Seguridad y privacidad en las redes móviles

Desafíos, propuestas y consideraciones para los gobiernos

Acerca de la GSMA

La GSMA representa los intereses de los operadores móviles de todo el mundo, reuniendo a casi 800 operadores con más de 300 compañías del amplio ecosistema móvil. Estas empresas incluyen fabricantes de teléfonos y dispositivos, 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 corporativo de la GSMA en www.gsma.com.
Siga a la GSMA en Twitter: @GSMA.

GSMA Latin America es el brazo de la GSMA en la región. Para más información en inglés, español y portugués ver www.gsmala.com.
Siga a GSMA Latin America en Twitter: @GSMALatam.

Contenido

Introducción

Los operadores de redes móviles enfrentan el permanente desafío de brindar a los usuarios una experiencia móvil segura, cumpliendo al mismo tiempo con las obligaciones de proteger la seguridad pública. 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 y por ser su objetivo las comunicaciones en general y no sólo las de un dispositivo móvil, las soluciones deben tener una visión integral.

Lógicamente, los gobiernos y los hacedores de políticas públicas desean prevenir este tipo de incidentes y proteger a los ciudadanos en la mayor medida de lo posible. Sin embargo, en un entorno tan complejo, 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 se 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 interceptarlas para proteger el bien público. Además, se debe tener en cuenta la naturaleza compleja y multipartita de muchos de estos servicios.

La industria móvil invierte esfuerzos e importantes sumas de dinero para permitir un uso seguro de sus servicios y proteger la privacidad de los usuarios. Con cada iteración tecnológica adicional, se introdujeron nuevas medidas, 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.

No obstante, la tecnología por sí sola no es suficiente. Es esencial dar una respuesta holística en la que participen todas las partes interesadas e involucradas, gobiernos, otros organismos y organizaciones no gubernamentales, además de los proveedores finales de los servicios proporcionados en línea.

Resumen Ejecutivo

A pesar de ser dos temas amplios, el abordaje de la seguridad y la privacidad puede delimitarse en cuatro pilares, agrupados en dos categorías:

Seguridad del usuario

1. Uso de los dispositivos móviles
Protección de la integridad física en su uso

2. Los datos y la privacidad
Protección de la privacidad del individuo, a través del almacenamiento seguro de sus datos

Seguridad del entorno

3. La seguridad pública
Rol y responsabilidades de los operadores móviles respecto de su colaboración con las agencias de gobierno para proteger al público.

4. Seguridad de las redes e integridad de los dispositivos
Garantizar la integridad y seguridad de la infraestructura de redes móviles y de los dispositivos.

Ninguna de estas cuestiones multidimensionales puede resolverse de manera simple ni mediante las acciones aisladas de una organización o un sector. A fin de obtener los mejores resultados posibles, tanto para los usuarios móviles como para la sociedad en general, 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, junto con el esfuerzo de los usuarios.

1

Uso de los dispositivos móviles

Promover el uso seguro de los servicios móviles a través de medidas proactivas para la protección del usuario, de actividades ilegales y perjudiciales vinculadas al uso de teléfonos móviles o facilitadas por estos:

- Pilares contra el robo de terminales
- Empoderamiento del usuario
- Dispositivos falsificados
- Registros nacionales de usuarios: un camino cuestionable

Enfoque de la industria

- Trabajar en colaboración con otros organismos para 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 usuario
- Enseñar al usuario conductas seguras relacionadas con el uso de aplicaciones y servicios móviles, para así aumentar su confianza.

2

Los datos y la privacidad de los usuarios y organizaciones

Promover medidas proactivas para proteger y respetar los intereses de privacidad del usuario, facilitando la toma de decisiones informadas sobre qué datos personales se recolectan y cómo se utilizan:

- Principios de privacidad
- La privacidad en Big Data
- Identidad digital

Enfoque de la industria

- Almacenamiento y tratamiento seguro de toda información personal y privada, conforme a los requisitos legales, cuando corresponda.
- Transparencia con el usuario 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 usuario pueda tomar decisiones simples y significativas sobre su privacidad.

PROTECCIÓN DEL USUARIO

PROTECCIÓN DE LA PRIVACIDAD

PRIVACIDAD PERSONAL, SEGURIDAD Y PROTECCIÓN DE DATOS

LA SEGURIDAD PÚBLICA

PROTECCIÓN DE LAS REDES Y LOS DISPOSITIVOS

3

Seguridad pública y cumplimiento de las obligaciones legales

Los operadores colaboran con los organismos de seguridad pertinentes para proteger la seguridad pública, en el marco de la ley y respetando los derechos humanos.

- Inhibidores de señal o Jammers.
- Nominatividad o Registro de tarjetas SIM.
- Intervención legal a las comunicaciones.
- Orden de Restricción de Servicio.

Enfoque de la industria

- Trabajar con los organismos pertinentes cuando la situación lo requiera, a fin de desarrollar e implementar soluciones adecuadas para alcanzar el objetivo final con el mínimo perjuicio al usuario y a los servicios críticos.
- Construir redes que tengan la funcionalidad de enfrentar situaciones de emergencia y seguridad, cuando corresponda.
- Comunicar las limitaciones existentes para cada eslabón de la cadena de valor y recomendar dónde deberían implementarse acciones preventivas.

4

Seguridad de las redes e integridad de los dispositivos

Proteger la infraestructura subyacente y asegurar que se provea al cliente el servicio de comunicaciones más seguro y confiable posible

- Ciberseguridad
- Seguridad en el Internet de las Cosas

Enfoque de la industria

- 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 proveedores de servicios o infraestructura.

Seguridad del usuario

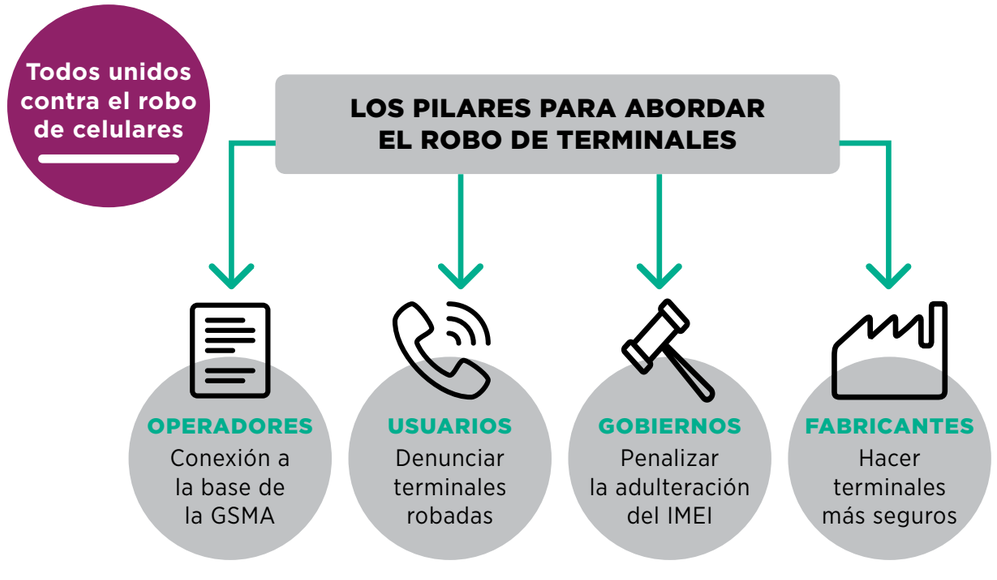
1. Uso de los servicios móviles

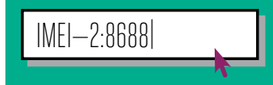
1.1 Pilares contra el robo de terminales

El robo de dispositivos celulares es un delito que ha crecido fuertemente en América Latina en los últimos años, debido al incremento en la adquisición de dispositivos móviles y en particular a la masividad del acceso a teléfonos inteligentes. El sector público y el privado trabajan colaborativamente contra el mercado negro y el crimen vinculado con el robo de dispositivos y el uso de terminales robados.

No existe una medida única efectiva para poder combatir el robo de terminales. Debe contemplarse una solución integral y abordarla de manera coordinada de acuerdo a la responsabilidad que cada pilar tenga: **USUARIOS, OPERADORES, GOBIERNOS Y FABRICANTES.** Sin ese trabajo conjunto no será posible tener éxito para reducir este flagelo.

LA CONEXIÓN, EL INTERCAMBIO Y EL FORTALECIMIENTO DE LA LISTA NEGRA DE GSMA ES EL PRINCIPAL APORTE DE LA INDUSTRIA Y CONSTITUYE EL MECANISMO MÁS SÓLIDO DISPONIBLE A NIVEL MUNDIAL, EN LOS ESFUERZOS GLOBALES DE LUCHA CONTRA ESTE FLAGELO QUE INCLUSO LLEGA A COBRAR VIDAS HUMANAS EN SITUACIÓN DE ROBO.





Todos los dispositivos conectados a la red móvil (teléfonos, tabletas, etc) poseen un número identificador **único conocido como IMEI (Identificador Internacional de Equipos Móviles, IMEI por su sigla en inglés),** compuesto por un código que indica fabricante y modelo, seguido por un número de serie. El IMEI **identifica unívocamente a cada dispositivo en el mundo.** La GSMA es la organización encargada de otorgar los rangos de TACs[1] válidos a cada fabricante legítimo de dispositivos móviles, a fin de que identifique sus productos.

La base de GSMA (IMEI Database) es mayoritaria y crecientemente usada por los operadores del mundo y de América Latina para compartir diariamente información de equipos robados con el objeto de impedir su uso.

IMEI DB

La GSMA mantiene un listado central de IMEI de terminales móviles, conocido como la base de datos de IMEI. **Allí, se listan todos los celulares reportados como robados o extraviados** por los clientes de los operadores de redes móviles de todo el mundo. Adicionalmente, a través de la misma base de datos, es posible verificar si un IMEI pertenece a un rango válido otorgado a por la GSMA.

[1] El TAC se compone de los primeros 8 dígitos del IMEI y especifica el fabricante y modelo del dispositivo. Los 7 dígitos restantes del IMEI son utilizados como número de serie.

1.2 Empoderamiento del usuario

Es clave que los **Estados** tipifiquen como **delito no sólo la adulteración del IMEI sino también la comercialización ilegal, cada vez más frecuente, de componentes provenientes de teléfonos robados.**

Para combatirlos es fundamental además que la policía y las fiscalías estén empoderadas para tomar las acciones necesarias al momento de realizar allanamientos en puntos de acopio y reprogramación de teléfonos robados.

Al mismo tiempo, es de vital importancia **concientizar a los usuarios para involucrarlos activamente** en la lucha contra el robo de teléfonos móviles.

El Sistema de Verificación de Dispositivos (IMEI Device Check) que GSMA pone a disposición de los usuarios **a través de la página web del Regulador,** permite **verificar de manera gratuita** si un dispositivo móvil ha sido reportado como robado en algún lugar del mundo.

De este modo, **cualquier persona puede comprobar la legitimidad del equipo antes de efectuar su compra.** Interrumpiendo así el circuito de demanda de equipos robados.

Esta herramienta **ha sido implementada exitosamente en México, Costa Rica, Honduras, Brasil y Argentina;** y se encuentra en proceso de implementación en Colombia, El Salvador y República Dominicana.

LA SEGURIDAD DE LOS CIUDADANOS Y SUS BIENES ES RESPONSABILIDAD DE LOS ESTADOS. LOS OPERADORES COLABORAN EN LA LUCHA CONTRA EL HURTO DE MÓVILES, COMPARTIENDO INFORMACIÓN Y BLOQUEANDO LOS TELÉFONOS DENUNCIADOS COMO SUSTRAÍDOS.

1.3 Dispositivos falsificados

Casi 1 de cada 5 dispositivos móviles puede ser falsificado[1]. Esto tiene efectos negativos para el consumidor, quien se arriesga a defectos en la calidad, seguridad, privacidad, e impacto en la salud y el medio ambiente.

La colaboración entre los múltiples afectados puede ayudar a combatir el problema desde su origen.

La GSMA ha puesto a disposición de la Organización Mundial de Aduanas (World Customs Organization) la base de datos de IMEI asignados a fin de establecer un **portal de seguridad global** a través del cual los **agentes aduaneros pueden verificar en línea la autenticidad del identificador de los dispositivos móviles.**

Al mismo tiempo, la GSMA alienta a los operadores a instalar sistemas como EIRs (Equipment Identity Registers) y a conectarse a la base de datos de IMEIs de la GSMA. De ese modo, estos pueden verificar si un IMEI pertenece a un rango válido otorgado a por la GSMA, y eventualmente, bloquear equipos falsificados con IMEIs inválidos.

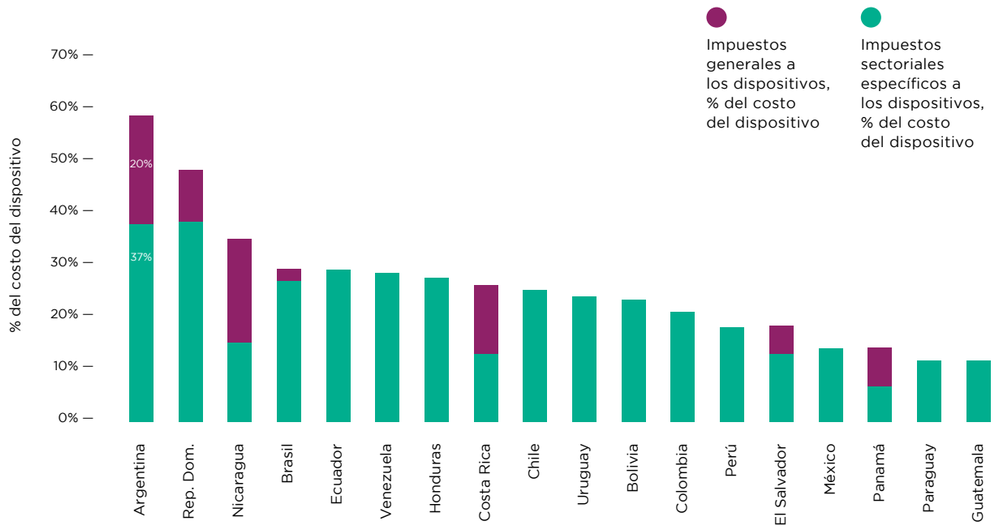
Algunos países están considerando la implementación de registros nacionales de dispositivos (en los cuales los suscriptores deben registrar sus dispositivos) para combatir las falsificaciones y el contrabando. Existe el riesgo de que estos mecanismos puedan restringir la libre elección del usuario, impedir el movimiento libre de dispositivos legítimos a través de las fronteras e introducir cuestiones de privacidad, pudiendo incluso ser ilegal en algunos países.

Las autoridades nacionales deberían estudiar qué factores afectan los precios de los dispositivos, tales como tasas de importación e impuestos específicos. Estos últimos constituyen una barrera a la asequibilidad y contribuyen a aumentar la demanda local de teléfonos en el mercado negro.

REDUCIR LA CARGA IMPOSITIVA PARA HACER MÁS ASEQUIBLES LOS DISPOSITIVOS LEGALES REDUCIRÍA AL MISMO TIEMPO LOS INCENTIVOS PARA EL DESARROLLO DE UN MERCADO NEGRO

[1] http://www.oecd.org/governance/one-in-five-mobile-phones-shipped-abroad-is-fake.htm

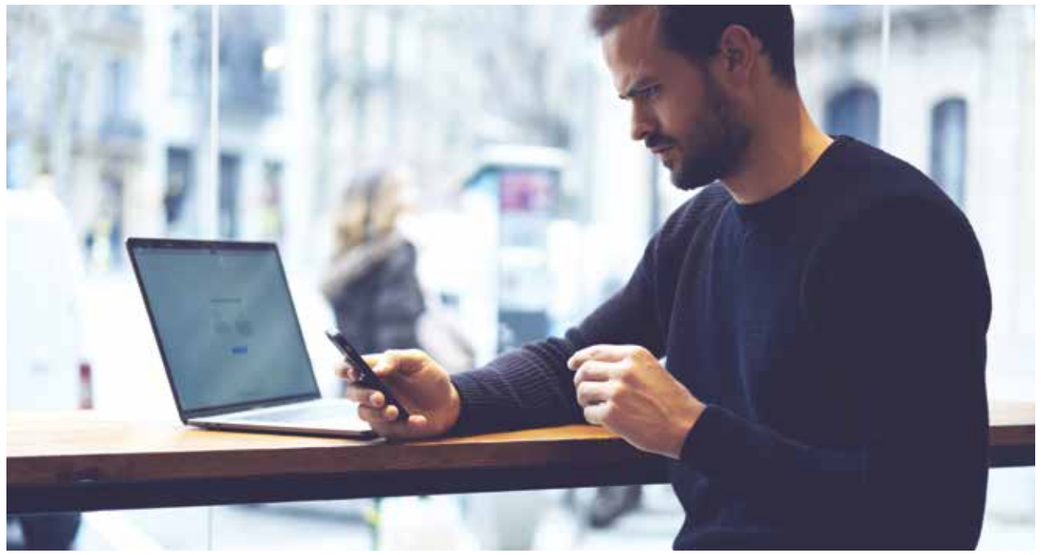
IMPUESTO A LOS DISPOSITIVOS COMO PORCENTAJE DE SU PRECIO FINAL, 2016



FUENTES: GSMA INTELLIGENCE, TARIFICA

En última instancia, si se decide utilizar registros nacionales de dispositivos, éstos deberían contener únicamente la información existente en la base de rangos de identificador válidos de la GSMA, que es la fuente concluyente de los identificadores asignados a los fabricantes legítimos en el mundo.

Finalmente, en caso de avanzar con esta clase de registros, los gobiernos deberían analizar con detenimiento las consecuencias no deseadas para los consumidores que hayan adquirido equipos falsificados de buena fe.



1.4 Listas blancas

En algunos casos, las autoridades nacionales han propuesto y promovido el uso de listas blancas, positivas o registros de dispositivos móviles para combatir el robo de celulares. Este tipo de listas están compuestas por los números de identificación (IMEI) de los teléfonos autorizados a conectarse a las redes celulares. De manera que es necesario registrar cada teléfono que pretenda ser utilizado. Este mecanismo invierte la lógica por la cual todo dispositivo es, en principio, legal. Requiriendo una gestión específica para ser considerado como tal y dado de alta en la lista, a fin de habilitar su uso.

Las listas negras alimentadas por la base de IMEIs denunciados como robados de la GSMA son el mecanismo más eficiente en la lucha contra el robo.

El uso de listas blancas nacionales podría impedir la libre circulación de dispositivos móviles por el mundo, sobrecargando al usuario con procesos de activación confusos. Además, implicaría inversiones desproporcionadas por parte de los operadores para poder gestionarlas. Estas consecuencias no deseadas constituyen efectivamente mayores barreras para la adopción por parte de los usuarios, sin ofrecer ventajas que las justifiquen.constituyen una barrera a la asequibilidad y contribuyen a aumentar la demanda local de teléfonos en el mercado negro.

EN LOS POCOS PAÍSES DONDE SE IMPLEMENTARON LISTAS BLANCAS, NO HUBO EVIDENCIA DE UN IMPACTO POSITIVO EN LA REDUCCIÓN DE LOS NIVELES DE ROBO DE EQUIPOS MÓVILES.

2. Los datos y la privacidad

2.1 Pilares de la privacidad

La privacidad de los usuarios se ve afectada por una serie de factores, a menudo controlados por múltiples partes involucradas - el proveedor de servicios o aplicaciones, el operador de telefonía móvil, el fabricante del equipo y el sistema operativo u otro proveedor de software.

Al mismo tiempo, la seguridad y la privacidad de la información personal están reguladas por una variedad de leyes nacionales, mientras que el servicio de Internet es internacional. Por otra parte, las reglas que rigen, como, por ejemplo, de tratamiento de datos personales, suelen ser diferentes para los operadores móviles que a las que rigen para las compañías de Internet (que muchas veces no están alcanzadas por ninguna norma de protección de datos personales).

Las diferencias entre los ámbitos de aplicación de las leyes nacionales de privacidad, por un lado, y las prácticas estándares de carácter global, por otro, dificultan la provisión de una experiencia de usuario consistente; pueden causar inseguridad jurídica desalentando la inversión e innovación; y generar niveles desiguales de protección, implicando riesgos para los usuarios en cuanto al acceso a sus datos personales exponiéndolos a posibles robos de identidad y fraude.

En este contexto, la GSMA desarrolló nueve principios de privacidad para fomentar las mejores prácticas y estándares que proporcionen, de modo consistente, transparencia, notificación, elección y control para los usuarios móviles.

LOS ESTADOS DEBEN GARANTIZAR QUE LA LEGISLACIÓN SEA TECNOLÓGICAMENTE NEUTRAL Y QUE SUS REGLAS SEAN APLICADAS CONSISTENTEMENTE POR IGUAL A TODOS LOS ACTORES DEL ECOSISTEMA DE INTERNET.

PRINCIPIOS DE PRIVACIDAD MÓVIL DE LA GSMA[2]

MÍNIMA RECOLECCIÓN 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.

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.

OPCIONES Y CONTROL DEL USUARIO

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

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.

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 obli- gaciones legales correspondientes.

EDUCACIÓN

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

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.

RESPONSABILIDAD Y EJECUCIÓN

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

[2] http://www.gsma.com/publicpolicy/mobile-privacy-principles

2.2 La privacidad y el Big Data

El incremento en la capacidad de almacenamiento y procesamiento de datos estadísticos, la Internet de las Cosas (IoT) y el desarrollo de las técnicas de análisis de Big Data hacen posible procesar grandes volúmenes de datos a mayor velocidad que nunca. Permitiendo extraer información significativa y útil para la toma de decisiones.

Al mismo tiempo, existe un número cada vez mayor de dispositivos con sensores que recopilan y comunican datos susceptibles de ser analizados.

Sin embargo, para hacerlo, es imprescindible contar con la confianza del consumidor.

Por lo tanto, para que una sociedad pueda alcanzar los beneficios del enorme potencial que estas tecnologías ofrecen, es importante que los principios de privacidad ya establecidos sean respetados, ayudando a fomentar un entorno de confianza.

PARA MAXIMIZAR LOS BENEFICIOS DEL BIG DATA LOS ESTADOS DEBERÍAN:

- Entender cómo funciona y el contexto en el que se utiliza.
- Promover enfoques innovadores para la transparencia y el consentimiento de los usuarios.
- Fomentar directrices y autorregulación para aprovechar, en lugar de obstaculizar, el análisis de Big Data.
- Implementar mecanismos de transferencia de datos a través de fronteras armonizados y con salvaguardas, tales como los ofrecidos por la UE y la APEC.

2.3 Identidad digital. Principios.

La identidad digital es un asunto estratégico para el desarrollo de la economía digital, que está en la agenda de gobiernos, reguladores y organizaciones comerciales.

En la actualidad, ciudadanos en todo el mundo pagan impuestos, gestionan cuentas bancarias, consumen bienes y servicios, y se conectan con amigos en redes sociales a través de canales digitales.

Al mismo tiempo, en las economías en desarrollo, existen diversas iniciativas digitales enfocadas en establecer infraestructuras de seguridad social para combatir la pobreza, proteger a los grupos vulnerables y ofrecer servicios de salud efectivos e inclusivos.

Pero a medida que crece el número y uso de identidades digitales de las personas, aumentan también los riesgos de robo de identidad y fraude asociados. Desafiando a todos los involucrados a definir políticas y servicios y a asegurar que los ciudadanos estén adecuadamente protegidos.

Esto requiere el desarrollo de soluciones de gestión de identidad innovadoras que se extiendan más allá de usuario y contraseña. Que sean capaces de ofrecer mayor privacidad, protección, más opciones y un acceso conveniente a diversos servicios en todo momento y lugar que sean requeridos.

Para ello, **la red móvil constituye una plataforma ideal por ser un medio seguro, de alta penetración y amplia cobertura.**

LOS ESTADOS DEBERÍAN ASEGURAR LA COHERENCIA ENTRE LOS DIFERENTES INSTRUMENTOS LEGALES Y REGULATORIOS QUE AFECTAN A LA IDENTIDAD DIGITAL, FACILITAR LA INTEROPERABILIDAD DE LAS TRANSACCIONES ELECTRÓNICAS Y MINIMIZAR LOS COSTOS DE CUMPLIMIENTO PARA LA INDUSTRIA.

LOS PRINCIPIOS EMERGENTES PARA UN ECOSISTEMA DE IDENTIDAD DIGITAL SÓLIDO DEBERÍAN INCLUIR:

- La cobertura y disponibilidad universal (incluida la accesibilidad para todos).
- Un diseño apropiado y efectivo que tenga en cuenta la interoperabilidad y la sostenibilidad.
- La necesidad de crear y mantener la confianza al garantizar la protección de la privacidad y los datos personales, y ofrecer a los consumidores supervisión y control de sus datos.

Mobile Connect es una solución de autenticación segura y universal por medio del teléfono móvil.

Al momento de necesitar probar su identidad, por ejemplo, al iniciar sesión en un sitio web o al realizar una compra, el usuario es derivado a un portal de Mobile Connect en donde debe introducir su número de línea móvil. Inmediatamente es contactado a través de su celular, solicitándosele una sencilla interacción a fin de autorizar el acceso o transacción.
Mobile Connect mejora la experiencia de usuario al simplificar el proceso de autenticación, al mismo tiempo que ofrece a los desarrolladores de servicios una interfaz única y estandarizada de alcance global para la autenticación de sus usuarios.

Seguridad del entorno

3. La seguridad pública

3.1 Inhibidores de señal/Jammers. Alternativas.

En los últimos años, ha proliferado la disponibilidad no autorizada de teléfonos móviles en las cárceles. Posibilitando la ejecución de ilícitos por los criminales convictos en ellas detenidos.

Como medida para limitar su uso en este contexto, las autoridades han promovido la implementación de inhibidores de señal de telefonía móvil.

Esto implica destinar recursos a degradar la calidad y capacidad de la red, en tiempos en que los usuarios demandan lo opuesto. Además, los inhibidores interfieren con la comunicación entre el terminal móvil y la estación base, siendo sólo parcialmente efectivos en el objetivo de privar de comunicaciones a los presidiarios, pero agregando una consecuencia negativa particular: **las áreas circundantes a los centros penitenciarios necesariamente se verán afectadas por los inhibidores de señal,** con lo cual, al menos **una fracción de la zona experimentará deterioro y cortes de señal.**

Dada la naturaleza probabilística de la señal móvil, es imposible garantizar el bloqueo total de señales en el área de una prisión. Esto es agravado por las diferentes condiciones atmosféricas, así como por la hora del día, que modifican la propagación de la radiofrecuencia.

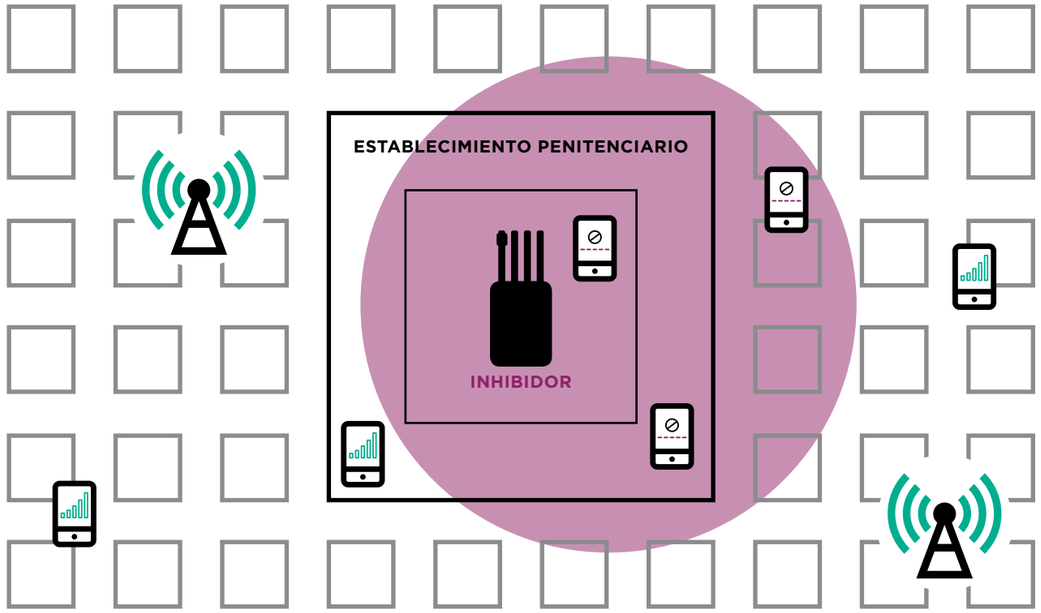
EL CRIMEN COORDINADO DESDE LAS CÁRCELES SÓLO PUEDE SER COMBATIDO CON SOLUCIONES INTERDISCIPLINARIAS, DONDE LA COOPERACIÓN DE LAS PARTES ES CLAVE.

FUNCIONAMIENTO DE LOS INHIBIDORES

PROPAGACIÓN DE LAS ONDAS DE RADIO

Las ondas de radio atraviesan las paredes permitiendo que haya señal incluso adentro de las contrucciones

Otros materiales, en general metálicos, pueden reflejar las ondas de radio, dificultando la contención de su propagación hacia otras zonas.



Los inhibidores actúan emitiendo una señal que interfiere la comunicación entre el móvil y las antenas

ES IMPOSIBLE DELIMITAR CON PRECISIÓN EL ÁREA A INTERFERIR

- Los teléfonos miden constantemente a las antenas que lo rodean y utilizan la que ofrece mejores condiciones
- Este mecanismo está diseñado para que la comunicación se mantenga aún en movimiento
- Los móviles interferidos constantemente intentarán conectarse con otras antenas alternativas

Una respuesta más completa al problema de fondo puede desarrollarse con distintas estrategias y mecanismos que suplementen o complementen el uso de bloqueadores, considerando entre otras soluciones: celdas dummies, intervención en base a patrones de uso, listas negras (GSMA IMEI DB) y, especialmente, mayor control en los recintos.

El uso de inhibidores de señal y – peor aún – el apagado de celdas implica inevitablemente afectar la calidad de servicio móvil, acarreando perjuicios individuales, así como para las comunidades y economías de los países.

Un conjunto de soluciones integrales y complementarias – distintas a los inhibidores - para eliminar el uso de comunicaciones móviles desde las cárceles puede incluir lo siguiente:

- **Scanners de ondas milimétricas y retro dispersión** en accesos a los penales (cómo las usadas en los aeropuertos): deberían ser el recurso primario (nunca faltar) en cada centro penitenciario. Si se controla con estos scanners se tendería a eliminar el acceso de dispositivos móviles, que es el origen de todo el problema.

- **Bloqueo de IMEIs en base a patrones de comportamiento:** si la legislación lo permite se podría bloquear IMEIs que evidencien un comportamiento que confirme el uso de móviles para actividades ilegales, considerando patrones específicos.

- **El uso de celdas dummies** al interior de los centros penitenciarios puede desvirtuar el uso de celulares encendidos en el interior de estos recintos, anclando la conexión de estos a una celda desconectada de la red.

LA SOLUCIÓN DEBERÁ SER INTEGRAL. PARA ENCONTRAR UNA RESPUESTA A LA PROBLEMÁTICA DE LOS TELÉFONOS ILEGALES EN LOS PRESIDIOS, ES NECESARIO UN ABORDAJE COORDINADO CON MÚLTIPLES ENFOQUES Y CONSTANTES AJUSTES, QUE INCLUYA TRABAJAR SOBRE EL INGRESO ILEGAL DE LOS MÓVILES.

3.2 Nominatividad o registro de tarjetas SIM.

Un número creciente de gobiernos ha implementado recientemente el registro obligatorio de usuarios de tarjetas SIM prepagas, con la esperanza de que esta política pudiera colaborar con los esfuerzos de la lucha contra crimen. Esto significa que debe registrarse un titular responsable al momento del alta de la línea, verificándose su identidad, comúnmente a través de la presentación de un documento oficial.

Por el contrario, si los requisitos de registro son desproporcionados para el mercado específico, la obligatoriedad de la política puede generar problemas de puesta en práctica y consecuencias imprevistas. Por ejemplo, se podría excluir involuntariamente a los consumidores vulnerables y desfavorecidos socialmente que carecen de los documentos de identidad necesarios, o podría generar la aparición de un mercado negro de tarjetas SIM robadas o registradas fraudulentamente.

Es clave realizar evaluaciones de impacto, involucrando a la industria, antes de decidir tanto la implementación como la revisión de normas de registro obligatorio existentes; a fin de analizar costos, beneficios y alternativas.

Por último, luego de efectuado los cambios, debe analizarse la eficacia del proceso y la medida en la que se han alcanzado los objetivos iniciales de la política.

DE ACUERDO A LA EVIDENCIA EMPÍRICA, EL REGISTRO DE SIMS NO MEJORA LA SEGURIDAD CIUDADANA.

SEGURIDAD DEL ENTORNO

3.3 Intervención legal de las comunicaciones.

Los operadores de redes móviles están sujetos a una **serie de regulaciones que los obligan a cooperar** con las actividades de **los servicios policiales y de seguridad en los países donde operan.**

Estos requisitos, que son diferentes en cada país, **ofrecen un punto de referencia legal** que sirve de orientación para los operadores de redes móviles **respecto a cómo responder a estas solicitudes.** Las cuales, al mismo tiempo, plantean un desafío al compromiso de la industria a proteger la privacidad de la información del consumidor.

Por lo general la legislación se encuentra atrasada respecto de los avances tecnológicos y es por ello que pueden surgir malentendidos sobre el nivel de capacidad técnica de los operadores de redes móviles para interceptar cierto tipo de comunicaciones.

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.**

Los operadores de redes móviles reconocen la importancia de la soberanía y legitimidad de los gobiernos en la defensa de la seguridad de sus ciudadanos. Para lograr este objetivo, **la interceptación de las comunicaciones a fines de la aplicación de la ley o de seguridad sólo debe tener lugar 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.

LA FALTA DE CLARIDAD EN EL MARCO LEGAL RESPECTO A DATOS CONFIDENCIALES E INTERCEPTACIÓN DE LAS COMUNICACIONES ES UNA DIFICULTAD PARA PROTEGER LA PRIVACIDAD DE LOS CIUDADANOS. LOS OPERADORES DEBERÍAN SIEMPRE DISPONER DE LA INSTANCIA LEGAL PARA RESPONDER A REQUERIMIENTOS DE ACCESO.

SEGURIDAD DEL ENTORNO

3.4 Orden de Restricción de Servicio (ORS).

Las Ordenes de restricción de servicio son órdenes emitidas por las autoridades competentes, que obligan a suspender o restringir el acceso a un servicio.

Los operadores móviles reciben ORS para impedir o restringir el acceso a su red móvil, un servicio de red o un servicio que funciona over-the-top (OTT). Esto puede llevarse a cabo por medio del bloqueo a contenidos particulares, la restricción de ancho de banda de datos o la degradación de la calidad de los servicios SMS o de voz.

En algunos casos, los operadores se exponen a sanciones penales o la pérdida de licencia si revelan que han recibido una ORS.

En estos casos, los operadores móviles sufren pérdidas económicas debido a la suspensión de los servicios, así como daño a su reputación. Su personal debe hacer frente a la presión de autoridades e, incluso, a represalias por parte de los usuarios.

Con el fin de contribuir a la transparencia, **los gobiernos solo deberían emitir las ORS a los operadores por escrito,** citando la base jurídica y **con un claro registro de actividades de la persona que autorizó la orden.** Adicionalmente, deberían informar a los ciudadanos al respecto, permitiendo a los operadores investigar los impactos y comunicarse libremente con sus clientes acerca de la orden.

POTENCIALES CONSECUENCIAS DE UNA ORS

- Seguridad nacional afectada si los poderes son mal utilizados.
- Seguridad pública en peligro si los servicios de emergencia y los ciudadanos no son capaces de comunicarse entre sí.
- Afectaciones a la libertad de expresión, libertad de reunión, libertad de empresa y otros derechos humanos.

LOS ESTADOS NO DEBERÍAN ABUSAR DE LAS ORS. RECURRIENDO A ELLAS CUANDO SEA ABSOLUTAMENTE NECESARIO PARA ALCANZAR UN OBJETIVO ESPECÍFICO Y LEGÍTIMO COMPATIBLE CON LOS DERECHOS HUMANOS Y LAS LEYES PERTINENTES.

4. La seguridad de las redes e integridad de los dispositivos

4.1 Ciberseguridad

La Ciberseguridad es una disciplina que tiene por objetivo asegurar que los recursos de tecnología de la información estén disponibles y accesibles para ser utilizados por los autorizados a hacerlo y, por el contrario, sean inaccesibles para quienes no lo están.

Como tal, abarca diversos aspectos de las redes de telecomunicaciones fija, móvil e Internet. Incluye desde la integridad física de los equipos hasta la seguridad de la información en ellos contenida.

Es por esto que la salvaguarda de la ciberseguridad impacta desde procesos organizacionales hasta estándares tecnológicos incluyendo, por supuesto, aspectos regulatorios y legales. Al mismo tiempo, la gestión de la ciberseguridad debe cubrir todo el ciclo de vida de un servicio, desde su diseño, pasando por su implementación y operación.

Para un correcto abordaje resulta imprescindible que los actores involucrados trabajen en conjunto y en forma coordinada, considerando en todo momento cuáles son los límites de responsabilidad en la infraestructura o servicio de cada uno de ellos.

El objetivo debe ser el desarrollo de un ecosistema confiable en donde las personas y negocios puedan interactúan manteniendo el control de su información y activos de valor, extendiendo así el alcance y beneficios del entorno digital.

LA REGULACIÓN DEBERÍA 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.

4.2 Seguridad en Internet de las Cosas

La mayoría de los servicios de IoT presentan los mismos desafíos de seguridad que enfrentan tantos otros servicios que dependen de la conectividad:

- **Disponibilidad**
  Asegurar una conectividad constante entre los terminales y sus respectivos servicios
- **Identidad**
  Autenticar los terminales, servicios y usuarios
- **Integridad**
  Asegurar que la integridad del sistema puede ser verificada y monitoreada
- **Privacidad**
  Reducir el potencial acceso a información por parte de personas no autorizadas

Al mismo tiempo, los dispositivos IoT son cada vez más baratos, tienen fuentes de alimentación limitadas, ciclos de vida largos (algunos hasta 10 años) y son físicamente más accesibles para los atacantes.

Dada la diversidad de tipos de servicios IoT, los desafíos de seguridad únicos de la IoT y la necesidad de un enfoque holístico hacia la seguridad, la GSMA cree que la seguridad para IoT se debe abordar mejor a través de un enfoque liderado por la industria que considere que:

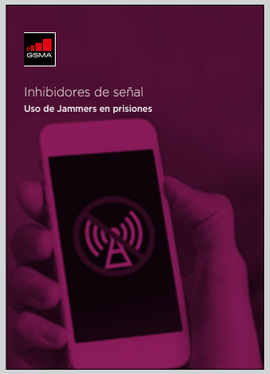
- La regulación específica es innecesaria y dificultaría la innovación.
- La flexibilidad para las verticales de la industria (en contraposición a una "talla única") para evaluar y abordar los riesgos específicos es crítica.
- La industria puede seguir las mejores prácticas para integrar la seguridad y la privacidad a través del ciclo de vida del servicio.

ES FUNDAMENTAL RECONOCER LA CONDICIÓN INCIPIENTE DEL ECOSISTEMA IOT, ACEPTANDO QUE SU DINÁMICA Y ORGANIZACIÓN DEFINITIVA AÚN SE DESCONOCEN. EN CONSECUENCIA, SE DEBERÍA EVITAR EXTENDER AUTOMÁTICAMENTE REGULACIONES HEREDADAS ENFOCADAS A SERVICIOS PREEXISTENTES, QUE PODRÍAN RESTRINGIR PREMATURAMENTE LA INNOVACIÓN.

OTROS ESTUDIOS PUBLICADOS

SEGURIDAD, PRIVACIDAD Y PROTECCIÓN DEL ECOSISTEMA MÓVIL

Este 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.



INHIBIDORES DE SEÑAL USO DE JAMMERS EN PRISIONES

Este reporte busca orientar a los encargados de políticas de seguridad pública acerca de las limitaciones y complejidad del uso de inhibidores de señal, a través de la explicación de los conceptos básicos de funcionamiento y casos de estudio. Además, se describen los marcos regulatorios aplicables en países de la región y se resumen las recomendaciones para su uso efectivo.

CALIDAD DE LOS SERVICIOS MÓVILES

Este reporte explica los diversos factores que afectan la calidad del servicio en las redes móviles, tanto propios del sistema como externos. Para luego presentar las estrategias regulatorias más convenientes para fomentar la mejora de la calidad de los servicios de telecomunicaciones móviles.

PARA ACCEDER A LOS REPORTES DE LA GSMA Y RECURSOS RELACIONADOS VISITE: WWW.GSMALA.COM/ES/RESOURCES

Para ver y descargar el reporte completo
por favor visitar www.gsmala.com

GSMA Latin America
Av. Del Libertador 6810 Piso 15
(Edificio Square Libertador)
C1429BMO, Buenos Aires, Argentina
Teléfono: +54 11 5367-5400
Mail: Infolatam@gsma.com
Sitio web: www.gsmala.com