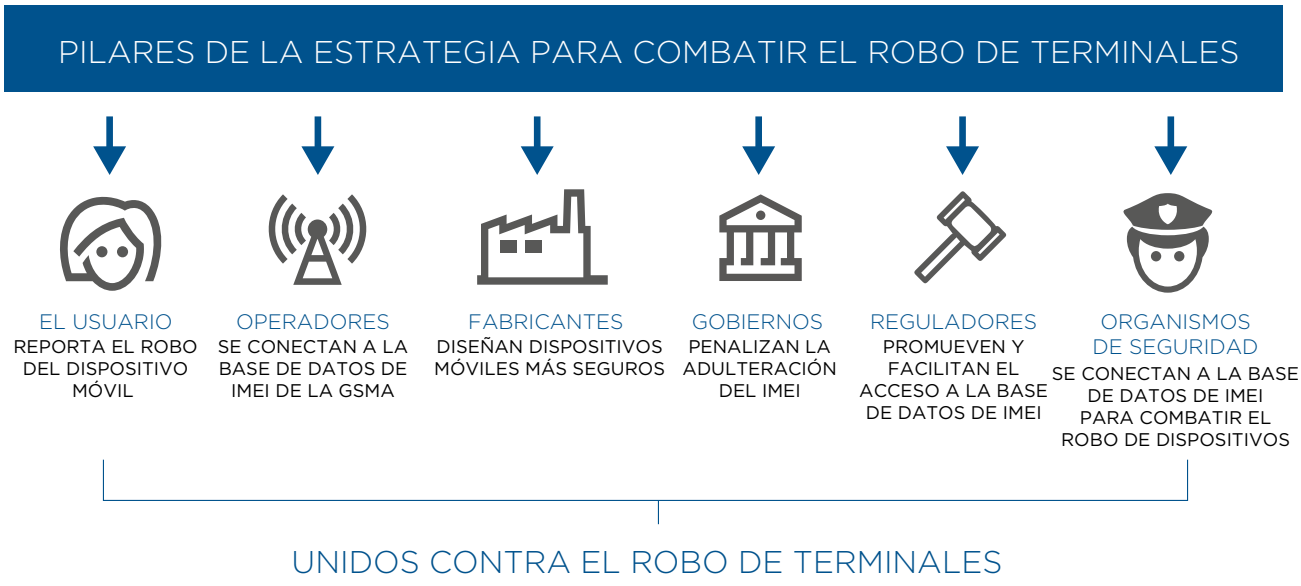
23. 3GPP nuclea a siete organizaciones de desarrollo de estándares de telecomunicaciones (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). Las especificaciones del 3GPP se publican, en forma gratuita, hasta cuatro veces al año. El término "especificación del 3GPP" abarca todas las especificaciones de GSM (incluyendo GPRS y EDGE), W-CDMA (incluyendo HSPA) y LTE (incluyendo LTE-Advanced y LTE-Advanced Pro). Para más información, consultar: www.3gpp.org
24. Para más información sobre la campaña "Nos Importa", consultar: http://www.gsma.com/latinamerica/es/nosimporta

El éxito del bloqueo en base al IMEI depende de la implementación segura por parte de los fabricantes de dicho IMEI en cada dispositivo móvil. Los fabricantes de dispositivos móviles líderes a nivel mundial han aceptado apoyar las dos iniciativas clave de la GSMA para fortalecer la seguridad de los IMEI, incluyendo la definición de principios de diseño técnico para la implementación de seguridad en los IMEI y la participación en el Procedimiento de Denuncia y Corrección de Vulnerabilidades de la Seguridad del IMEI [IMEI Security Weakness Reporting and Correction Process] de la GSMA.[25] Algunos fabricantes de dispositivos podrían implementar medidas adicionales para mejorar los niveles de seguridad relativos a la integridad del IMEI, un elemento esencial para el bloqueo efectivo de los dispositivos. Los operadores de redes móviles, como también otros grandes proveedores y negocios minoristas de venta de dispositivos móviles, pueden tomar decisiones de compra informadas al seleccionar los dispositivos que venderán a sus consumidores, si toman en consideración la seguridad de la implementación del IMEI y la conformidad con los principios técnicos de diseño de los dispositivos. Es importante que todos los interesados –fabricantes, operadores de redes móviles, gobiernos y consumidores– colaboren en garantizar la total integridad del IMEI y la inmediata corrección de cualquier problema que surja. Asimismo, los gobiernos deben reconocer el rol central de la integridad del IMEI en el bloqueo de dispositivos robados y penalizar el cambio no autorizado del IMEI de un dispositivo móvil (también denominado reprogramación o adulteración de IMEI). En algunos países, este cambio realizado luego de su fabricación es un delito penal. Se exhorta a los demás países a hacer lo propio e identificar y procesar en forma proactiva a los delincuentes a fin de desalentar la evasión de los controles de seguridad.

Una forma de impedir el robo de dispositivos móviles es el "*kill switch*" [Interruptor de desactivación]. Un *kill switch* es una forma de deshabilitar las funcionalidades esenciales de un dispositivo móvil. Básicamente, esta funcionalidad es parte del sistema operativo del dispositivo móvil, y, una vez activada, el dispositivo deja de funcionar y solo podrá ser reactivado o utilizado nuevamente si el dueño legítimo autoriza dicha reactivación. La GSMA desarrolló el documento de "Requisitos de funciones antirrobo para dispositivos" [Anti-Theft Device Feature Requirements] para los fabricantes de dispositivos, operadores de redes móviles y gobiernos, en el que define el conjunto de funcionalidades que el dueño de un dispositivo puede invocar para localizar, deshabilitar y volver a habilitar su dispositivo en caso de extravío, pérdida o robo.[26]

Figura 4

Pilares de la estrategia para combatir el robo de terminales



25. Para información sobre el Proceso de Denuncia y Corrección de Debilidades de Seguridad, consultar: http://www.gsma.com/publicpolicy/wp-content/uploads/2007/07/IMEI-Weakness-Reporting-and-Correction-Process-3.2.0.pdf
26. GSMA, 2016. "Anti-Theft Device Feature Requirements, Version 3.0"

Implicancias clave para el gobierno, la industria y otros interesados relevantes

La GSMA desea ayudar a todo interesado externo a restringir la venta y el uso de dispositivos robados o perdidos. La GSMA y sus miembros pueden ofrecer conocimientos técnicos y recursos, tanto a los gobiernos como a cualquier otro interesado que quiera desarrollar, en forma colaborativa, soluciones locales relevantes, enfocadas en el consumidor. Por ejemplo, la GSMA sugiere lo siguiente:

- Un enfoque colaborativo entre los principales interesados es esencial:[27]
  - El usuario puede denunciar el robo de su dispositivo ante su operador móvil, habilitar la funcionalidad antirrobo en su dispositivo y, en aquellos países donde los operadores están conectados a la Base de Datos de IMEI, utilizar el IMEI para verificar el estado del dispositivo que planea comprar
  - Los operadores de redes móviles pueden bloquear el uso de dispositivos robados en sus redes, conectarse a la base de datos de IMEI de la GSMA para intercambiar la información de la lista negra y alentar a sus proveedores de dispositivos a proteger correctamente la integridad de la implementación del IMEI en sus productos
  - Los fabricantes de dispositivos pueden diseñar dispositivos más seguros (es decir, hacer que la reprogramación del IMEI sea imposible) e implementar la funcionalidad de *kill switch* para que el usuario pueda deshabilitar el dispositivo perdido o robado en forma remota
  - Los operadores de tiendas de aplicaciones pueden obtener los IMEI de los dispositivos robados de la GSMA y utilizarlos para denegar el acceso de los dispositivos denunciados como robados a sus tiendas
  - Los gobiernos pueden introducir legislación para penalizar la reprogramación no autorizada de un IMEI y, además, apoyar los esfuerzos de la industria y los organismos de seguridad en la lucha contra el robo de dispositivos
  - Los reguladores pueden alentar a las redes locales a conectarse a la Base de Datos de IMEI de la GSMA para compartir información sobre dispositivos robados, proporcionar y/o facilitar la provisión de servicios de verificación de IMEI para que el usuario pueda constatar el estado del dispositivo antes de comprarlo y, en general, ofrecer un entorno regulatorio favorable para la implementación de soluciones efectivas y fáciles para el consumidor, a fin de combatir el robo de dispositivos
  - Los organismos de seguridad pueden procurar tener la capacidad de verificar el estado de los dispositivos mediante la obtención del acceso gratuito a la información sobre dispositivos robados de la GSMA y concentrar su atención y recursos en el robo de dispositivos, garantizando así la identificación y procesamiento de los criminales
- Es importante evitar soluciones que quizás sean menos efectivas y/o incluso tengan consecuencias negativas no deseadas:
  - Las listas negras son la solución óptima para prevenir el uso a nivel de red de los dispositivos perdidos o robados. Se debe evitar el uso de listas blancas para estos fines, ya que fueron diseñadas para otros propósitos, como, por ejemplo, ayudar a combatir los dispositivos falsificados, aunque la efectividad de este método aún no ha quedado demostrada
  - Exigir el uso de soluciones no estándares para combatir el robo de dispositivos móviles, dado que las soluciones propietarias son costosas y difíciles de implementar a nivel técnico
  - Métodos contrarios a los estándares móviles mundiales, como, por ejemplo, la vinculación de un dispositivo específico a un usuario móvil específico, dado que el cumplimiento por parte de los usuarios y los proveedores de servicios tiende a ser difícil y oneroso –y, en algunos casos, hasta desproporcionado- y pueden plantear una serie de complejos problemas legales y restrictivos de la competencia
  - El desarrollo de una base de datos nacional de identificadores de dispositivos representa gastos y esfuerzos innecesarios. La base de datos de IMEI de la GSMA, que ya existe, puede satisfacer toda necesidad de bloqueo e intercambio de información de dispositivos. Asimismo, es preferible mantener un único repositorio global de datos sobre dispositivos para garantizar la consistencia y el intercambio más amplio de información más amplio, al tiempo que se evita la fragmentación, la cual tiene un impacto en la eficacia de cualquier solución

27. GSMA, 2016. "La Economía Móvil: América Latina y Caribe 2016"

Caso de ejemplo

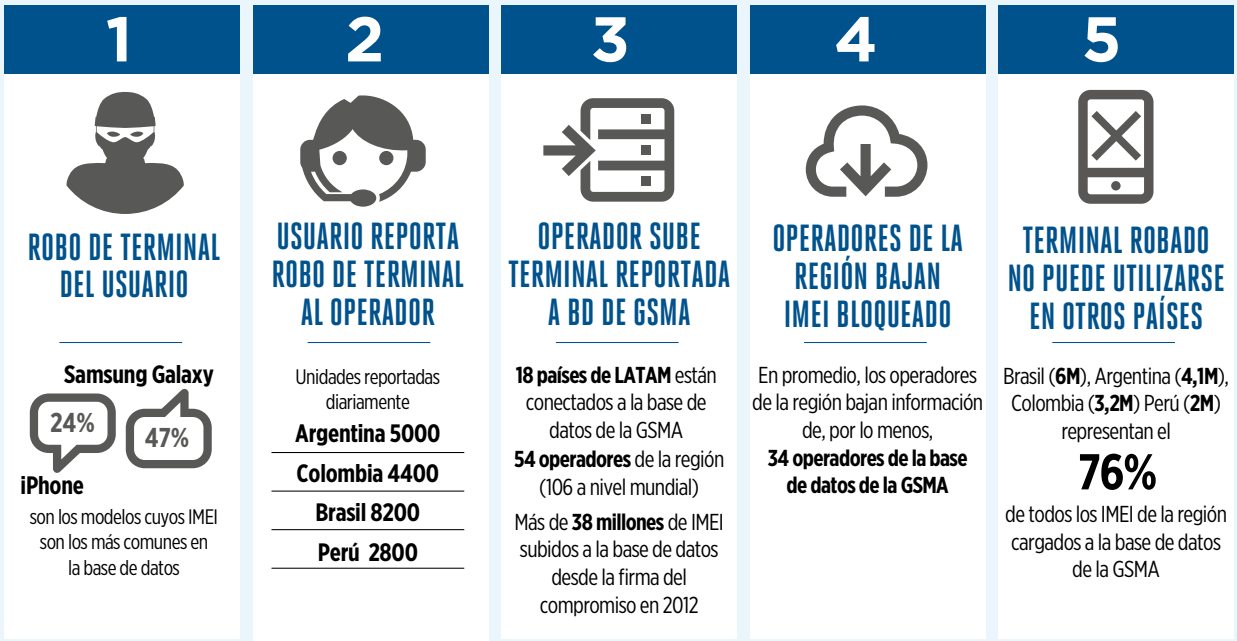
Aporte de la industria a la lucha contra el robo de dispositivos en América Latina

En los últimos años, el aumento en el robo de dispositivos ha sido significativo dado el crecimiento en la adopción de teléfonos móviles y, en especial, de *smartphones*. El robo de dispositivos está aumentando vertiginosamente en América Latina. Por ejemplo, durante el primer trimestre de 2014, las denuncias de robo ascendieron a 1,2 millones de teléfonos móviles en Perú, un incremento de 34% respecto del mismo período en el año 2013. Si bien no todos los incidentes fueron reportados, en 2014 había 14 millones de teléfonos móviles registrados como robados en la Base de Datos de IMEI solo en los países andinos: Ecuador, Colombia, Perú y Bolivia.

En muchos casos, los teléfonos móviles robados cruzan las fronteras para aprovechar las oportunidades de arbitraje de precios y/o encontrar alternativas para eludir las iniciativas del país en el que se realizó el robo destinadas a bloquear los dispositivos utilizando el IMEI. Por lo tanto, para verdaderamente combatir este problema, es vital que la información sea compartida entre los operadores de un mismo país y que también sea posible hacerlo a nivel regional y mundial.

En 2011, la Comisión Interamericana de Telecomunicaciones (CITEL) aprobó una resolución que, entre otras propuestas, recomendaba: 'Reglamentar a nivel regional el intercambio de bases de datos de listas negras y el bloqueo de los códigos de identificación únicos (IMEI) para prevenir la activación y el uso de teléfonos celulares robados en otros mercados y contribuir a controlar el tráfico ilegal de dispositivos entre los países de la región'. En 2012, trece operadores de redes móviles latinoamericanos, miembros de la GSMA, se comprometieron a trabajar juntos y a colaborar con los gobiernos de toda la región en el bloqueo del uso de dispositivos robados. Esta iniciativa voluntaria permite el intercambio de información sobre dispositivos móviles robados para poder proceder a su bloqueo y crea mayores obstáculos para el tráfico y la reutilización de los mismos en toda la región.

La GSMA continúa trabajando y promoviendo la adopción de estas directrices por parte de todas las compañías miembro de la GSMA en América Latina mediante la firma de memorandos de entendimiento entre los operadores en cada país, con el objetivo de garantizar el intercambio de la totalidad de la información a lo largo de la región.



Venta y uso de dispositivos falsificados

Un dispositivo móvil falsificado infringe expresamente la marca comercial o diseño de un producto "de marca" original o auténtico, aunque haya una mínima variación en el nombre comercial. Por su carácter de ilegales, estos dispositivos móviles generalmente son despachados y vendidos por las redes del crimen organizado en los mercados negros de todo el mundo. Es por eso que la sensibilización de consumidores y gobiernos sobre la verdadera escala e impacto de la comercialización de estos dispositivos móviles falsificados, es limitada. Se estima que, en 2013, se vendieron 143 millones de dispositivos móviles ilegales en todo el mundo.[28]

Si bien la producción y distribución de artículos falsificados es un problema grave que viola las normas de propiedad intelectual y del comercio legítimo, dada la consiguiente pérdida de ingresos por ventas de los fabricantes y de ingresos fiscales de los gobiernos, los dispositivos falsificados también afectan al consumidor. 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 que está frecuentemente asociada al funcionamiento y uso de dispositivos falsificados, se ha reportado que muchos de estos dispositivos contienen materiales peligrosos para el medio ambiente. Varios estudios han demostrado la presencia de materiales peligrosos en algunos dispositivos falsificados, como plomo en las soldaduras de las juntas, en niveles superiores a los límites permitidos a nivel mundial,[29] definidos en las reglamentaciones con las que cumplen los dispositivos móviles de fabricación legítima. Asimismo, estos dispositivos móviles falsificados plantean una amenaza para el medio ambiente si su eliminación no se realiza en base a procedimientos idóneos a nivel ambiental.

No es fácil identificar y bloquear los dispositivos móviles falsificados porque muchos tienen un IMEI que parece legítimo. Hoy en día es común que los falsificadores pirateen rangos de números de IMEI asignados a fabricantes de dispositivos legítimos para utilizarlos en sus productos, dificultando aún más la diferenciación entre los productos legítimos y los falsificados.

28. The Mobile Manufacturers Forum (MMF), 2014. "Teléfonos móviles falsificados/subestándar: guía de recursos para los gobiernos"
29. Ibídem.

Restricción de la venta y uso de dispositivos falsificados

Para ayudar a resolver este problema, se pueden utilizar las listas blancas (un registro de los rangos de números de identificación asignados a todos los fabricantes de dispositivos legítimos) de la base de datos de IMEI administrada por la GSMA, para detectar aquellos dispositivos que contienen un IMEI inválido o inexistente y, si fuese necesario, denegarle el acceso a la red. No obstante, no es fácil diferenciar y separar al dispositivo legítimo del falsificado en los casos en que el IMEI fue asignado a un dispositivo legítimo pero es utilizado en un producto falsificado. 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 que comercializa productos falsificados. Estas medidas no deberían causar un 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 apuntar, específicamente, a la fabricación y distribución de dispositivos falsificados para sacarlos de circulación antes de que lleguen a un consumidor desprevenido.

En septiembre de 2016, la GSMA y la Organización Mundial de Aduanas (OMA) celebraron una alianza para colaborar en la lucha contra la falsificación y el comercio fraudulento de dispositivos móviles. La integración con la Base de Datos de IMEI permitirá la verificación cruzada y el filtrado de los dispositivos identificados como falsificados, en base al IMEI, en el punto de importación. Sin embargo, esta solución no se puede aplicar a los dispositivos móviles que se trafican e importan fuera del proceso aduanero como contrabando: en este caso, la aduana y los organismos de seguridad deben concentrarse en combatir el tráfico ilegal.

Debido a la complejidad de este asunto, los esfuerzos de los organismos de seguridad para combatir la distribución y venta de dispositivos falsificados no han sido suficientes para contener el problema. El alcance de la legislación y las reglamentaciones nacionales vigentes es limitado porque la distribución de dispositivos falsificados es, por lo general, internacional y los esfuerzos para imponer restricciones en países específicos son fáciles de evadir. Asimismo, la creación de listas blancas nacionales de dispositivos constituye una estrategia que aún no ha sido comprobada y no existe evidencia alguna que respalde su eficacia en la lucha contra la venta y el uso de dispositivos falsificados. Esta estrategia podría resultar en un obstáculo para la libre circulación de dispositivos móviles en el mundo y, en algunos países, sería considerada ilegal. Por el contrario, se deben desarrollar soluciones globales con la participación de los múltiples interesados, tal como se describe en la próxima sección.

Implicancias clave para el gobierno, la industria y otros interesados relevantes

La GSMA reconoce los problemas que la falsificación de terminales plantea para los usuarios, las redes, los fabricantes legítimos y los gobiernos, y apoya la necesidad de mantener la integridad del mercado de dispositivos móviles. La GSMA está dispuesta a trabajar con sus miembros, los gobiernos y otros interesados para desarrollar soluciones efectivas a fin de combatir la fabricación y oferta de dispositivos falsificados.

- La colaboración entre todas las partes interesadas es esencial:
  - Los reguladores pueden trabajar con los fabricantes de dispositivos y los operadores de redes locales para entender el nivel de utilización de dispositivos falsificados en el mercado local y, en consulta con los mismos, desarrollar y acordar las medidas que se deberían tomar para no penalizar a los fabricantes de dispositivos legítimos ni a los usuarios inocentes que fueron víctimas de los falsificadores
  - Los gobiernos pueden ayudar a desbaratar el mercado negro de dispositivos mediante la reducción de aranceles y derechos aduaneros sobre dispositivos legítimos importados, lo cual reducirá el costo de propiedad del dispositivo legítimo. Asimismo, pueden apoyar los programas de información y educación del consumidor para destacar los riesgos que conlleva comprar un dispositivo falsificado
  - Las agencias aduaneras pueden asegurarse de que tienen la capacidad de verificar si los dispositivos contienen identificadores legítimos en el punto de importación mediante la obtención de acceso gratuito a la información de IMEI de la GSMA. Asimismo, pueden concentrar su atención y recursos en la identificación y procesamiento de los delincuentes
  - Los fabricantes de dispositivos pueden trabajar con el gobierno, los reguladores y las agencias aduaneras en contribuir a la educación de todos los interesados sobre dispositivos falsificados y ofrecer inteligencia sobre las actividades relacionadas con la fabricación, distribución y venta de dispositivos falsificados a las autoridades correspondientes
  - Los operadores de redes móviles pueden conectarse a la Base de Datos de IMEI de la GSMA para tener acceso a 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 planea comprar a través del servicio de verificación prestado por terceros, cuando está disponible
- Es importante evitar soluciones que quizás sean menos efectivas y/o incluso tengan consecuencias negativas no deseadas:
  - Se debe evitar exigir el uso de soluciones que no estén basadas en estándares para combatir los dispositivos móviles falsificados, dado su carácter de tecnología propietaria y porque su implementación es, por lo general, costosa y difícil a nivel técnico

    No se deben promover métodos contrarios a los estándares móviles mundiales, como, por ejemplo, la vinculación de un dispositivo específico a un usuario móvil específico, porque cumplir con estos requerimientos tiende a ser difícil y oneroso –y, en algunos casos, hasta desproporcionado- tanto para los usuarios como para los proveedores de servicios, y pueden plantear una serie de complejos problemas legales que pueden redundar en la limitación de la competencia

Fraude con dispositivos móviles

El fraude puede tomar muchas formas, algunas de las cuales utilizan a los dispositivos móviles como canal. Entre ellas, cabe mencionar ataques tales como el fraude de servicios (por ejemplo, fraude de identidad o de dinero móvil), el *spam* móvil[30] y, cada vez más, el fraude por "ingeniería social" (por ejemplo, *Phishing*, *SMiShing* o *Vishing*),[31] en base a los cuales 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 en peligro

El fraude por ingeniería social recurre a la manipulación para incitar a las personas a tomar medidas peligrosas, tales como divulgar información personal o contraseñas. Una vez que tienen acceso a dicha información privada, los delincuentes pueden registrarla y utilizarla para cometer otros delitos asociados al fraude, tales como el robo de identidad y el fraude bancario. En general, los estafadores que interactúan con sus potenciales víctimas desarrollan una relación de empatía y confianza, muchas veces aprovechando la información disponible públicamente.

El fraude por ingeniería social está en aumento y la organización internacional de policía criminal, INTERPOL, lo identificó como una de las tendencias emergentes de fraude a nivel mundial. Por ejemplo, en el Reino Unido, las cifras registradas por la Dirección Nacional de Inteligencia sobre el Fraude [National Fraud Intelligence Bureau] muestran un aumento de 21% en los incidentes denunciados durante los 12 meses entre octubre de 2014 y octubre de 2015.

Afrontar y minimizar el fraude

Los defraudadores tienen éxito cuando logran convencer a su víctima de que son legítimos, ya sea en persona o a través de un servicio o sitio web. Las soluciones tecnológicas ofrecen cierta defensa, como, por ejemplo, la adopción por parte de los operadores de redes móviles de las técnicas recomendadas por la GSMA para detectar y manejar la transmisión internacional de spam móvil fraudulento.

Si bien no era muy común, en el pasado, los sistemas de correo de voz fueron objeto de ataques destinados a poner en riesgo la seguridad del usuario móvil al permitir que terceros no autorizados escucharan los mensajes o realizaran llamadas fraudulentas. Dado que los sistemas de correo de voz pueden ser utilizados como un medio 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 las cuentas de correo de voz, garantizando que solo el usuario legítimo tenga acceso a los servicios correspondientes, de manera tal que se alcance un equilibrio entre la usabilidad y la seguridad del mismo. No obstante, dado que el comportamiento humano es también un elemento central del fraude móvil, la educación sobre cómo proteger la información personal y la concientización sobre las potenciales amenazas, son herramientas fundamentales para minimizar el riesgo. Los operadores de redes móviles están en una posición privilegiada para ayudar a educar a los consumidores sobre la necesidad de mantenerse alertas y atentos. Sin embargo, el proveedor final del servicio, como, por ejemplo, bancos y negocios minoristas, quien está en aún mejor posición para ofrecer y exigir el cumplimiento de las medidas técnicas de seguridad particulares relacionadas con su propio servicio, debe reforzar los mensajes más detallados.

Para apoyar a los operadores móviles en esta tarea, la GSMA recomienda tres principios rectores[32] para la elaboración de mensajes para el consumidor sobre este tema:

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

Fraude por ingeniería social: ejemplos

- ***Phishing –*** método utilizado para infectar una computadora o un dispositivo móvil con el objeto de obtener acceso a valiosa información personal. Estos defraudadores utilizan las comunicaciones, como el correo electrónico, para incitar a las personas a entrar a sitios web o servicios que aparentemente son auténticos para extraer su información personal.
- ***SMiShing –*** o 'SMS *phishing*' es el uso de mensajes de texto para presentar un "señuelo" que luego conduce a las personas a divulgar su información personal.
- ***Vishing –*** cuando los defraudadores persuaden a las víctimas a suministrar información personal o transferir dinero, por teléfono, haciéndose pasar por un servicio legítimo como puede ser un banco.

30. '*Spam* Móvil' se refiere a mensajes móviles masivos no solicitados. La mayor parte del *spam* está destinado a estafar o engañar al receptor y depende del modelo de cobro implementado (es decir, barrera baja para el emisor si se cobra al receptor)
31. Ver barra lateral sobre Ingeniería Social
32. L. Gilman, 2012. "Mitigating the risk of fraud through consumer communication", GSMA

Implicancias clave para el gobierno, la industria y otros interesados relevantes

El fraude, en todas sus formas, es un problema de alta complejidad y, en la mayoría de los casos, es considerado ilegal en gran parte de los países. Las acciones de los operadores móviles solo pueden influir en el comportamiento de los consumidores con el objeto de mitigar el riesgo de fraude a través de la prevención. La legislación y la regulación deberían enfocarse en los autores del delito. La educación y la concientización deben ser los principales medios para promover la capacidad de autoprotección del consumidor. Especialmente en aquellos mercados en los que el nivel de comprensión tecnológica es bajo, los consumidores a menudo no aprovechan al máximo el potencial de las funcionalidades que ofrece la tecnología para su protección.

- Es importante que el proveedor del servicio final (por ejemplo, los bancos en el caso de los servicios financieros) implemente el más alto nivel de seguridad posible, correspondiente a su mercado
- Se deben utilizar y promover controles preventivos, tales como campañas de concientización del consumidor, destinadas a mejorar su conocimiento y protección, a fin de ayudarlos a minimizar su exposición al fraude
- Los operadores de redes móviles deben elaborar estrategias robustas de gestión de riesgos para mitigar la amenaza de fraude. Los tipos de medidas a tomarse y el nivel de implementación serán determinados por la evaluación realizada por cada operador y serán específicos para los servicios que ofrece y los consumidores en sus mercados

Estudio de caso

Gestión de riesgo de dinero móvil: comunicación con el consumidor

El caso del servicio M-PESA ofrecido por 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 principales prioridades del servicio M-PESA de Safaricom es mitigar la amenaza de estafas al consumidor. Además de las medidas reactivas, y en lugar de intentar usar solo controles de detección (es decir, monitorear y reportar tendencias a posteriori), Safaricom depende en gran medida del control preventivo para reducir el riesgo de dichas estafas. Safaricom encontró que el control preventivo más efectivo es la concientización del usuario a través de comunicaciones claras. Para llegar a los usuarios de M-PESA, Safaricom utiliza una estrategia multidimensional. Sus campañas de concientización del consumidor incluyen desde envíos de SMS masivos y anuncios por radio en dialectos locales hasta avisos en el periódico. Concientizar al consumidor a través de comunicaciones claras fue esencial para que Safaricom gestionara con éxito el fraude contra los consumidores de M-PESA.

La comunicación con el consumidor es una herramienta que se debe utilizar como parte de una estrategia de gestión de riesgos más amplia y que debe ser complementada con los datos y paneles de control correspondientes, además de los procedimientos internos establecidos. Por ejemplo, la GSMA desarrolló un marco integral de gestión de riesgo de dinero móvil y un kit de herramientas para operadores.

4 Protección de la privacidad del consumidor

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 mismas compañías de internet que los proveen tienen acceso a información vital sobre los usuarios, desde su identidad, con quién se comunican y su ubicación hasta datos sobre sus intereses personales, a través de los sitios y servicios a los cuales tienen acceso. Los proveedores pueden analizar las comunicaciones, como las palabras ingresadas en los motores de búsqueda o la ubicación ingresada en una aplicación de mapas, combinar todos estos conjuntos de datos e inferir intereses y objetivos.

El uso de datos personales por parte de los operadores para la provisión de los servicios de comunicaciones es limitado. Son otras compañías del ecosistema de internet las que utilizan la información personal en forma más intensa.[33]

Si bien los usuarios pueden no siempre advertirlo, muchos de los servicios en línea se ofrecen en forma gratuita a condición de que el proveedor pueda utilizar los datos personales para vender publicidad u ofrecer servicios pagos al usuario. Esta sección se enfoca en la recolección de datos del usuario en todo el ecosistema de internet y la forma en que son almacenados y utilizados, cómo es el acceso a los mismos, así como también las implicancias de privacidad asociadas.

Las áreas de análisis específicas son las siguientes:

- Recolección y uso de datos, con foco en el sustento de la innovación
- Elección del consumidor, con foco en la incorporación de la elección de servicios y aplicaciones en línea
- Flujo transfronterizo de datos, reconociendo la necesidad de considerar la seguridad nacional

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y los demás interesados. Más adelante, en este capítulo, se describen en forma detallada.

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 las reglamentaciones y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia a través de 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 responsables de gobierno digital que se encuentren alineadas con las reglamentaciones locales. 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 recolectan y cómo se utilizan, mediante la implementación de políticas tales como:

- **Almacenamiento y tratamiento seguro de toda información personal y privada, conforme a los requisitos legales, cuando corresponda**
- **Transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y el pleno cumplimiento con los requisitos legales**
- **La entrega de información y herramientas para que el consumidor pueda tomar decisiones simples y significativas sobre su privacidad**

33. Para un análisis más detallado de dichos servicios, consultar el documento de la GSMA, preparado en 2016 por A.T. Kearney, "The Internet Value Chain: A study on the economics of the internet", pág. 11

Recolección y uso de datos

La GSMA prevé que la cantidad de *smartphones* crecerá de 2600 millones a fines de 2015 a 5800 millones para el año 2020. Paralelamente, se espera que el tráfico de datos crezca a una tasa de crecimiento compuesto anual (*Compounded Annual Growth Rate* o *CAGR*, por sus siglas en inglés) de 49% durante el mismo período.[34] Esta proliferación de dispositivos y datos permite a personas, compañías y gobiernos innovar en formas novedosas e inesperadas.[35]

No obstante, mientras los consumidores utilizan cada vez más estos servicios, diversos estudios muestran que también están preocupados por su privacidad y buscan garantías de que pueden confiar su información a las compañías. Un estudio de la GSMA reveló que ocho de cada diez usuarios móviles siente preocupación respecto de compartir su información personal al utilizar el internet o las aplicaciones móviles. El estudio también planteó que casi la mitad de los usuarios móviles preocupados por la privacidad estaría dispuesto a limitar el uso de las aplicaciones si no se sintiera seguro de que su información personal se encuentra salvaguardada de mejor manera.[36]

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

- Las leyes sobre privacidad, cuando las hubiere, varían de una jurisdicción a otra y no existe un marco interoperable a nivel mundial. A menudo, las organizaciones regidas por estas leyes tienen presencia internacional, lo cual genera incertidumbre respecto de la base de referencia legal pertinente y plantea el interrogante sobre qué leyes deberían aplicarse respecto del uso de los datos, si las del país del usuario o las del país del proveedor de servicios. Esto puede complicarse aún más si el proveedor de servicios almacena y procesa los datos en un tercer país
- La segunda distinción tiene que ver con el operador de redes móviles y los servicios y aplicaciones en línea provistos por terceros, a los que los usuarios pueden acceder a través de la red móvil. La mayoría de los operadores móviles están sujetos a leyes y obligaciones establecidas en sus licencias relativas a la protección de la privacidad que no aplican a los demás servicios en línea del ecosistema de internet.

4

Terminología

Datos personales

Datos personales – pueden significar muchas cosas para muchas personas en el mundo en línea y existen diferentes significados definidos en las leyes. El objeto del presente documento no es reinterpretar la ley, pero, al utilizar el término 'datos personales', se pretende incluir, aunque sin carácter limitativo, la información relacionada con una persona física y que es:

- **Obtenida directamente del usuario (por ejemplo, ingresada por el usuario a través de la interfaz de usuario de una aplicación y que puede incluir nombre, domicilio y detalles sobre tarjetas de crédito)**
- **Recolectada en forma indirecta (por ejemplo, número de teléfono móvil, dirección de correo electrónico, nombre, género, datos de nacimiento, datos de ubicación, dirección IP, IMEI, identificación única del teléfono)**
- **Relativa a la conducta del usuario (por ejemplo, datos de ubicación, datos de uso de productos y servicios, visitas a sitios web)**
- **Generada por el usuario y mantenida en el dispositivo del usuario (por ejemplo, registros de llamadas, mensajes, imágenes generadas por el usuario, listas de contactos o libretas de direcciones, notas y credenciales de seguridad)**

Usuario – Cuando 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.

34. GSMA, 2016. "La economía móvil 2016"
35. Ibídem.
36. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers" [Privacidad móvil: conclusiones y consideraciones para formuladores de políticas sobre estudios sobre consumidores]

La falta de alineación entre las leyes de privacidad nacionales y/o del sector de mercado, sumado a los flujos de datos mundiales, hacen prácticamente imposible que todas las partes satisfagan las expectativas de privacidad del consumidor consistentemente. Probablemente, este entorno de aplicación irregular de las normas se vea exacerbado aún más a medida que aumenta la interconexión de dispositivos y sensores causada por el 'Internet de las Cosas' (*Internet of Things*, o IoT, por sus siglas en inglés)[37], dado que los servicios de IoT son, por lo general, globales e incluyen múltiples tipos de proveedores de servicios en diferentes sectores.

Esta falta de congruencia en los requerimientos de privacidad de los diferentes servicios y aplicaciones puede llevar a una situación en la que el usuario brinda fácil acceso a su información personal, en forma involuntaria, dejándolo expuesto a circunstancias que no quieren ni desean. Asimismo, algunas prácticas utilizadas por aplicaciones y servicios en línea llevan al consumidor a "aceptar" términos y condiciones relativos a la privacidad sin leer el aviso ni entender las implicancias de sus decisiones. Un estudio encargado por la GSMA muestra que el 82% de los usuarios acepta los avisos de privacidad sin leerlos porque son demasiado extensos o contienen demasiado lenguaje jurídico.[38] Dado que no está clara distinción entre el operador de redes móviles y los demás servicios a los que el usuario tiene acceso a través de su dispositivo móvil, existe también el riesgo de que no sepa quién está tratando sus datos y, en algunos casos, crea que su privacidad está mejor protegida que lo que en realidad está.

Análisis más profundo

Big Data

El aumento en la capacidad de la computación, la caída de los costos y los avances en el análisis, aprendizaje automático y disciplinas asociadas, permite procesar y analizar enormes volúmenes de datos. De esta forma, se puede extraer importante información, cuando proceda, de meras correlaciones de datos en lugar de tener que identificar conexiones causales. Por lo general, estas capacidades son llamadas técnicas de análisis de *big data* y 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 acuciantes de nuestro tiempo, desde la administración vial en áreas urbanas congestionadas y contaminadas hasta comprender y prevenir la propagación de enfermedades.

Cada vez más, los operadores móviles utilizarán los datos que recolectan y accederán a datos contextuales de otras fuentes para 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.

Por ejemplo, para ayudar a combatir la epidemia de Ébola, Orange Telecom (África Occidental) trabajó con la Facultad de Salud Pública de Harvard [Harvard School of Public Health, HSPH] y Flowminder para predecir la propagación de la enfermedad utilizando datos recabados de teléfonos móviles. Orange Telecom acumuló los datos extraídos de teléfonos celulares en Costa de Marfil (en 2011) y Senegal (en 2013), los anonimizó y luego autorizó su divulgación a Flowminder. Estos datos fueron utilizados para desarrollar un modelo que permitió observar los movimientos de la población regional y que luego fueron considerados en la elaboración de recomendaciones sobre dónde focalizar los esfuerzos de atención médica (MIT Review, 2014. "Cell-Phone Data Might Help Predict Ebola's Spread" [Los datos de los teléfonos celulares pueden ayudar a predecir la propagación del Ebola]).

Por otro lado, Telenor Group y Telenor Pakistán, junto con HSPH, realizaron el primer esfuerzo a nivel nacional en la historia de Pakistán, para entender y modelar la propagación del dengue utilizando datos de movilidad anonimizados. Este proyecto no solo fue el más grande de este tipo -en términos de cantidad de suscriptores analizados- sino que también representa el primer intento de estudiar los brotes de dengue mediante el análisis de los registros de detalles de llamadas [Call Detail Record, CDR]. El objetivo era diseñar estrategias de prevención basadas en métodos fundamentados en datos, en los que Telenor aprovechó su competencia interna principal de análisis y la combinó con el conjunto de datos exclusivos, para crear un valor compartido, tanto para Telenor como para la sociedad. El estudio demostró cómo utilizar los datos del consumidor, recolectados por los operadores móviles respetando la privacidad del usuario, para resolver y brindar soporte a la solución de problemas sociales. Mediante esta metodología, se tradujo a términos operativos un mapa de las zonas de riesgo de dengue que puede servir como herramienta útil para los médicos y el gobierno de Pakistán. Asimismo, brindó información para diseñar mejores estrategias de prevención. (Telenor, 2017).

La industria móvil está decidida a ayudar a materializar los beneficios económicos y sociales que brinda el análisis del big data a través de buenas prácticas de responsabilidad digital para que la sociedad pueda liberar el enorme potencial del análisis de big data de forma tal que se respeten los principios de privacidad ya consolidados y promuevan un entorno de confianza.

En colaboración con representantes del ecosistema móvil, la GSMA también está trabajando en los aspectos relativos a la privacidad del análisis de big data, sustentados por los Principios de Privacidad Móvil.

37. El capítulo "Protección de la seguridad de las redes y la integridad de los dispositivos" analiza el Internet de las Cosas en mayor profundidad.
38. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers" [Privacidad móvil: conclusiones y consideraciones para formuladores de políticas sobre estudios de consumidores]

Consideración de la privacidad del consumidor al recolectar y utilizar datos

La GSMA desarrolló un conjunto de Principios de Privacidad Móvil que describen la forma en que se debería respetar y proteger la privacidad del consumidor móvil al utilizar aplicaciones y servicios que tienen acceso, utilizan o recolectan 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.[39] El objeto de estos principios es lograr un equilibrio entre proteger la privacidad de una persona y garantizarle un trato justo, a la vez que se permite a las entidades alcanzar sus objetivos comerciales, sociales y de política pública. En términos generales, son lo suficientemente flexibles como para incluir, a medida que van surgiendo, nuevas tecnologías y metodologías de negocios. Seis de los nueve principios tienen particular relevancia para la recolección y el uso de datos personales:

- Apertura, transparencia y notificación
- Seguridad
- Propósito y uso
- Niños y adolescentes
- Datos mínimos y retención de datos
- Responsabilidad y ejecución

Figura 5

Principios de Privacidad Móvil de la GSMA[40]

APERTURA, TRANSPARENCIA Y NOTIFICACIÓN

Las personas responsables deben ser abiertas y honestas con los usuarios y asegurarse de que se les suministre información clara, en forma prominente y oportuna, sobre su identidad y las prácticas de privacidad de datos. Se debe suministrar información al usuario respecto de las personas que recolectan su información personal, el propósito de una aplicación o servicio como también respecto del acceso, recolección, distribución, divulgación y uso posterior de la información personal del usuario, incluyendo a quién se puede divulgar su información personal, permitiendo así a los usuarios tomar decisiones informadas sobre si utilizar o no una aplicación o servicio móvil.

SEGURIDAD

La información personal se debe proteger utilizando garantías razonables y adecuadas a la sensibilidad de la información.

RESPONSABILIDAD Y EJECUCIÓN

Todas las personas a cargo son responsables de asegurar el cumplimiento de estos principios.

PROPÓSITO Y USO

El acceso, recolección, distribución, divulgación y uso posterior de la información personal del usuario estarán limitados a fines comerciales legítimos, tales como la provisión de aplicaciones o servicios solicitados por el mismo usuario o, de lo contrario, a cumplir con las obligaciones legales correspondientes.

NIÑOS Y ADOLESCENTES

Las aplicaciones o servicios dirigidos a niños y adolescentes deben garantizar que la recolección, el acceso y el uso de información sea apropiado, en todo tipo de circunstancias, y compatible con las leyes nacionales.

DATOS MÍNIMOS Y RETENCIÓN DE DATOS

Solo se debe recolectar la mínima cantidad de información personal necesaria para cumplir con los fines comerciales legítimos y para proporcionar, suministrar, mantener o desarrollar aplicaciones o servicios. La información personal no se debe mantener más tiempo que el necesario para los fines comerciales legítimos o para cumplir con las obligaciones legales correspondientes, y luego debe ser eliminada o se deben anonimizar dichos datos personales.

RESPETO A LOS DERECHOS DEL USUARIO

Se debe suministrar información a los usuarios respecto de sus derechos al uso de su información personal y una forma sencilla de ejercerlos.

OPCIONES Y CONTROL DEL USUARIO

OPT IN OPT OUT

Los usuarios deben tener la oportunidad de ejercer la elección y el control de su información personal.

EDUCACIÓN

El usuario debe recibir información sobre las cuestiones de privacidad y seguridad y las formas de administrar y proteger su privacidad

39. GSMA, Principios de privacidad móvil (2016), consultar: http://www.gsma.com/publicpolicy/mobile-privacy-principles
40. http://www.gsma.com/publicpolicy/mobile-privacy-principles

Implicancias clave para el gobierno, la industria y otros interesados relevantes

La GSMA y sus miembros están convencidos de que la privacidad y la seguridad son aspectos fundamentales para consolidar la confianza del consumidor en los servicios móviles y se comprometen a trabajar con todos los interesados, a lo largo y ancho de la industria móvil, en la elaboración de una estrategia común para proteger la privacidad y promover la confianza en los servicios móviles. En relación con los servicios brindados a sus clientes, los operadores móviles procurarán proteger su identidad digital y asegurar las comunicaciones y los datos personales de los mismos. La amplia gama de servicios de terceros que están disponibles a través de los dispositivos móviles ofrece diferentes niveles de protección de la privacidad. Por este motivo:

- Para que el consumidor pueda confiar en que sus datos personales están bien protegidos, independientemente del servicio o dispositivo, se debe brindar un nivel de protección equivalente para todos los servicios
- Las garantías necesarias deben ser el resultado de una combinación de estrategias acordadas a nivel internacional junto con legislación nacional 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 deben:

- Ser claros con el consumidor sobre qué es lo que 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. Si bien un consumidor sofisticado pueda entenderlo, la mayoría de los segmentos de consumidores no lo saben

Al formular o revisar la legislación y la regulación:

- Los gobiernos deben asegurar que la legislación sea neutra respecto de los servicios y tecnología, para que sus normas se apliquen en 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 más que en intentar legislar el tipo de datos específico. Por ejemplo, el mismo elemento de datos se puede utilizar para obtener un valor que puede ser comercial (por ejemplo, si es vendido a una organización de terceros), operativo (por ejemplo, si se informa a la persona responsable de la toma de decisiones y de la asignación de recursos internos) o público (por ejemplo, si se informa a los responsables de los esfuerzos de recuperación ante desastres)

Elección del consumidor

Empoderaramiento del consumidor para elegir

Muchos servicios en línea se ofrecen a los consumidores en forma gratuita, ya que el proveedor obtiene sus ganancias de ingresos relacionados con la publicidad en dicho servicio. Con el objeto de maximizar estos 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 presenten propuestas para publicar un anuncio (en diferentes formatos) frente a ese usuario. Este tipo de microsegmentos y subastas de milisegundos son cada vez más frecuentes y dependen de que el proveedor de servicios utilice la información de usuarios que haya comprado o pueda haber obtenido en forma directa. Si bien no caben dudas de que se debe lograr un equilibrio entre la entrega de cierta información a cambio del uso del servicio gratuito, 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[41] demuestra que los usuarios móviles quieren opciones simples y claras para controlar el uso de su información y revela que es una preocupación para más del 80% de los usuarios de internet móvil en todo el mundo compartir sus datos personales al tener acceso a aplicaciones y servicios. Además, antes de instalar una aplicación, la mayoría (65%) de los usuarios procura averiguar a qué información contenida en su dispositivo accederá la aplicación, lo cual demuestra el deseo de entender en qué medida puede verse afectada su privacidad. La mayoría de los usuarios móviles (81%) también quiere que se les pida permiso antes de que terceros tengan acceso a los datos personales contenidos en sus dispositivos móviles, para así tener más control sobre los tipos de datos a los que pueden tener acceso las diferentes compañías

4

41. La GSMA trabaja codo a codo con sus miembros para enfrentar en forma proactiva los desafíos clave de la privacidad móvil y, como parte de esto, encargó investigaciones mundiales sobre más de 11 500 usuarios móviles (Brasil, Colombia, Indonesia, Malasia, Singapur, España y el Reino Unido). Las conclusiones demuestran que los usuarios móviles de todos los países comparten actitudes y preocupaciones similares respecto de su privacidad. El documento "MOBILE PRIVACY: Consumer research insights and considerations for policymakers" presenta las conclusiones clave de las investigaciones y analiza las implicancias para los legisladores. Para ver el informe detallado, consultar http://www.gsma.com/publicpolicy/mobile-privacy-consumer-research-insights-and-considerations-for-policymakers

Implicancias clave para el gobierno, la industria y otros interesados relevantes

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

- Elección y control del usuario: los usuarios deben tener la oportunidad de realizar elecciones significativas y controlar su información personal[42]
- Respeto a los derechos del usuario: se debe suministrar información al usuario sobre sus derechos en cuanto al uso de su información personal y brindarle una forma sencilla de ejercerlos
- Educación: el usuario debe recibir información sobre las cuestiones relacionadas con la privacidad y la seguridad y las formas de gestionar y proteger la misma

Siguiendo estos principios, la GSMA también elaborará un conjunto de "Directrices para el diseño de privacidad en el desarrollo de aplicaciones móviles" en colaboración con representantes del ecosistema móvil. Estas directrices están diseñadas para ayudar a los desarrolladores de aplicaciones a incorporar la privacidad en futuras aplicaciones y servicios.

No obstante, aún cuando estos principios tengan plena vigencia, no son suficientes para brindarle al consumidor el nivel de elección requerido. Los operadores de redes móviles no tienen gran influencia sobre los términos y condiciones de privacidad utilizados por los proveedores de servicios en línea. Se corre el riesgo de que las nuevas leyes y regulaciones generen el efecto no deseado de agobiar al usuario móvil y exacerbar el 'síndrome de fatiga de privacidad' provocado por la necesidad de aceptar condiciones que el usuario ni siquiera ha leído o entendido.

En cuanto a los servicios ofrecidos por los operadores de redes móviles, estos últimos procurarán 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 todas las partes interesadas de la industria móvil para desarrollar una estrategia consistente a fin de proteger la privacidad y promover la confianza en los servicios móviles. Como resultado de este compromiso, además de otras iniciativas, se desarrollaron las "Directrices para el diseño de privacidad en el desarrollo de aplicaciones móviles" de la GSMA que enfatizan los siguientes aspectos:

- Los operadores de redes móviles deben garantizar que los riesgos de la privacidad son tomados en cuenta en el diseño de aplicaciones y servicios nuevos, así como en la elaboración de soluciones que ofrezcan a los clientes una forma fácil de entender las opciones de privacidad y de controlar sus datos
- Los desarrolladores de aplicaciones para dispositivos móviles deben incorporar los principios de privacidad elaborados por la industria y las directrices de diseño, tales como los Principios de Privacidad Móvil de la GSMA
- El diseño de las nuevas aplicaciones y servicios debe incorporar la protección (es decir, la privacidad por diseño) para ofrecer transparencia, opciones y control al usuario individual, y así fortalecer la confianza

42. En los Principios de Privacidad de la GSMA, a los datos personales se los denomina 'información personal'

Flujo transfronterizo de datos

El tercer aspecto de la privacidad del consumidor está relacionado con la(s) jurisdicción(es) en las que se almacenan los datos personales y/o se tiene acceso a los mismos, y las implicancias del flujo transfronterizo de datos. Almacenar y procesar datos en una ubicación centralizada, por lo general, permite a los operadores de redes móviles mejorar el desempeño y el aspecto económico de la provisión de sus servicios, los cuales no serían viables si se debieran implementar para un solo país. Gracias a este tipo de operación, el consumidor puede disfrutar de los beneficios brindados por más servicios, mayor innovación y soporte. Al desplazar los datos de un territorio a otro, surge la pregunta de cuál es la jurisdicción legal competente. Puede ser de gran ayuda para los gobiernos contar con un marco interoperable y mecanismos de identificación de responsabilidad a fin de enfrentar los desafíos que presentan las distintas jurisdicciones y facilitar así el flujo transfronterizo de datos.

Nuevos marcos legales, tales como las Reglas de Privacidad Transfronteriza [*Cross Border Privacy Rules*, CBPR] de APEC [*Asia-Pacific Economic Cooperation Forum* - Foro de Cooperación Económica Asia-Pacífico] y las Normas Corporativas Vinculantes de la UE establecen los principios internacionales comunes, incluidos los mecanismos de responsabilidad que rigen la forma en que se deben tratar los datos durante su transferencia entre países. Sin embargo, el éxito de la adopción de estos principios se ve afectado por la implementación, por parte de los gobiernos, de normas de 'localización de datos' (también conocidas como 'soberanía de datos') que imponen requerimientos locales de almacenamiento o uso de tecnología,[43] y pueden encontrarse en una amplia variedad de normas específicas para un sector o una temática, incluyendo a los proveedores de servicios financieros, el secreto profesional o el sector público. En ocasiones, los países imponen este tipo de reglas convencidos de que las autoridades de supervisión podrán inspeccionar los datos almacenados localmente con mayor facilidad.[44] Si bien algunas de estas normas procuran proteger la privacidad del individuo, también están creando un conglomerado fragmentado de leyes y regulaciones que confunde y pone en riesgo los beneficios que ofrece una infraestructura abierta de redes. Estas normas de localización de datos también pueden tener un impacto negativo en el comercio digital y el crecimiento económico mundial.

Soluciones para la privacidad y seguridad del flujo transfronterizo de datos

Operar una red móvil genera grandes cantidades de datos a diario. Para poder facturar los servicios a cada usuario, cada llamada y cada transferencia de datos debe ser registrada, para luego ser procesada en base a tarifas y saldos de cuentas. De esta manera, se generan y almacenan grandes cantidades de datos operativos asociados a las cargas de tráfico, registros de fallas o consultas del cliente (por ejemplo, cambio de tarifa, cambio de dirección). Como resultado de estas demandas, los operadores de redes móviles son los principales usuarios de servicios de almacenamiento y procesamiento en centros de datos globales. Los consumidores disfrutan los beneficios que ofrece esta amplia gama de servicios, innovación y soluciones de avanzada que los operadores pueden ofrecer, ya sea en forma directa o a través de terceros, al acceder y utilizar estos servicios globales, directamente de manos del operador o de terceros.

Garantizar la integridad y la seguridad de esos datos es una tarea de gran envergadura y requiere soluciones complejas. Para muchos operadores de redes móviles, en particular aquellos que son subsidiarias de grupos internacionales o que eligen utilizar a un proveedor externo, posiblemente la mejor solución sea alojar y procesar los datos en múltiples países, lo cual les permite desarrollar economías de escala y conocimientos técnicos mediante la agregación de las necesidades de varios países en el diseño de una solución holística y robusta, con más funcionalidades, seguridad y mejor redundancia de la que sería posible si se tratara de una solución 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 viables, o ni siquiera posibles, desde el punto de vista económico, para una única operación en un solo país. Por supuesto, la implementación de este tipo de soluciones requiere el desplazamiento de datos del consumidor a los centros de datos multinacionales que, en muchos casos, se encuentran en países distintos del país del operador de redes original.

Si bien los beneficios técnicos están claros, las implicancias legales son complejas: las normas de protección de datos de qué país deberían aplicarse: ¿las del país donde se procesan los datos, las del país del usuario final o las del país donde está ubicado el inspector de datos (por ejemplo, el operador de redes móviles)?

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

43. Anupam Chander y Uyen Le, 2015. "Data Nationalism", Emory Law Journal; and Jonah Force Hill, 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", Hague Institute for Global Justice ["Nacionalismo de datos", Emory Law Journal; y Jonah Force Hill, 2014. "El aumento en la localización de los datos luego de Snowden: análisis y recomendaciones para formuladores de políticas y líderes de mercado de EE. UU."]
44. European Commission, "Building a European Data Economy Communication", pg.5 [Comisión Europea "Construir una economía de datos europea", pág. 5]

las expectativas y estándares de ese país: una forma obvia de exigir el cumplimiento es requerir 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 sus consiguientes beneficios.

Las restricciones no necesariamente redundan en una mejor protección de la información personal. Un enfoque fragmentado genera desigualdad en la protección (por ejemplo, diferencias entre jurisdicciones y sectores respecto de lo que se puede almacenar y la duración de dicho almacenamiento) y provoca confusión, con el consiguiente impacto en la gestión segura de los datos personales. La fragmentación causada por la localización también puede levantar barreras que vuelven prohibitiva toda inversión en la protección de la seguridad. En conjunto, todo esto puede socavar los esfuerzos de los operadores de redes móviles por desarrollar tecnologías y servicios que mejoren la privacidad a fin de proteger al consumidor.

Aquí es importante reformular la distinción entre los datos personales, a los cuales tienen acceso y procesan los operadores de redes móviles, y los datos personales recolectados y almacenados por proveedores de servicios en línea e intermediarios de internet. Como se analizó en la sección sobre elección del consumidor, estos servicios son muy diferentes y el hecho de que sean operados desde fuera del país de uso, en la mayoría de los casos, multiplica aún más las complejidades legales. Si bien aquí las inquietudes y cuestiones de privacidad son igual de relevantes, en este caso exceden el control de los operadores de redes móviles, tanto en términos de datos transferidos por los usuarios, como de la forma en que se puede tener acceso a los mismos

Implicancias clave para el gobierno, la industria y otros interesados relevantes

El flujo internacional de datos juega un papel importante en la innovación, la competencia y el desarrollo socioeconómico. Por este motivo:

- Toda restricción y condición impuesta sobre el flujo internacional de datos debe ser minimizada y solo debe ser aplicada en circunstancias excepcionales
- Las normas de flujo transfronterizo de datos deben estar basadas en el riesgo y deben también respaldar toda medida que asegure que el tratamiento de los datos se realiza en base a garantías adecuadas y proporcionales, a la vez que ayudan a materializar los potenciales beneficios socioeconómicos
- Asimismo, en la medida en que los gobiernos necesiten inspeccionar los datos para fines oficiales, deben hacerlo a través de medios lícitos y mecanismos intergubernamentales adecuados que no restrinjan el flujo de datos

Los operadores de redes móviles reconocen la preocupación relacionada con mantener la seguridad de los datos y ayudar a garantizar que los derechos de las personas no se vean perjudicados. También reconocen los desafíos más amplios que presenta la vigilancia nacional e internacional. No obstante:

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

Una cuestión fundamental es que, en la actualidad, el flujo transfronterizo de datos está regulado por un conglomerado de instrumentos y leyes internacionales, regionales y nacionales. Si bien todos adoptan los principios comunes, no establecen un marco regulatorio interoperable que refleje la realidad, los desafíos y el potencial de un mundo globalmente conectado. Las normas de protección de datos deberían ser compatibles entre países y regiones en la mayor medida posible, ya que se crea así una mayor seguridad y previsibilidad jurídica y se facilita que las compañías desarrollen un marco escalable y responsable de protección y privacidad de datos.

Un marco de protección de datos interoperable ayudaría a fortalecer y promover mecanismos adecuados y eficaces para garantizar el tratamiento de los datos de forma tal que se protejan los derechos e intereses de los consumidores y los ciudadanos. Todo marco interoperable que incorpora mecanismos eficaces de responsabilidad puede ayudar a fortalecer y proteger importantes derechos que favorecen la prosperidad de las personas y las economías. Por ejemplo, el trabajo para que el sistema CBPR de APEC y las Normas Corporativas Vinculantes de la UE sean compatibles ofrece beneficios potenciales para la industria, el comercio digital y los intereses y derechos de los consumidores.

La GSMA y sus miembros mantienen su compromiso de trabajar con todos los interesados 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.

5 Protección de la seguridad pública

Como proveedores de infraestructura nacional crítica, las redes móviles desempeñan un papel clave en la protección del público en general y la sociedad en su conjunto. Por ejemplo, las redes móviles se utilizan como medio de comunicación para servicios de emergencia, especialmente para responder a acontecimientos graves, a la vez que muchos otros incidentes son informados por el público a través de sus dispositivos móviles.

Los operadores de redes móviles deben colaborar con los organismos de seguridad, conforme a las leyes y reglamentaciones, las obligaciones contenidas en las licencias y la legislación local, en línea con el objetivo general de proteger la seguridad púbica. Por ejemplo, como parte de una investigación criminal, se puede otorgar una orden judicial a un organismo de seguridad para monitorear las comunicaciones de un sospechoso en particular, tanto las que recibe como las que realiza y las que intercambia con otros sospechosos. Por lo tanto, un requisito típico de la mayoría de las licencias es que los operadores de redes móviles deben ofrecer los medios técnicos para cumplir con sus obligaciones legales de colaborar con la aplicación de la ley. En la mayor parte de los países, dichas intervenciones se limitan y están sujetas al debido proceso legal.

La Declaración Universal de los Derechos Humanos (DUDH)[45] y el Pacto Internacional de Derechos Civiles y Políticos (PIDCP)[46] reconocen que todas las personas

45. 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. Establece, por primera vez, los derechos humanos fundamentales que deben protegerse en el mundo entero. El derecho a la privacidad se refleja en el Artículo 12 y el derecho a la libertad de expresión, en el Artículo 19. Para la DUDH, consultar: http://www.un.org/es/universal-declaration-human-rights/

46 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 refleja en el Artículo 17 y el derecho a la libertad de expresión, en el Artículo 19. Para el tratado, consultar: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en

del mundo tienen derecho a comunicarse entre sí en privado y tienen también derecho a la libertad de expresión, dentro del ámbito, los límites y la moral pública de cualquier Estado. Los instrumentos de derechos humanos internacionales 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.

Puede darse que haya conflicto entre el objetivo de la seguridad nacional y la aplicación de la ley a fin de proteger la seguridad pública y los derechos a la privacidad, la libertad de expresión y al acceso a la información. En la mayoría de los países, estas necesidades, potencialmente opuestas, redundan, por defecto, en la postura de que las personas deben poder comunicarse con libertad y privacidad y que las intervenciones e interrupciones solo se deben aplicar en casos excepcionales, en una medida necesaria y proporcionada, y estar sujetas al debido proceso legal. La mayoría de los países cuenta con garantías para evitar el abuso y uso excesivo de las facultades capaces de socavar la privacidad de la comunicación.

Esta sección examina los tres ejemplos típicos de intervención de la seguridad pública y las cuestiones que surgen cuando las diferentes partes procuran enfrentarlas en la práctica, específicamente:

- Solicitudes de asistencia para aplicación de la ley, con foco en la necesidad de transparencia y garantías
- Restricción de servicio, con foco particular en el uso de inhibidores de señales móviles
- Registro de usuarios, con foco en el registro de consumidores de tarjetas SIM prepagas

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y otros interesados, que también se describen más adelante en este capítulo.

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 los organismos de seguridad, conforme a las leyes y reglamentaciones, las obligaciones contenidas en las licencias y la legislación local. Es importante que el gobierno garantice la existencia de un marco legal adecuado que describa claramente las facultades de los organismos nacionales de seguridad. Asimismo, este marco debe garantizar 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 con toda obligación, establecida por ley o por sus licencias, relacionada con temas de protección o seguridad pública en los países en los que operan, a la vez que cumplen con los principios de derechos humanos. Los operadores colaborarán con los organismos de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- **Trabajar con los organismos pertinentes cuando la situación particular así lo requiera, a fin de desarrollar e implementar soluciones adecuadas para alcanzar el objetivo final con el mínimo trastorno al consumidor y los servicios críticos**
- **Construir redes que tengan la funcionalidad de enfrentar situaciones de emergencia y seguridad, cuando corresponda**
- **Ser claros sobre las limitaciones de las acciones que se pueden tomar en relación con la cadena de valor e indicar cuándo se deben implementar acciones por parte de terceros**

Solicitud de asistencia a organismos de seguridad

Cumplimiento con solicitudes de asistencia a organismos de seguridad

En general, las licencias otorgadas a los operadores de redes móviles establecen las obligaciones que deben cumplir para apoyar las actividades de los organismos de aplicación de ley y seguridad nacional del país emisor. En general, cuando existen, esas leyes y obligaciones contenidas en las licencias requieren que los operadores de redes móviles retengan información[47] sobre el uso que el usuario le da a los servicios móviles y la compartan con el organismo de seguridad, conforme a una legítima solicitud. Asimismo, los operadores deben tener la capacidad de interceptar comunicaciones en tiempo real, siempre que cuenten con una solicitud legítima.

Las leyes generalmente definen las condiciones y, en algunos casos, los procesos conforme a los cuales los organismos de seguridad pueden solicitar a un operador de redes que otorgue acceso o información sobre las comunicaciones llevadas a cabo en su red. Asimismo, ofrecen un punto de referencia legal que sirve de orientación para los operadores de redes móviles respecto de cómo responder a estas solicitudes. En noviembre de 2016, el Reino Unido (RU) aprobó una nueva legislación[48] 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 RU son aceptables o no, lo importante es que las normas fueron públicamente debatidas y promulgadas. Es posible que falte claridad en el marco legal de algunos países sobre la reglamentación de la divulgación de datos o la interceptación legítima de las comunicaciones de los consumidores, lo cual plantea un desafío para la industria cuando debe intentar proteger la privacidad de la información del consumidor y cumplir con las obligaciones de asistir a los organismos de seguridad contenidas en su licencia.

En los últimos años, se ha dado un importante debate público a nivel global sobre el alcance, necesidad y legitimidad de los poderes legales que las autoridades de gobierno utilizan para tener acceso a las comunicaciones de las personas físicas. También han surgido preguntas respecto del papel que desempeñan los proveedores de redes y servicios de telecomunicaciones en relación a dicho acceso. En virtud de lo anterior, en 2011, un grupo de proveedores y operadores de redes móviles creó el Diálogo de la Industria [Industry Dialogue, ID] de las Telecomunicaciones (ver más abajo) para trabajar conjuntamente en cuestiones de privacidad y libertad de expresión y definir los principios que describen la responsabilidad de las compañías de telecomunicaciones en la protección de la libertad de expresión y la privacidad. Uno de los resultados del trabajo del ID fue que muchas de las compañías miembro decidieron, siempre que fuera posible, divulgar proactivamente información sobre la naturaleza y el volumen de las solicitudes de acceso a información que reciben de parte del gobierno, en cada país en el que operan.[49]

Dado que la legislación, por lo general, se encuentra atrasada respecto de los avances tecnológicos,[50] pueden surgir malentendidos sobre el nivel de capacidad técnica para interceptar las comunicaciones de los operadores de redes móviles. La interceptación de una llamada telefónica y de un mensaje SMS estándar, dirigidos a un usuario específico o enviado por el mismo, es técnicamente posible. Desde hace décadas ya que los estándares móviles mundiales describen los requisitos y capacidades para una interceptación legítima. En cambio, las comunicaciones entre usuarios sobre una plataforma basada en internet generalmente están fuera del alcance de los operadores de redes móviles, aun cuando dicho tráfico es cursado en sus redes. Algunos servicios populares, tales como WhatsApp, WeChat y Signal, están encriptados y los operadores de redes móviles no tienen la posibilidad de guardar dichos mensajes ni tienen a su disposición las claves de decodificación. Esto significa que, aun cuando reciban una solicitud legítima, el operador de redes no podrá tener acceso y, por lo tanto, no podrá entregar el contenido de los mensajes (en la próxima sección, ver 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 relación con la defensa de la seguridad de sus ciudadanos. Para lograr este objetivo, la interceptación de las comunicaciones a fines de la aplicación de la ley o de seguridad solo debe tener lugar

47. 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
48. Para más información, consultar: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
49. Sin embargo, muchos países prohíben expresamente a los operadores de redes móviles la divulgación de hasta detalles importantes sobre la naturaleza y el volumen de las solicitudes de interceptación que reciben.
50. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles: Acceso gubernamental"
51. Telecompaper, 2016. "El Salvador introduces 5% telecoms tax" [El Salvador aprueba impuesto de 5% a las telecomunicaciones]

bajo un marco legal claro, compatible con los principios de derechos humanos de necesidad y proporcionalidad y mediante procesos y autorizaciones correspondientes, según lo especifique dicho marco.

Por último, la responsabilidad y, a menudo, también los costos de las actividades encaradas por los operadores de redes móviles para apoyar las necesidades de seguridad pública son asumidos, cada vez con más frecuencia, por los operadores. El Salvador es un ejemplo extremo de lo anterior, donde, en noviembre de 2015, se aprobó un impuesto del 5% a los servicios de comunicaciones para financiar los planes de seguridad general del gobierno.[51] Si bien la política tributaria es un asunto que deben decidir los gobiernos, imponer tributación 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 invierte en la seguridad pública.

Implicancias clave para el gobierno, la industria y otros interesados relevantes

Los operadores de redes móviles tienen la responsabilidad de asegurarse de responder solamente a solicitudes legítimas (es decir, mandatos judiciales) recibidas 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 proporcionado que especifique claramente las facultades de vigilancia a disposición de los organismos nacionales de seguridad.[52]

- Toda interferencia con el 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[53]
- 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, proporcionado, justificado y compatible con los principios de derechos humanos, incluidas las obligaciones resultantes de los tratados internacionales de derechos humanos aplicables, tales como el Pacto Internacional sobre Derechos Civiles y Políticos
- Dada la constante expansión de la gama de servicios de comunicaciones, el marco legal debe consagrar la neutralidad tecnológica[54]
- Los gobiernos deben proveer limitaciones de responsabilidad civil apropiadas o indemnizar a los proveedores de telecomunicaciones frente a demandas judiciales entabladas respecto de su cumplimiento con las solicitudes y obligaciones para la retención, revelación e interceptación de comunicaciones y datos, así como el retiro del acceso a redes y servicios[55]
- Asimismo, los costos de cumplir con todas las leyes que regulan la interceptación de las comunicaciones como también 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[56]

La GSMA y sus miembros apoyan toda iniciativa tendiente a aumentar la transparencia del gobierno y la publicación por parte del mismo de las estadísticas relativas a las solicitudes de acceso a los datos de cliente[57] cuando sea posible

5

52. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles: Acceso gubernamental"
53. Ibídem.
54. Ibídem
55. Ibídem.
56. Ibídem
57. Ibídem.

Estudio de caso

Diálogo de la Industria de las Telecomunicaciones —información sobre transparencia (divulgación de solicitudes de autoridades)

Por qué informar...

El Diálogo de la Industria [Industry Dialogue, ID] de las Telecomunicaciones, lanzado oficialmente en 2013, es 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 dentro del contexto de los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas. Estas compañías tienen presencia internacional y ofrecen servicios y equipos de telecomunicaciones a consumidores, empresas y gobiernos en casi 100 países a nivel mundial.

Compartir aprendizajes es uno de los propósitos claves del ID. Además, para expandir la noción de transparencia, los operadores del ID —AT&T, Millicom, Orange, Telenor Group, Telia Company y Vodafone Group— publican periódicamente informes de conocimiento púbico sobre las solicitudes que reciben de los organismos de seguridad, con la expectativa de que ayuden al público a entender el contexto en el cual operan e interactúan con dichos organismos.

Qué se informa...

Normalmente, los objetivos de estos informes son:

- **Explicar los marcos legales y la capacidad de aplicación de la ley en sus mercados de operación**
- **Explicar las políticas públicas y los procesos conforme a los cuales responden a las exigencias de organismos y autoridades**
- **Siempre que sea posible, divulgar las estadísticas sobre la cantidad de solicitudes de datos de consumidores recibidas de los organismos de seguridad en ciertos países o regiones**

Cuáles son las limitaciones...

A menudo, la legislación sobre la aplicación de la ley y la seguridad nacional incluye rigurosas restricciones que impiden a los operadores divulgar cualquier información relacionada con los requerimientos que reciben de organismos y autoridades, incluida la divulgación de estadísticas globales. Muchos países también prohíben a los operadores suministrar información al público sobre los medios a través de los cuales se implementan estos requerimientos. Estas restricciones pueden representar importantes obstáculos para que los operadores puedan dar respuesta a la petición de mayor transparencia por parte del público

No obstante, estos operadores consideran que, si bien los Estados son los que tienen la principal responsabilidad de ser transparentes, medir la cantidad de solicitudes recibidas de las autoridades, con todas sus fallas, constituye la medición más sensata disponible, sin ser demasiado compleja. También hacen hincapié en que solo los gobiernos que realizan estas solicitudes a los proveedores de comunicaciones pueden ofrecer un panorama completo del alcance de las solicitudes.
(Diálogo de la Industria de las Telecomunicaciones, ver: https://www.telecomindustrydialogue.org/)

5

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 (*service restriction orders* o *SRO*, por sus siglas en inglés), en base a las cuales se requiere 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 referirse al 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 a cumplir por ley, en algunos casos, los operadores de redes móviles podrían recibir sanciones penales (incluido el encarcelamiento de su personal jerárquico) o correr el riesgo de perder su licencia, si divulgaran haber recibido una SRO o si se negaran a cumplir con dicha orden.

Las SRO pueden tener una serie de consecuencias graves. Por ejemplo, se puede ver afectada la seguridad nacional en caso del uso indebido de las facultades (es decir, depender de una restricción en la red a fin de 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), y también puede poner 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. De igual modo, los operadores de redes móviles se ven afectados. 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 estar sometido a presiones por parte de las autoridades y, posiblemente, hasta sufrir represalias por parte del público.

Un ejemplo de este tipo de situación ocurrió en Brasil recientemente, país en el que el servicio de mensajería WhatsApp supuestamente no brindaba la asistencia necesaria a diferentes investigaciones penales.[58] En tres ocasiones distintas desde diciembre de 2015, en respuesta, el gobierno exigió a los operadores de redes móviles brasileños que restringieran el acceso a los servicios de WhatsApp.[59] El principal efecto de esta acción fue impedir el uso de la aplicación de mensajería móvil más popular del país a los 100 millones de usuarios en Brasil. Cada uno de los fallos fue revocado después de que se presentaran apelaciones ante tribunales superiores dado que el impacto se consideraba 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 las mismas debido al uso de encriptación punta a punta. No obstante, muchos de los usuarios afectados generalmente culpan al operador de redes móviles por la interrupción del servicio.

En algunos países, se registraron ejemplos aún más extremos de desconexión de redes, en algunos casos, con el objetivo de limitar la capacidad de organización de un oponente político del gobierno.[60] Como primer paso, los operadores de redes móviles instan a los gobiernos a ser transparentes con sus ciudadanos respecto de su rol en la desconexión o la restricción de redes y servicios, como también de las justificaciones legales de las mismas. Más importante aún, estas órdenes de desconexión deberían incluir el permiso a las compañías de informar oportunamente a sus clientes que la restricción en el servicio tuvo lugar de conformidad con una orden del gobierno.[61]

58. Financial Times, 2016. "WhatsApp ban ignites Brazil censorship fears" [La prohibición de WhatsApp enciende el temor a la censura]
59. The Guardian, 2016. "WhatsApp ofcially un-banned in Brazil after third block in eight months" [Prohibición de WhatsApp en Brasil oficialmente levantada luego del tercer bloqueo en ocho meses]
60. En la Base de datos de retrospectiva del "Internet & Jurisdiction" se pueden encontrar ejemplos de desconexiones. Favor consultar: http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTEifQ
61. Para más información sobre la declaración conjunta del Diálogo de la Industria de las Telecomunicaciones y la Iniciativa de Red Global,consultar: http://www.telecomindustrydialogue.org/wp-content/uploads/GNI-ID-Joint-Statement-Network-and-Service-Shutdowns-SPANISH-1.pdf

Uso de inhibidores de señal

Otra forma de restringir las comunicaciones móviles es la utilización de inhibidores de señal, también conocidos como bloqueadores [*jammers*].
Se trata de dispositivos que generan una interferencia que interrumpe, en forma intencional, los servicios de radiocomunicación al obstruir la conexión entre el terminal móvil y la estación radiobase. En general, estas herramientas rudimentarias se utilizan para impedir las comunicaciones en centros penitenciarios o entre terroristas o grupos políticos considerados subversivos, a menudo, en lugares donde se realizan 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 utilizan para evitar el uso ilegal de dispositivos móviles en lugares sensibles, como prisiones. Sin embargo, el bloqueo de la señal no soluciona la raíz del problema, el hecho de que los dispositivos móviles llegan a 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 se circunscribirá a un área específica. Por lo tanto, dicha interferencia afecta a los ciudadanos, a los servicios y a las organizaciones de seguridad pública. Asimismo, tiene un efecto dominó para muchos otros usuarios, especialmente aquellos que viven y trabajan en las inmediaciones de la prisión y 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, redunda en un impacto negativo en los operadores móviles.

Cualquier interrupción en las redes de comunicaciones, los servicios de red o el internet (tales como redes sociales, motores de búsqueda o 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.

5

Implicancias clave para el gobierno, la industria y otros interesados relevantes

Si bien, por un lado, la GSMA entiende y está de acuerdo con el uso adecuado de una interceptación legítima en pos de una mejor seguridad pública, por otro lado, la GSMA no está de acuerdo con el uso de órdenes de restricción de servicios (SRO) e inhibidores de señal.

Los gobiernos solo deberían recurrir a las SRO en circunstancias excepcionales y predeterminadas y solo en los casos en que sean estrictamente necesarias y proporcionales a fin de alcanzar un objetivo específico y legítimo, conforme a las leyes pertinentes y los derechos humanos reconocidos internacionalmente.[62] Existen otras cuestiones que también deben ser consideradas:

- A fin de promover la transparencia, toda SRO del gobierno debería ser emitida solo por escrito a los operadores, citando los fundamentos legales y estableciendo un claro mecanismo de auditoría que indique quién es la persona que autoriza dicha orden. Asimismo, se debe informar a los ciudadanos que es el gobierno el que ordena la restricción del servicio y que fue aprobada por autoridad judicial o cualquier otra que tenga competencia, de conformidad con los procedimientos administrativos establecidos por ley. Deben 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 a dicha orden. En caso de que esta comunicación con el cliente afecte la seguridad nacional si se hiciera al momento de la restricción, entonces se deberá informar a los ciudadanos a la mayor brevedad posible, con posterioridad al hecho[63]
- 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 debería apuntar a contenidos o usuarios específicos. En todo caso, la SRO debe siempre especificar una fecha de finalización. Se deben establecer mecanismos de supervisión independientes para garantizar el cumplimiento de estos principios[64]
- Los operadores de redes móviles pueden desempeñar un papel importante en la concientización de los funcionarios de gobierno sobre el potencial impacto de una 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 misma, si fue aprobada por una autoridad judicial, si es válida y vinculante y si es apelable. También pueden trabajar con el gobierno para limitar el alcance y el impacto de la orden. Los procedimientos pueden incluir una orientación sobre cómo el personal local debe gestionar una SRO (por ejemplo, cómo escalar a representantes corporativos superiores)[65]

Primero y principal, toda decisión debe ser tomada teniendo en cuenta la seguridad de los clientes, las redes y el personal del operador móvil, con el objetivo de restablecer los servicios lo más rápidamente posible[66]

La GSMA y sus miembros se comprometen a trabajar con los gobiernos a fin de utilizar la tecnología como herramienta para mantener los dispositivos móviles fuera de áreas sensibles, 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 de largo plazo que no afecte negativamente a los usuarios legítimos ni a las inversiones sustanciales de los operadores móviles realizan para mejorar su cobertura.[67]

- Los inhibidores de señal deben utilizarse únicamente como último recurso o solamente implementarse en coordinación con los operadores de redes móviles con licencia local. Dicha coordinación debe continuar durante todo el proceso, para garantizar que se minimice la interferencia en áreas adyacentes y que los usuarios de dispositivos móviles legítimos no se vean afectados[68]
- Además, las autoridades regulatorias deben prohibir el uso de inhibidores de señal por parte de entidades privadas y establecer sanciones para aquellas que los utilicen o comercialicen sin permiso de autoridad correspondiente[69]
- La importación y venta de inhibidores o bloqueadores debe restringirse a aquellas personas habilitadas y autorizadas para hacerlo y su operación debe estar autorizada por el regulador nacional de telecomunicaciones
- Asimismo, fortalecer la seguridad en áreas sensibles, tales como las prisiones, para evitar el contrabando de dispositivos inalámbricos, es la medida más efectiva contra el uso ilegal de dispositivos móviles en las mismas, porque no afecta los derechos de los usuarios legítimos de servicios móviles que se encuentran en las inmediaciones[70]

62. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles: órdenes de restricción de servicios"
63. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles: órdenes de restricción de servicios"
64. Ibídem.
65. Ibídem.
66. Ibídem.
67. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles; inhibidores de señal"
68. Ibídem.
69. Ibídem.
70. Ibídem.

Análisis más profundo

Mitigación del impacto de las órdenes de restricción de servicio

En casos de emergencias, las autoridades del gobierno en algunos países tienen la facultad de exigir respuestas extremas a los operadores de redes, tales como la desconexión total o parcial de la red y/o de los servicios, durante un período de tiempo. Cuando se cita la seguridad nacional como el fundamento para dichas solicitudes, es muy posible 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 presentan 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 esta orden por escrito, citando la ley pertinente y firmada por autoridad competente, en la cual se indicaba que el incumplimiento podía redundar en sanciones. Luego, la orden fue publicada en un periódico panafricano. Las compañías cumplieron con esta orden, provocando así la suspensión de los servicios de SMS hasta el 24 de julio. Como resultado de este hecho, la compañía aprendió varias lecciones, como la importancia de la cooperación entre pares al responder a exigencias de gobierno que presentan irregularidades y que la transparencia puede ser una herramienta útil para una compañía al momento de responder a estas peticiones. (Diálogo de la Industria de Telecomunicaciones, 2016. “Aportes presentados al Relator de la ONU David Kaye”)

2) En AT&T, las solicitudes son evaluadas por empleados (incluidos los abogados de AT&T y, si fuese necesario, también el asesor legal local que esté familiarizado con la legislación aplicable) capacitados para confirmar si las solicitudes fueron debidamente emitidas por entidad competente, conforme a autoridad legal válida y en cumplimiento de los requerimientos aplicables. La compañía rechaza toda petición del gobierno que no cumpla con estos requisitos. Cuando corresponde, la compañía solicita una aclaración o modificación de la solicitud o presenta una objeción a la petición del gobierno o la orden judicial en la instancia correspondiente. Estos esfuerzos ayudan a minimizar el posible impacto de una solicitud 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) En 2015, la situación de seguridad en las operaciones de América Central de Millicom era todo un desafío. Desde el año anterior, las autoridades de Guatemala, El Salvador y Honduras habían aprobado leyes que obligaban a todos los operadores de telecomunicaciones a desconectar servicios o a reducir la capacidad de señal dentro y alrededor de las prisiones, porque las autoridades sospechaban que las pandillas criminales seguían operando desde el interior de las mismas mediante el uso de dispositivos móviles ingresados a las instalaciones en forma ilegal. En principio, se solicitó a los operadores de telecomunicaciones que desconectaran las torres de las radiobases, las cuales prestaban servicios a una extensa zona, 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 compañía trabajó en forma proactiva, tanto con las autoridades como con sus pares de la industria móvil, y se dedicó a buscar soluciones alternativas que pudieran resolver el problema sin afectar a la población que vive en las inmediaciones de las prisiones. Estas soluciones incluyeron varios aspectos, desde un nuevo diseño de cobertura de redes alrededor de las prisiones y soluciones de terceros de funcionamiento similar al de los bloqueadores para restringir las señales en una zona física específica hasta la reubicación de prisiones fuera de áreas densamente pobladas.

   Como resultado, a fines de 2015, todas las restricciones para señales de dispositivos móviles en 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

El tercer aspecto de seguridad pública que ha sido objeto de gran debate en los últimos años es el registro obligatorio de tarjetas SIM móviles prepagas, en virtud del cual se requiere a todos los usuarios que demuestren su identidad al momento de comprar una tarjeta de módulo de identificación del suscriptor [*Subscriber Identity Module, SIM*] prepaga o de 'pago por consumo' para utilizar servicios móviles.

Era práctica habitual que un operador de redes móviles,[71] en especial un nuevo entrante al mercado, ofreciera tarjetas SIM a potenciales clientes, a veces, literalmente regalándolas en una esquina. Luego, los clientes compraban crédito a través de un cupón prepago y utilizaban la tarjeta SIM y el número telefónico al que correspondía.

Varios gobiernos argumentaron que esta modalidad permite a los delincuentes aprovechar el anonimato para llevar a cabo diferentes actividades ilegales, como, por ejemplo, pedir un rescate después de un secuestro o planear un ataque terrorista. La percepción es que este anonimato hace más difícil rastrear el uso de la tarjeta SIM móvil a un usuario real. En respuesta, algunos gobiernos exigieron que los operadores de redes móviles lleven un registro de todos sus clientes, actuales y futuros.

Una vez implementadas, estas medidas tuvieron una serie de consecuencias no deseadas, incluyendo:

- La exclusión de usuarios, que no contaban con la documentación necesaria, del acceso a los servicios móviles, generalmente aquellos en condiciones más pobres y vulnerables. Dependiendo del país y de la disponibilidad de un documento de identidad estándar, esto puede ser un obstáculo importante[72]
- El aumento del robo de dispositivos móviles y el surgimiento de un mercado negro de tarjetas SIM registradas en forma fraudulenta o robadas,[73] originado por el deseo de algunos consumidores -incluidos los delincuentes- de mantener su anonimato
- Una mayor preocupación del consumidor en relación con el acceso, seguridad, uso y retención de sus datos personales, en particular ante la ausencia de leyes nacionales sobre privacidad y libertad de expresión[74]

Estudio de caso

Colaboración de la Industria

En 2012, la Comisión de Comunicaciones de Uganda [*Uganda Communications Commission*] anunció que los operadores de redes móviles debían bloquear todas las tarjetas SIM que no estuvieran registradas al término del plazo (final) del 31 de agosto de 2013.

En un esfuerzo por adelantarse a este plazo, los operadores de redes móviles Airtel y Warid lanzaron campañas innovadoras para motivar a más personas a registrarse. Además de enviar a sus clientes recordatorios por SMS del plazo de registro final, ofrecieron minutos y mensajes de texto gratis a quienes se registraran antes del mismo. Asimismo, ofrecieron a los consumidores la opción de un registro parcial, mediante el envío de un mensaje de texto con su número móvil no registrado a un número gratuito, para evitar la desactivación de su tarjeta SIM una vez que se cumpliera el plazo fijado. Esta opción de registro parcial permitió a los consumidores indicar que sus tarjetas SIM se encontraban activas y, por lo tanto, tuvieron más tiempo para registrarse en persona, aunque no hubieran cumplido con el plazo.
(GSMA, 2013. "El Registro Obligatorio de Usuarios de Tarjetas SIM Prepagas: A White Paper")

5

71. Dentro de 'Registro de Usuarios', los operadores de redes móviles incluyen a otros operadores que ofrecen servicios de comunicaciones inalámbricas sin ser propietarios de la red, tales como operadores de redes móviles virtuales [*Mobile Virtual Network Operators, MVNO*] u otros operadores móviles con licencia [*Other Licensed Operators, MOLO*]
72. GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice" [El registro obligatorio de tarjetas SIM prepagas: cómo enfrentar los desafíos a través de mejores prácticas]
73. GSMA, 2013. "The Mandatory Registration of Prepaid SIM Card Users" [El registro obligatorio de tarjetas SIM prepagas]
74. Ibídem.

Es cada vez mayor el número de gobiernos que han introducido el registro obligatorio de usuarios de tarjetas SIM prepagas, principalmente, como herramienta para combatir el terrorismo y mejorar la aplicación de la ley.[75] No obstante, a la fecha, no existe evidencia empírica de que dicho registro tenga un efecto directo en la reducción de los delitos.[76] A pesar de la ausencia de esta evidencia, varios gobiernos todavía creen que el registro obligatorio de tarjetas SIM ayudará en la lucha contra el delito y el terrorismo. Por lo general, cuando se impone la obligación de efectuar un registro de usuarios de tarjetas SIM prepagas, el costo de implementación se traslada a los operadores de redes móviles. Este costo puede ser considerable y afectar la capacidad de inversión de los operadores móviles en la provisión de servicios a aquellos clientes de menor ARPU. Algunos países, incluido el Reino Unido, analizaron[77] en detalle estos programas y concluyeron que los costos para la sociedad (en forma de cargas burocráticas y bases de datos de registro) superan los beneficios, por lo cual decidieron no adoptar esta política. Estas decisiones son de carácter nacional y dependen de las circunstancias de cada país, como también de los problemas que se procuran resolver con el registro.[78]

El lado positivo de estos registros es que facilitan el acceso del consumidor a servicios móviles y digitales de valor agregado, tales 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 creen resultados valiosos para los mismos, 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 estos beneficios ni resultados positivos depende del mandato obligatorio de registro de tarjetas SIM que pueda emitir un gobierno. Por el contrario, esos resultados se pueden obtener a través del registro voluntario del cliente, quien decide hacerlo a fin de tener acceso a servicios que considera valiosos, tales como los servicios de dinero o comercio móvil o de gobierno electrónico. No obstante, el registro voluntario está sujeto a que el consumidor tenga acceso a un documento para comprobar su identidad.

Estudio de caso

Alternativas al registro — México

Con el objetivo de combatir la actividad criminal, México introdujo el registo obligatorio de tarjetas SIM ('RENAUT') en el año 2009.

Al momento de entrar en vigencia el 'RENAUT', la privacidad y la seguridad de datos eran temas de preocupación constante y los problemas de registrar, en un plazo de implementación muy breve, a gran parte de la población que no contaba con un documento de identificación oficial eran cuestiones serias. Esta solución tampoco pudo combatir la actividad criminal y, como resultado, incrementó el robo de equipos.

Luego de consultas a la industria, la academia y las ONG, el programa de registro RENAUT cesó sus operaciones en el año 2012. La base de datos fue desactivada y se dio por perdida la importante inversión financiera realizada por los operadores de redes 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 reglamentarias, no exige que el usuario proporcione detalles de registro para utilizar los servicios prepagos. Por el contrario, la ley potencia las diferentes obligaciones de los operadores de redes móviles (por ejemplo, interceptación legítima) para ayudar al gobierno y a los servicios de seguridad a combatir la actividad criminal. (GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice" [El registro obligatorio de tarjetas SIM prepagas: cómo enfrentar los desafíos a través de mejores prácticas])

75. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones: Registro obligatorio de tarjetas SIM de prepago"
76. GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice" [El registro obligatorio de tarjetas SIM prepagas: cómo enfrentar los desafíos a través de mejores prácticas]
77. Lord West de Spithead, en respuesta a una 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
78. GSMA, 2016. "Mandatory Registration of Prepaid SIM Cards: Addressing challenges through best practice" [El registro obligatorio de tarjetas SIM prepagas: cómo enfrentar los desafíos a través de mejores prácticas]

Cuando el registro de tarjetas SIM es obligatorio, se debe notificar a los clientes existentes la necesidad de registrarlas, el procedimiento correspondiente y las consecuencias de no hacerlo (por ejemplo, la posible desactivación de la tarjeta SIM en caso de no registrarse). 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 de mercado local relevantes podemos mencionar si el acceso de los ciudadanos a un documento de identidad nacional es común en todo el país, si el gobierno mantiene registros exhaustivos de 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 el gobierno, la industria y otros interesados relevantes

Si bien el registro de usuarios de tarjetas SIM prepagas podría ofrecer valiosos beneficios a los ciudadanos y consumidores, no debe ser obligatorio. Si se toma la decisión de exigir su implementación, el gobierno debe tener en cuenta las mejores prácticas internacionales y ofrecer mecanismos de registro flexibles, proporcionales y relevantes a su mercado, incluyendo el nivel de penetración de documentación de identidad oficial en el mismo.[79]

Si se cumplen estas condiciones, serán más altas las probabilidades de que este ejercicio de registrar 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 usuarios puede facilitar la creación de soluciones de identidad digital por parte de los operadores de redes móviles, las cuales empoderarán a sus clientes para tener acceso a una variedad de servicios móviles y no móviles. Dado el gran tamaño de las bases de clientes existentes en todos los países, se debe considerar cuidadosamente 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 la introducción o revisión de un 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 la seguridad nacional y la protección de los derechos de los ciudadanos, en particular en aquellos casos en que el gobierno exija el registro de tarjetas SIM por motivos de seguridad
- Procurar que existan garantías de seguridad adecuadas y una supervisión legal efectiva para proteger los datos y la privacidad del cliente
- Fijar plazos realistas para los procesos de diseño, prueba e implementación del registro
- Brindar certeza y claridad sobre los requisitos de registro antes de su implementación
- Permitir y/o incentivar el almacenamiento de registros electrónicos y el diseño de procesos de registro 'livianos' desde el punto de vista administrativo
- Permitir y/o invitar a los clientes que ya tengan su 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

79. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones: Registro obligatorio de tarjetas SIM de prepago"

Análisis más profundo

Asociaciones público-privadas para registro en América Latina

Durante 2009, en Ecuador, y en 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 codo a codo con el gobierno para implementar 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" [*Interactive Voice Response* o *IVR*, por sus siglas en inglés]. La mejora respecto del procedimiento anterior que ofreció este servicio fue la verificación cruzada de la identidad del consumidor con el Registro Civil.

En Argentina, Telefónica desarrolló una aplicación que se activa al insertar la tarjeta SIM en el dispositivo móvil. Esta aplicación recolecta la información de la tarjeta SIM, además de la identificación personal del usuario móvil. Este sistema digital se está utilizando para crear una base de datos que captura el vínculo único entre el propietario y la tarjeta SIM y entre la tarjeta SIM del dispositivo móvil y el mismo dispositivo.

Gracias a estas experiencias de trabajo en colaboración con las autoridades nacionales correspondientes, Telefónica aprendió las siguientes tres lecciones claves:

1. Existen varias formas de validar el proceso de registro de tarjetas SIM y cada operador de redes móviles debe desarrollar la que considere más apropiada
2. Contar con un cronograma es esencial para lograr una implementación exitosa. Por ejemplo, en Ecuador, los operadores de redes móviles y el regulador trabajaron juntos 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 satisface las necesidades de todos los interesados en forma equilibrada, se deben considerar las asociaciones público-privadas cerradas y la colaboración entre operadores de redes móviles y el gobierno

5

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

La seguridad de la infraestructura de redes es lo que sustenta el uso seguro de los servicios móviles. En su sentido más simple, esto significa que los operadores de redes móviles protegen la integridad de las comunicaciones en toda la red mediante la salvaguarda de los activos críticos (hardware, software y datos) y la prevención de la intrusión o acceso no autorizado a todo nodo o vínculo que forme parte de sus redes. Dado que el dispositivo móvil del usuario final es el primer punto de acceso a la red desde la perspectiva del usuario, proteger su integridad se convirtió recientemente en un requerimiento crítico. 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. Asimismo, estas redes de comunicaciones 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. Por lo tanto, en la práctica, proteger las redes y los dispositivos es sumamente complejo.

En un principio, la infraestructura de redes de telecomunicaciones estaba diseñada como un sistema seguro de circuito cerrado. En el punto en el que había interconexión de redes, como era el caso de las fronteras entre países (por lo general, los primeros operadores de redes en la mayoría de los países eran monopolios nacionales estatales), se realizaba la implementación en base a una relación transparente, bilateral y confiable. Desde entonces, estas mismas redes se han multiplicado y han evolucionado dado que el mundo está cada vez más interconectado y la tecnología continúa avanzando. En la actualidad, lo más probable es que cualquier llamada telefónica o transmisión de datos atraviese muchas redes y, en el caso de los datos, que una misma comunicación tome múltiples rutas. Como resultado, han surgido una gran variedad de posibles vulnerabilidades, que requieren que todos los operadores de redes y el ecosistema de la industria más amplio se mantengan alertas y den una respuesta.

La Figura 6 presenta un resumen de las amenazas que tienen el potencial de afectar la integridad de las redes al permitir la interceptación, la suplantación de identidad o la interrupción del servicio no autorizados. La principal respuesta de la industria móvil ante estas amenazas ha sido optimizar la solidez y salud de la seguridad, promover el debate transparente sobre el equilibrio entre la conveniencia y la seguridad e incorporar en las normas y protocolos técnicos funcionalidades de seguridad cada vez más sofisticadas, a medida que se desarrolla e implementa cada nueva generación de redes móviles.

Esta parte del reporte se dedica a las cuestiones de seguridad que afectan a las redes y los dispositivos y que tienen el potencial de poner en peligro la seguridad necesaria para mantener la salvaguarda y protección de las comunicaciones del cliente:

- Seguridad de la red
- Integridad de los dispositivos móviles
- Futuros desarrollos de la red

Cada una de estas cuestiones tiene una serie de implicancias importantes para el gobierno, la industria y demás interesados, que también se describen más adelante en este capítulo.

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

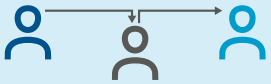
Los actores de la industria deben trabajar codo a codo y en forma coordinada con los organismos internacionales de seguridad para compartir inteligencia sobre amenazas a fin de responder a ataques maliciosos en las redes y dispositivos móviles e identificar a los autores. Esto se puede lograr con la participación de los equipos de respuesta ante incidentes de seguridad y la creación de nuevos equipos, si fuese necesario, para resolver cualquier deficiencia. Cuando sea necesario, la regulación debe aplicarse de manera consistente a todos los proveedores de la cadena de valor, en forma neutral respecto de los servicios y la tecnología, preservando al mismo tiempo el modelo de gobernanza de internet de múltiples interesados y permitiendo su evolución. Con esto en mente, la GSMA y sus operadores móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas para proteger la infraestructura subyacente y asegurar que se provee 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 público-privadas para minimizar el riesgo de *hackeo* o uso de la red para fines maliciosos a través de estrategias globales y coordinadas**
- **Ser claros sobre qué parte de la infraestructura es responsabilidad del operador y dónde se encuentra la demarcación con otros servicios o infraestructura**

Figure 6

Protección de redes

OBJETO DE LA PROTECCIÓN	DESCRIPCIÓN DE LA AMENAZA	POSIBLE ATAQUE
INTEGRIDAD – EVITAR LA ALTERACIÓN DE LOS DATOS	ADULTERACIÓN NO AUTORIZADA	ATAQUE POR INTERCEPTACIÓN 
CONFIDENCIALIDAD – MANTENER LA PRIVACIDAD DE LOS DATOS	ACCESO NO AUTORIZADO	ESCUCHAS 
DISPONIBILIDAD – MANTENER LA DISPONIBILIDAD DE LA RED Y LOS DATOS PARA LOS USUARIOS LEGÍTIMOS	DESTRUCCIÓN, ROBO, ELIMINACIÓN O PÉRDIDA DE DATOS O REDES NO DISPONIBLES	DENEGACIÓN DE SERVICIO 

6

Seguridad de la red

Infraestructura física de la red

La seguridad de las redes móviles empieza con su misma infraestructura física, incluyendo las torres celulares, la red de transmisión de retorno [*backhaul*] y activos de la red central. Por ejemplo, en toda red existen funciones primordiales, tales 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 vendedores de equipos continúan desarrollando e implementando nuevas soluciones a fin de que estas funciones sean más robustas (con éxito hasta la fecha), pero esto requiere de inversión constante en el desarrollo e implementación de nuevas funciones y prestaciones.

El uso de radiobases móviles falsas o captadores de IMSI [*International Mobile Subscriber Identity*, identidad internacional de suscriptor móvil], es una vulnerabilidad causada por la ausencia de autenticación mutua en las tecnologías 2G. Esta funcionalidad puede cambiar la configuración de los dispositivos 3G y 4G, en forma automática, para que utilicen una red 2G. La radiobase falsa engaña a los dispositivos móviles a su alcance para que se conecten a ella en vez de a la red real, a la que el operador de la radiobase falsa retransmite la llamada. Este ataque de "intermediario" [*man in the middle*] crea una serie de vulnerabilidades, tales como interceptación, rastreo de ubicación, denegación de servicio y fraudes. En la actualidad, los formuladores de políticas, como el Comité de Supervisión y Reforma de Gobierno de EE.UU., se encuentran en el proceso de elaborar recomendaciones sobre la protección del uso no autorizado de estos dispositivos.[80] Los operadores de redes móviles pueden implementar medidas estándares de redes y seguridad para ayudar a mitigar este riesgo y la GSMA desarrolló directrices para colaborar con ellos.

Comunicaciones a través de las redes

La actualización de la tecnología utilizada en las redes móviles se realiza en forma periódica; las mejoras más nuevas son implementadas conforme a un plan determinado. El alto nivel de inversiones continuas en nueva infraestructura ha tenido un papel preponderante en garantizar que la infraestructura de redes sea todo lo robusta posible, dentro de lo razonable. 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 cuya regla es el cambio constante.

En 1991, el lanzamiento de redes de segunda generación (2G) introdujo el uso de la modulación digital, la cual hizo posible la implementación de protección y seguridad más robustas. El estándar GSM, que sustenta a un gran número de redes 2G, utiliza la tecnología SIM [módulo de identidad del suscriptor] para autenticar a un usuario para fines de identificación y facturación, como también para soportar la encriptación del dispositivo a modo de protección contra ataques, tales como la interceptación. El concepto de SIM física, basado en la tecnología de tarjetas inteligentes, demostró ser excepcionalmente fuerte y sigue siendo un componente crítico de las redes 4G actuales. Esto continuará en el futuro a través de innovaciones como la *embedded-SIM*.[81]

Si bien, en principio, las redes 2G fueron diseñadas para soportar comunicaciones de llamadas de voz, contaban también con capacidades de transmisión de datos básicas y, además, introdujeron el popular servicio de mensajería de texto SMS. Las redes 3G, lanzadas a comienzos de la década del 2000, fueron las primeras en incorporar la transmisión de datos como capacidad central, introduciendo la integración de multimedios y la navegación en la web a velocidades casi similares a los de la banda ancha, además de incorporar capacidades adicionales de seguridad.

80. Committee on Oversight and Government Reform, 2016. "Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations" [Comité de supervisión y reforma gubernamental, 2016 "Utilización de tecnología de simulación de celdas celulares por parte de organismos de seguridad: cuestiones y recomendaciones sobre privacidad]

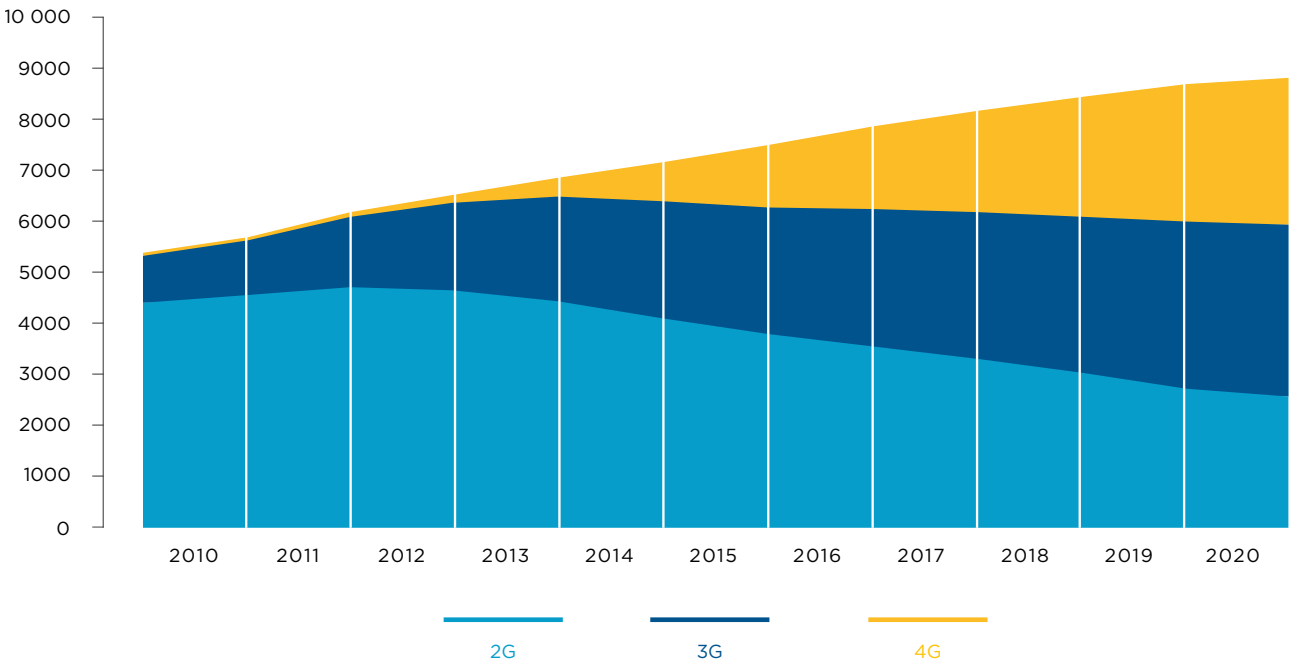
81. La *embedded-SIM* es un chip incluido en los dispositivos móviles que ofrece el mismo nivel de seguridad que la tecnología SIM actual. Brinda flexibilidad adicional al permitir la descarga de los perfiles de los operadores, de forma tal que los usuarios pueden cambiar de proveedor sin necesidad de cambiar el chip físico. Esto es particularmente relevante para los dispositivos máquina a máquina (M2M). Consultar: http://www.gsma.com/newsroom/press-release/leading-m2m-alliances-back-the-gsma-embedded-sim/

Sin embargo, las debilidades relacionadas con seguridad que presenta el protocolo Sistema de Señalización por canal común Número 7 [*Signalling System Number 7, SS7*] definido por la UIT, junto con otros protocolos de interconexión que se utilizan para enrutar llamadas de voz y soportar servicios entre redes y a través de las mismas, puede exponer a las redes móviles y a sus clientes a diferentes vulnerabilidades, tales como escuchas, rastreo de ubicación o interceptación de datos. El objetivo de las actuales funciones de monitoreo, detección y bloqueo es mitigar todas las amenazas a las que están expuestos los protocolos de interconexión y la mensajería. La GSMA reconoce la necesidad de que los operadores de redes móviles ofrezcan una respuesta integral y colectiva a fin de mitigar estos riesgos. El Grupo de Seguridad y Fraude de la GSMA encaró un importante trabajo para brindar asesoramiento a los operadores de redes sobre cómo mitigar los riesgos de seguridad que presenta el protocolo SS7.[82] Asimismo, los operadores deben tomar todas las precauciones de protección necesarias contra la interceptación de datos sensibles, incluyendo los detalles sobre las credenciales de sus suscriptores.

La cuarta generación de estándares de comunicaciones móviles (4G) ofrece acceso de banda ancha móvil de alta velocidad para *smartphones* y otros dispositivos. La adopción de redes inalámbricas 4G (ver Figura 7) introdujo el cambio total a tecnología IP [*Internet Protocol*, Protocolo de Internet], resolviendo así la vulnerabilidad planteada por el SS7, una vez que el protocolo IP es implementado por ambos operadores. No obstante, esta misma adopción de un nuevo protocolo crea nuevos desafíos en cuanto a la seguridad. Se puede minimizar la explotación de las vulnerabilidades de estas redes mediante la correcta implementación y configuración de las capacidades de seguridad inherentes a los estándares. La GSMA ofrece asesoramiento sobre cómo lograrlo de la mejor manera.

Figura 7

Conexiones internacionales por tecnología (en millones, no incluye M2M)



82. Para más información, consultar: http://www.gsma.com/newsroom/all-documents/ir-70-sms-ss7-fraud/

Uno de los desafíos más frecuentes de las comunicaciones es el de los gateways GSM o "*SIM Boxes*", como se los denomina habitualmente. Un *gateway GSM* permite que terceros no autorizados interfieran con el enrutamiento de llamadas hacia redes móviles y sus clientes, generando así una preocupación en cuanto a su seguridad y protección. Por lo general, dado que los *gateways GSM* no soportan la funcionalidad de identificación de llamada *calling line identity* o *CLI*, por sus siglas en inglés, los servicios que de ella dependen, no están disponibles para los usuarios hacia quienes los *gateways GSM* enrutan el tráfico (por ejemplo, se puede denegar el servicio a un usuario de servicios prepagos que debe recargar su crédito). La ausencia de CLI también puede tener implicancias para la interceptación legítima y las obligaciones legales de los operadores de redes a fin de apoyar a los organismos de seguridad en los mercados en los que cuentan con licencia para operar. Debido al impacto en la disponibilidad de los servicios y en la seguridad general, el uso de *gateways GSM* es ilegal en algunos mercados. En los casos en los que están permitidos, se alienta a los operadores de redes móviles a implementar medidas para evitar su uso por parte de terceros operadores.

Si bien los operadores de redes móviles continúan mitigando los riesgos de sus redes y consumidores, cabe destacar que lo mismo debería esperarse de los operadores de redes inalámbricas públicas, tales como los 'puntos de acceso Wi-Fi' (*hotspots*) o conexiones Wi-Fi de los hoteles. Los operadores de estas redes y sus clientes deberían implementar la protección adecuada (por ejemplo, redes privadas virtuales) para ayudar a garantizar la seguridad del ecosistema de comunicaciones más amplio.

Implicancias clave para el gobierno, la industria y otros interesados relevantes

Si bien no se puede garantizar que una tecnología de seguridad sea infalible, los ataques a las redes y los servicios GSM no son frecuentes, dado que la mayoría requeriría considerables recursos, desde equipos especializados y capacidad de procesamiento computacional ingente hasta conocimientos técnicos que exceden las habilidades de la mayoría de las personas u organizaciones.[83]

Las barreras para realizar concesiones respecto de la seguridad móvil han sido muy altas y la GSMA considera que las investigaciones que describen las posibles vulnerabilidades, en general, han sido principalmente de naturaleza académica.[84] No obstante, el panorama de la tecnología en constante evolución, y el surgimiento de nuevas amenazas y fuentes de ataque, requieren que la industria adopte un enfoque aún más proactivo a fin de proteger las redes en el futuro:

- Es importante que la industria móvil asegure la implementación de adecuados mecanismos, herramientas y oportunidades para facilitar el intercambio de información sobre amenazas y ataques y asegurar la divulgación inmediata de la información en respuesta a incidentes. Esta iniciativa podría incluir a reguladores u otras autoridades de gobierno, tales como los Equipos de Respuesta ante Emergencias Informáticas [*Computer Emergency Response Teams, CERT*] nacionales.
- 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 como también del 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 la instalación 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 la definición de los requerimientos básicos de seguridad para su adopción por parte de todos los operadores de redes móviles
- Si bien el constante desafío que representa la seguridad será aún mayor con la evolución a la tecnología 5G, también constituirá una oportunidad de reconsiderar el concepto de seguridad y la forma en que se la puede proveer

Cuando se necesita aplicar una regulación, se debe hacerlo de manera igualitaria para 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 interesados y permitiendo su evolución.

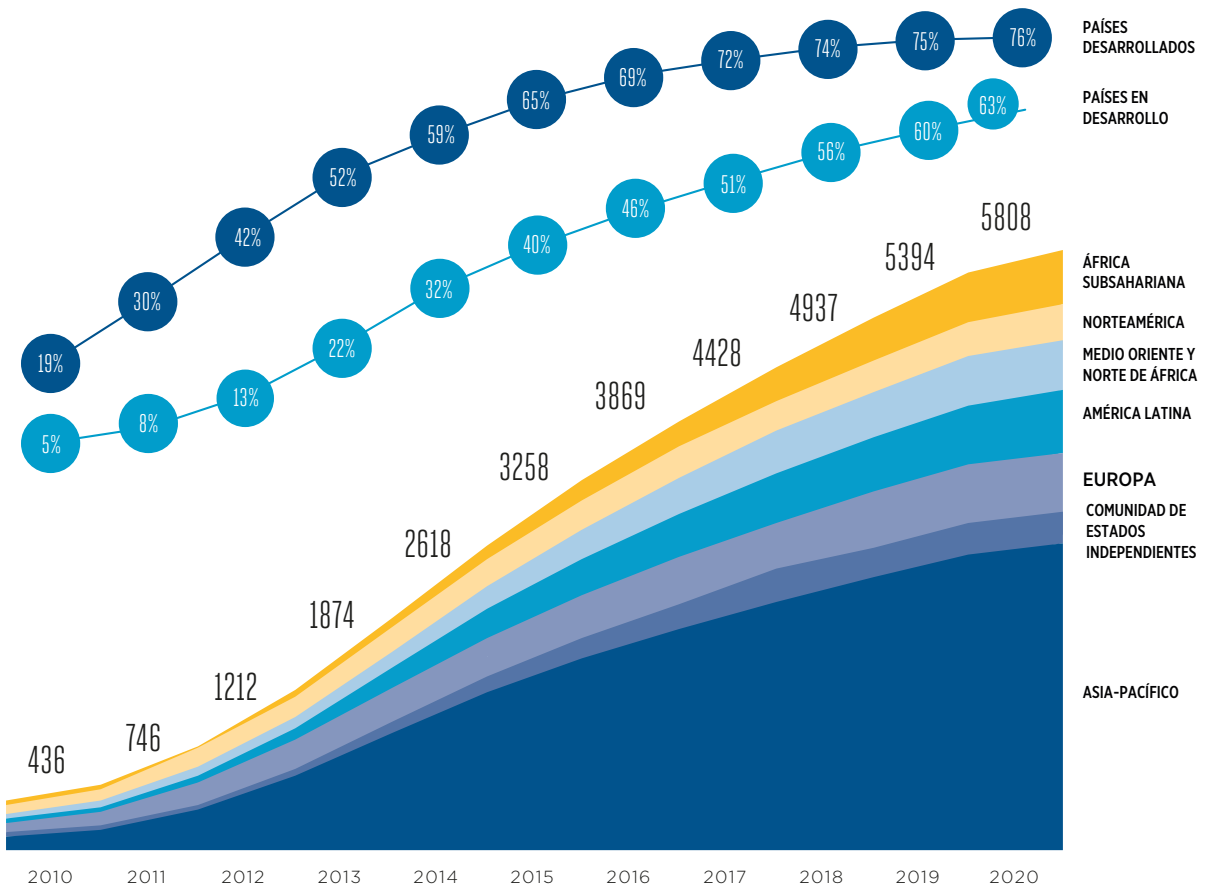
83. GSMA, 2016 "Manual de políticas públicas de telecomunicaciones móviles: Seguridad móvil"
84. Ibídem.

Integridad de los dispositivos móviles

A medida que se implementan las redes 3G, 4G y, en el futuro, 5G, aumenta la adopción y el uso de dispositivos móviles tales como los *smartphones*. Se espera que para el año 2020, dos de cada tres conexiones, en mercados emergentes, y tres de cada cuatro, en mercados desarrollados, se realicen desde un *smartphone* (ver Figura 8). Los proveedores de aplicaciones están analizando cómo un *smartphone*, quizás con un módulo *plug-in*, puede reemplazar a un dispositivo dedicado, en puntos de conexión (*hotspots*) y otros entornos altamente sensibles. Además, para el año 2020 se esperan, por lo menos, mil millones de conexiones máquina a máquina (M2M), lo cual tendrá un impacto en los hogares, las fábricas, el transporte,

Figura 8

Conexiones y adopción a nivel global de *smartphones* (en millones)



85. GSMA, 2014. "Cellular M2M forecast and assumptions: 2010-2020" [Proyecciones de M2M celulares y supuestos correspondientes, 2010-2020]

etc., y representará, por lo menos, 10% del mercado móvil mundial.[85]

Para el consumidor y la empresa, la oportunidad de utilizar estos servicios conlleva también el riesgo de que una gestión inadecuada de los dispositivos pueda crear 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 una variedad de motivos. Al ser un artículo atractivo para los ladrones (debido a su valor relativamente alto y su tamaño reducido), el crimen organizado intenta cambiar el número de IMEI[86] del dispositivo móvil robado para poder reactivarlo luego de haber sido reportado como robado. Otros criminales utilizan software malicioso para ejecutar funciones que causan un daño al usuario, por lo general, debido al robo de identidad y fraudes relacionados.[87]

Quizás la amenaza más grave sea un ataque premeditado y sistemático de gran escala, diseñado para dejar inoperable toda la red y afectar a todos los usuarios. Se corre el riesgo de que las violaciones a los dispositivos móviles (por ejemplo, a través de software malicioso enviado a través de correos electrónicos de *phishing*) se utilicen como punto de entrada para propagarse a otros dispositivos conectados y luego atacar otras redes basadas en IP. Por ejemplo: el ataque al importante controlador de infraestructura del sistema de nombres de dominio, Dyn,[88] llevado a cabo el 21 de octubre de 2016, se originó en un software malicioso de una computadora, que luego se propagó a otros dispositivos, creando así el botnet que eventualmente fue utilizado para realizar un ataque DDoS (*Distributed Denial of Service*, denegación de servicio distribuido).[89] A una escala aún 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 los organismos de seguridad, como parte de un plan de seguridad global, porque atacar las redes móviles es solo una de las posibles vías de ofensiva utilizadas por terceros hostiles

La GSMA colaboró en el desarrollo de mecanismos de protección, tales como los descritos en las "Directrices para la eficiencia en la conexión del Internet de la Cosas" [*IoT Connection Efficiency Guidelines*][90] de la GSMA destinados a proteger las redes móviles de la implementación masiva de dispositivos IoT ineficientes, inseguros o defectuosos. Además, la GSMA alienta a sus miembros a implementar parches críticos de seguridad de dispositivos tan rápido como sea razonablemente posible.

Implicancias clave para el gobierno, la industria y otros interesados relevantes

Es esencial que los proveedores de la industria adopten buenas prácticas y políticas de seguridad. Programas tales como el "Esquema de acreditación de seguridad" de la GSMA [*Security Accreditation Scheme*][91], ofrecen una certificación de proveedores, aseguran que se promueva y se pueda demostrar el compromiso con los niveles de seguridad. Durante un tiempo, la GSMA se encargó de garantizar la seguridad de los proveedores y sus productos a través del "Esquema de acreditación de seguridad" para proveedores de tarjetas SIM y el desarrollo actual del programa para fabricantes de equipos originales [*original equipment manufacturers, OEM*] de infraestructura.

Además, la GSMA intenta 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 la tarjeta SIM, como alternativa a la incorporación de la seguridad en el propiol dispositivo móvil o en una tarjeta digital externa (microSD), dado que la tarjeta SIM demostró su resiliencia ante ataques.[92]

86. En la Sección 3 se analizan en mayor detalle el IMEI y los problemas relacionados con el robo de dispositivos móviles. Protección del consumidor.
87. Estas cuestiones se analizan en mayor detalle en el capítulo "Protección del consumidor."
88. Dyn es un proveedor de sistemas de nombres de dominio [domain name system, DSN] para proveedores de servicios de internet, incluidos Twitter, Amazon, AirBnB y Spotify. La organización pudo restablecer sus servicios después de cada ataque, evitando una caída de todo el sistema, y mitigar un tercer ataque sin impacto para el consumidor. Para acceder la declaración pública, ver: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
89. USA Today, 2016. "Hacked home device caused massive Internet outage" [El *hackeo* de un dispositivo del hogar causa una caída masiva de internet]
90. Para más información, consultar: http://www.gsma.com/iot/wp-content/uploads/2016/11/TS.34_v4.0.pdf
91. Para más información, consultar: http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
92. GSMA, 2016 "Manual de políticas públicas de telecomunicaciones móviles: Seguridad móvil"

Desarrollos futuros de la red

El Internet de las Cosas (*Internet of Things*, IoT) es un conjunto ingente de desarrollos que incluye la conexión a internet de una gran variedad de nuevos dispositivos, desde automóviles hasta electrodomésticos. Estos dispositivos se conectarán a diferentes redes, incluyendo redes Wi-Fi, redes dedicadas de baja potencia y redes móviles, utilizando espectro con y sin licencia. La próxima generación de tecnología de redes, por ejemplo, virtualización de funciones de red y 5G, proporcionará parte de la conectividad necesaria para IoT, abrirá las puertas a una era de banda ancha móvil aún más rápida y allanará el camino para los servicios 5G optimizados, los cuales podrán incluir soporte para tecnologías de vanguardia, tales como el internet táctil, la realidad virtual y servicios de radiodifusión más avanzados.

Seguridad en el Internet de las Cosas (IoT)

El IoT presenta enormes oportunidades de crecimiento tanto para la industria móvil como para muchas otras industrias. Con la llegada de nuevos socios comerciales y nuevos proveedores de equipos, es esencial que la seguridad sea la prioridad para quienes ingresan al espacio comercial. La mayoría de los dispositivos y equipos que antes no se conectaban a ningún tipo de red, ahora deben ser diseñados con las protecciones de seguridad adecuadas, las cuales deben ser incorporadas al equipo y servicio desde su concepción. Eso exigirá a los proveedores y desarrolladores, que nunca antes habían tenido que considerar esos temas, que incluyan una seguridad robusta y sofisticada en un corto tiempo. La GSMA elaboró directrices de seguridad para el IoT[93], junto con un sistema de autoevaluación de seguridad[94] para los diversos actores del ecosistema.

Los estándares y protocolos para 5G, incluidos los relacionados con la seguridad de redes, se están elaborando específicamente para esta tecnología. La GSMA desempeña un rol protagónico en captar y priorizar los requerimientos, como también en velar por su consideración e incorporación a los nuevos estándares. Sin embargo, este esfuerzo aislado se enfoca en un único vínculo dentro del futuro IoT y es necesario dedicar grandes esfuerzos y atención a fin de garantizar la seguridad de los demás componentes y servicios que se encuentran dentro de la infraestructura altamente interconectada que formará parte del IoT a medida que continúa evolucionando.

Implicancias clave para el gobierno, la industria y otros interesados relevantes

El objetivo de la GSMA es desempeñar un importante papel para ayudar a delinear el desarrollo estratégico, comercial y regulatorio del IoT, así como del ecosistema 5G.[95]

- La GSMA reconoce que es clave su rol en reunir y priorizar los requerimientos para la normalización de la seguridad de la tecnología 5G. Ya se están llevando a cabo debates y la GSMA y sus miembros invitan a otros expertos en la materia y a organismos de seguridad a participar para asegurar que se comprendan bien todas las necesidades
- El gobierno debe apoyar la naturaleza global de los futuros mercados de redes y la amplia variedad de servicios que se conectarán al internet en el futuro, como también trabajar a nivel interjurisdiccional para asegurar la consistencia y claridad en las obligaciones establecidas en la regulación con relación a la seguridad de redes para todos los actores que participen en esta compleja área de rápida evolución
- La industria móvil continuará participando en el ecosistema más amplio y promoverá las inversiones correspondientes, ya sea en forma directa o a través de proveedores y socios del ecosistema, a fin de garantizar la seguridad de las redes y los dispositivos a medida que se desarrolla la tecnología, en especial en relación con la transición hacia la virtualización de funciones de red y 5G

6

93. Para más información sobre las "Directrices de seguridad para el IoT" de la GSMA, consultar http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
94. Para más información sobre el "Esquema de autoevaluación de seguridad de IoT" de la GSMA, consultar http://www.gsma.com/connectedliving/iot-security-self-assessment/
95. GSMA, 2016. "Manual de políticas públicas de telecomunicaciones móviles: 5G — El camino hacia la siguiente generación"

6

7 Principios de seguridad, privacidad y protección de la industria móvil

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

La GSMA y sus organizaciones miembros establecieron los siguientes principios, que brindan orientación sobre cómo continuar desarrollando soluciones para las cuestiones planteadas en este reporte.

Protección del Consumidor

Para promover el uso seguro y responsable de los servicios y dispositivos móviles en línea, es necesario contar con el esfuerzo de las múltiples partes interesadas. En particular, los gobiernos y sus organismos de seguridad deben garantizar la existencia de marcos legales, recursos y procesos adecuados para impedir, identificar y sancionar conductas delictivas. A menudo, esto requerirá de la cooperación global. Asimismo, otros actores del ecosistema de la industria, como fabricantes de dispositivos y proveedores de servicios móviles, deberían participar en las iniciativas destinadas a proteger al consumidor en relación al uso de servicios y dispositivos móviles y educarlos sobre conductas seguras y buenas prácticas para que puedan continuar aprovechando estos servicios en forma segura. Los operadores juegan un papel clave en recordarle al consumidor que debe mantenerse consciente y alerta, además de 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 móviles o facilitadas por estos, mediante los siguientes esfuerzos:

- **Trabajar en colaboración con otros organismos en pos de encontrar soluciones multilaterales adecuadas**
- **Implementar soluciones diseñadas con el objeto 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**
- **Enseñarle al consumidor 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 se mantienen protegidos de forma adecuada y conforme con las reglamentaciones y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia a través de 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 responsables de gobierno digital que se encuentren alineadas con las reglamentaciones locales. 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 recolectan y cómo se utilizan, mediante la implementación de políticas tales como:

- **Almacenamiento y tratamiento seguro de toda información personal y privada, conforme a los requisitos legales, cuando corresponda**
- **Transparencia con el consumidor sobre qué datos se comparten en forma anonimizada y el pleno cumplimiento con los requisitos 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 los organismos de seguridad, conforme a las leyes y reglamentaciones, las obligaciones contenidas en las licencias y la legislación local. Es importante que el gobierno garantice la existencia de un marco legal adecuado que describa claramente las facultades de los organismos nacionales de seguridad. Asimismo, este marco debe garantizar 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 con toda obligación, establecida por ley o por sus licencias, relacionada con temas de protección o seguridad pública en los países en los que operan, a la vez que cumplen con los principios de derechos humanos. Los operadores colaborarán con los organismos de seguridad pertinentes para proteger la seguridad pública mediante las siguientes acciones:

- **Trabajar con los organismos pertinentes cuando la situación particular así lo requiera, a fin de desarrollar e implementar soluciones adecuadas para alcanzar el objetivo final con el mínimo trastorno al consumidor y los servicios críticos**
- **Construir redes que tengan la funcionalidad de enfrentar situaciones de emergencia y seguridad, cuando corresponda**
- **Ser claros sobre las limitaciones de las acciones que se pueden tomar en relación con 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 codo a codo y en forma coordinada con los organismos internacionales de seguridad para compartir inteligencia sobre amenazas a fin de responder a ataques maliciosos en las redes y dispositivos móviles e identificar a los autores. Esto se puede lograr con la participación de los equipos de respuesta ante incidentes de seguridad y la creación de nuevos equipos, si fuese necesario, para resolver cualquier deficiencia. Cuando sea necesario, la regulación debe aplicarse de manera consistente a todos los proveedores de la cadena de valor, en forma neutral 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 móviles miembros acordaron el siguiente principio:

Los operadores tomarán medidas para proteger la infraestructura subyacente y asegurar que se provee 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 público-privadas para minimizar el riesgo de *hackeo* o uso de la red para fines maliciosos a través de estrategias globales y coordinadas**
- **Ser claros sobre qué parte de la infraestructura es responsabilidad del operador y dónde se encuentra la demarcación con otros servicios o infraestructura**

7

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

GSMA LATAM
Av. Del Libertador 6810,
piso 15
Buenos Aires, C1429BMO,
Argentina
Tel: +54 (11) 5367 5400