Thomas Kershaw
Vicepresidente Sénior
Soluciones para interconexión

www.telcordia.com

One Telcordia Drive
Piscataway, NJ 08854
Estados Unidos de América

T +1 732 699 2035
tkershaw@telcordia.com

21 de julio 2011
Doctor
CRISTHIAN LIZCANO
Director
Comisión de Regulación de Comunicaciones -CRC-
Bogotá
Colombia

Ref: Proyecto de Resolución por medio de la cual se establecen las condiciones regulatorias para el control del uso de Equipos Terminales Móviles hurtados y/o extraviados y con alteraciones en sus mecanismos de identificación

Dr. Lizcano:

A continuación la empresa Telcordia Technologies INC presenta sus comentarios al proyecto de norma de la referencia después de haber revisado y estudiado tanto el "Proyecto de Resolución" como el documento soporte a la norma, todo esto con el ánimo que el regulador colombiano pueda incorporar nuestras sugerencias realizadas por nuestros grupos de gestión y de ingeniería de productos, que pueden contribuir a mejorar la eficacia y lograr el éxito del ambicioso e importante proceso que será un hito para la regulación regional sobre este tema de gran importancia.

De considerarlo pertinente, podremos poner a disposición de ustedes nuestra importante experiencia y conocimiento que del tema tenemos gracias al desarrollo de nuestro sistema de registro centralizado de información de dispositivos móviles que hemos implementado y que en la actualidad operan en varios países del mundo.

Atentamente,

Thomas Kershaw
Vicepresidente Senior
Soluciones para interconexión

Anexos:

Comentarios a la CRC de Colombia con relación a la implantación de un Registro de dispositivos
Comentarios de Telcordia sobre el borrador del Proyecto de Resolución

Comentarios de TELCORDIA TECHNOLOGIES INC al proyecto de Resolución por medio de la cual se establecen las condiciones regulatorias para el control del uso de Equipos Terminales Móviles hurtados y/o extraviados y con alteraciones en sus mecanismos de identificación.

Resumen Ejecutivo

Los cambios en el modo de fabricación de los dispositivos móviles , junto con las nuevas y abiertas plataformas de software para la operación de dispositivos móviles, han cambiado la manera cómo los gobiernos deben mirar a las soluciones móviles orientadas a los dispositivos.

las soluciones tradicionales, solamente para Equipment Identity Registry (EIR) ya no bastan para la gestión de dispositivos móviles en cuanto a la lucha contra el robo, la aprobación de dispositivos móviles y la conciliación con las importaciones, ya que un número cada vez mayor de fabricantes que no cumplen han ignorado las convenciones de la industria en la identificación, la certificación de funcional, la valoración de la importación y las mejores prácticas de salud y seguridad.

Además, las brechas causadas por el retraso en la implementación de la distribución de datos a los operadores y la reprogramación de dispositivos socavan aún más estos sistemas tradicionales. Estas prácticas, junto con la reprogramación ilícita de los dispositivos móviles y la falsificación, dificultan el interés nacional de Colombia en un mercado dinámico y competitivo para los dispositivos móviles.

Los métodos manuales, tales como los intentados recientemente en México con el esquema de Renault, han demostrado ser ineficaces, ya que las tasas de registro nunca alcanzan niveles lo suficientemente altos para proporcionar un contexto suficiente para la vigilancia del cumplimiento.

Como resultado de estas cuestiones, en la mayoría de las implementaciones nacionales los esquemas tradicionales de registro de dispositivos permanecen latentes, como elementos disuasorios fracasados que apoyan a una variedad de objetivos de la política.

Telcordia considera que sólo los esquemas automatizados de recolección de datos, incluyendo los de datos de activación del dispositivo, datos de registro dentro de la red y otras formas de registros y datos públicos, aplicados de una forma centralizada, representan el único enfoque viable para cumplir con los objetivos de la política expresada por Colombia en esta regulación. Su Registro central de información sobre dispositivos (CDIR) puede cumplir con los objetivos de la política expresada en el presente regulación sin dejar de ser adaptable a las futuras amenazas reconocidas en el ecosistema de la red móvil

I- Algunos antecedentes y experiencias que justifican los sistemas de Registros de dispositivos móviles.

En la red móvil tradicional, ideada y diseñada en el siglo pasado, el entorno para la fabricación de dispositivos móviles era muy diferente a lo que es hoy. Los dispositivos móviles provenían de operaciones integradas verticalmente, siendo diseñados y fabricados por un puñado de empresas con una combinación de hardware, software y capacidad de producción, cumpliendo estrictamente con las especificaciones sectoriales (por ejemplo, ETSI, GSMA) y las regulaciones gubernamentales (por ejemplo, FCC, CE). Tomando como un hecho el alto costo inicial para la fabricación de dispositivos, un esfuerzo significativo en el desarrollo de cadenas verticales de suministro y en el establecimiento de canales de distribución internos, ya fuera a través de los distribuidores o de los propios operadores, dio lugar a un ecosistema de buen funcionamiento abarcando dispositivos móviles legítimos, con identificadores únicos, vendidos a través de canales bien definidos.

La última década ha traído consigo cambios importantes en la industria de los dispositivos móviles. A medida que la fabricación de teléfonos móviles se desplazó desde las operaciones con integración vertical hacia una industria impulsada por la integración, los componentes clave se convirtieron en productos básicos ("commodities"); el software para teléfonos móviles emergió como plataformas independientes del hardware y la fabricación se tercerizó con contratistas que ofrecen menores costos unitarios y distribución localizada.

La anterior tendencia entró en conflicto con la recesión mundial que empezó a finales de 2007, cuando los grandes fabricantes de dispositivos redujeron drásticamente su capacidad, suprimieron los acuerdos de subcontratación y redujeron la compra de componentes, dejando a los subcontratistas inactivos con acceso a un decreciente inventario de componentes. En algunos casos, como en el de HTC, estos subcontratistas aprovecharon este cambio como una oportunidad para desarrollar su propia marca, retirándose del trabajo por contrato como fabricantes de dispositivos originales y haciendo énfasis en sus propios productos; otros se enfocaron en dispositivos móviles sin marca y en muchos casos falsificados, manipulando componentes genéricos y plataformas de software para reproducir dispositivos móviles populares y de marca, a costos artificialmente bajos para los consumidores.

A pesar de que estos fabricantes de dispositivos falsificados — conocidos popularmente como dispositivos "Shanzhai" debido a la ciudad china de Shenzhen, una ubicación central para la fabricación de estos dispositivos — son capaces de ofrecer precios bajos a los consumidores, esto representa un alto costo para las empresas legítimas. Al operar entre las sombras de la industria, evaden los requisitos de licencias, roban los diseños y las marcas de los fabricantes legítimos, compran a los proveedores de materias primas componentes rechazados y de calidad inferior, e ignoran las convenciones industriales sobre identificación y certificación. Se ha sabido que estos dispositivos explotan por causa de baterías de mala calidad, presentan perfiles de emisión de RF que varían enormemente, y en muchos casos carecen de los números únicos de Identidad internacional de equipos móviles (IMEI).

Enfoques tradicionales y desafíos de próxima generación

En la aplicación de un Registro de Identidad de Equipo (EIR) tradicional, la representación de IMEI únicos de los dispositivos es básica para el modelo de seguridad, proporcionando un medio por el cual un operador de telefonía móvil (o en el caso de un EIR centralizado, un grupo de operadores) puede bloquear dispositivos individuales o grupos de dispositivos para diversos propósitos, tales como robo, pérdida, falta de cumplimiento contractual, etc. Cuando los fabricantes de dispositivos que no cumplen o los reprogramadores de dispositivos ilícitos optan por ignorar u ocultar las convenciones para la asignación de IMEI, ya sea usando el mismo número en miles de dispositivos, clonando los IMEI de los dispositivos legítimos, o simplemente no incluyendo el IMEI, resulta ineficaz implementar solamente soluciones EIR tradicionales, ya que un solo IMEI aparentemente bloqueado en forma legítima puede bloquear miles de otros dispositivos adquiridos por clientes que desconocen y no pueden identificar el fraude subyacente.

Como la industria aprendió gracias a los ataques terroristas en Mumbai [India] en noviembre de 2008, los IMEIs inválidos representan un riesgo para la seguridad de los estados modernos, ya que el

seguimiento de los dispositivos móviles, en particular cuando se mueven entre redes, es casi imposible si la identidad subyacente está oculta, ya sea a propósito o sin conocimiento. Al dar el primer paso - bloqueando los dispositivos sin números de IMEI - países como la India han dado comienzo al manejo de esta amenaza. Sin embargo, con esta amenaza más reciente - IMEIs clonados e ilegales - el problema ya no es tan simple, y las soluciones tradicionales para hacer frente a la amenaza resultan cada vez más ineficaces.

Es por la razón antes expuesta que nuestro primer comentario y sugerencia al proyecto regulatorio es que Colombia entre en su proceso regulatorio de definición de las condiciones de los registros móviles en una solución no tradicional sino más avanzada o que llamamos "próxima generación" como más adelante lo describiremos.

Nuevos participantes en el ecosistema

Al mismo tiempo, las nuevas plataformas de software para teléfonos inteligentes, tales como Android, iOS, Microsoft Phone y WebOS, están desplazando rápidamente a los sistemas operativos tradicionales para móviles hechos a la medida, que dominaron la anterior generación de dispositivos móviles. En combinación con una nueva generación de hardware que permite funciones avanzadas, tales como SIM múltiples, Wi-Fi basada en 802.11 y aplicaciones móviles avanzadas que se acercan rápidamente a las capacidades de la computación de escritorio moderna, estos dispositivos vienen con nuevos identificadores vinculados con la Internet de mayor alcance, independientemente de los sistemas de gestión de seguridad y de abonados del operador móvil subyacente.

En muchos casos, el vínculo entre el dispositivo móvil y su proveedor de plataforma es muy superior al que existe entre el dispositivo móvil y su operador de telefonía móvil subyacente. Por ejemplo, un dispositivo móvil de Apple no puede ser legítimamente activado sin establecer una identidad directamente con Apple, conocida como una ID de Apple; esta identidad a su vez habilita una variedad de soluciones posteriores, tales como la ubicación, los servicios de distribución y restitución de aplicaciones, independientemente del operador y de su propia infraestructura de identidad de abonado, que se manifiesta en la identidad internacional del abonado móvil de la tarjeta SIM del operador (IMSI) y vinculada al sistema de aprovisionamiento de suscriptores. Existen procesos similares para activación automática en Windows Mobile, Symbian, Android y otras familias de plataformas de dispositivos, aunque los datos recogidos a través de cada plataforma son diferentes.

En este mundo cada vez más orientado a plataformas, las soluciones tradicionales orientadas al operador, tales como la configuración y administración de dispositivos según OMA, cada vez resultan más irrelevantes a medida que los fabricantes vinculan las funciones críticas para la gestión de dispositivos a los ecosistemas de servicios que subyacen en estas nuevas plataformas, en lugar de las interfaces de gestión del operador; esto deja a los operadores con una capacidad reducida para poder aportar datos vitales sobre los usuarios de los dispositivos. Si se suma a esta tendencia la aplicación de la potabilidad de números móviles, permitiendo a los dispositivos móviles y su número de teléfono subyacente moverse entre los operadores de telefonía móvil, se vuelve casi imposible para un operador de redes móviles correlacionar los datos críticos sobre identidad, seguimiento y otros relacionados con el suscriptor.

Requerimientos funcionales

En opinión de Telcordia, el objetivo central de Colombia en cuanto a la disuasión del robo de los dispositivos móviles requiere la participación activa de todas los partes del ecosistema móvil, muchas de las cuales han sido destacadas en la extensa documentación de la CRC. Sin embargo, creemos que una visión más amplia de los datos disponibles proveería un registro centralizado más abundante y más preciso, reduciendo la tasa de error global al tiempo que aumentaría la eficacia de la disuasión contra el hurto de terminales móviles en el país.

Por ejemplo, aunque la conciliación de las listas de importación de móviles y las certificaciones industriales/gubernamentales de los distintos modelos de dispositivos móviles por parte de los fabricantes proporciona una garantía de que los dispositivos traídos a Colombia cumplen con los requerimientos sobre identificación básica, derechos de importación, salud y seguridad de acuerdo a lo dispuesto por el Gobierno, la información adicional como la recogida en los procesos de activación del dispositivo o aquella relacionada con los servicios asociados también resulta valiosa para la calificación de la autenticidad de los dispositivos que funcionan en Colombia, ayuda a establecer la identidad y la propiedad de los terminales móviles, y podría contribuir a implementar un método de bajo impacto para inscribir los dispositivos en el registro centralizado, sin crear metodologías onerosas para la recolección centralizada de datos.

Mejor dicho, un dispositivo que coincida con un IMEI y registro de importación válidos y haya sido activado a través de un fabricante del dispositivo o habilitador de plataforma representa el dispositivo ideal para su inclusión en una "lista verde" centralizada. Para aquellos fabricantes de dispositivos sin activación del dispositivo o proceso de recolección de datos de usuarios operativos, la recopilación de datos se puede realizar a través de SMS, Web u otros medios dentro de un período prescrito por la CRC y administrado por el registro centralizado mediante un cargo.

En el marco general funcional para el registro de dispositivos móviles también deben ser abordados la clonación ilícita, las asignaciones ilegítimas de IMEI al dispositivo y la reprogramación no autorizada de los dispositivos. Al tener acceso a una variedad de herramientas, implementadas tanto para fines legítimos como para fines ilícitos, un punto de servicio puede modificar los dispositivos móviles a fin de que exhiban un número IMEI ilegítimamente asignado al operador de red móvil, lo que hace imposible el bloqueo de los dispositivos robados. Al combinar los datos del fabricante del dispositivo, incluyendo los datos de activación, con los análisis llevados a cabo en un registro centralizado para monitoreo de la totalidad de los dispositivos móviles activos en el país, Telcordia cree que un registro que funcione bien debería ser capaz de marcar los dispositivos sospechosos, proporcionar un marco para la validación o la incautación, realizar el seguimiento del MSISDN y de otros datos de identificación de estos dispositivos no válidos a fin de producir informes y hacer cumplir el bloqueo consistente de los dispositivos que no estén conformes dentro de Colombia. Al mismo tiempo, el gobierno colombiano podría seguir el ejemplo de otros países con problemas similares, tales como el Reino Unido, donde la reprogramación no aprobada de los dispositivos móviles fue criminalizada en 2002 bajo la Ley de reprogramación de teléfonos móviles; no estamos seguros si este tipo de penalización quedó incluido en la Ley de Seguridad Ciudadana. A medida que las redes móviles se desplazan desde las simples llamadas vocales hacia una amplia variedad de usos, desde tabletas móviles, pasando por la vigilancia de brazaletes GPS, hasta llegar a la medición de servicios públicos, resulta fundamental asegurarse que el equipo implementado para estos propósitos quede protegido como un elemento identificable en la red móvil.

Ya que estos tipos de análisis avanzados requieren una enorme cantidad de datos para realizar una correlación cruzada, factores tales como la duración del uso, la persistencia del emparejamiento IMSI-IMEI, y el uso simultáneo de IMEIs con múltiples IMSI o en múltiples redes contribuyen al objetivo básico principal del bloqueo, requiriendo la verificación o la limpieza de los dispositivos móviles para su uso en el país.

Además, el conjunto de los datos recogidos puede ayudar a todos los participantes en el esquema en la detección, análisis y disuasión de otras actividades ilícitas, tales como la importación desde el extranjero

de dispositivos móviles para el mercado negro o gris, el contrabando de dispositivos móviles no conformes y el seguimiento de elementos móviles relacionados entre sí durante todo su ciclo de vida, proporcionando al mismo tiempo nuevas fuentes de datos para la valoración económica y la segmentación de la industria móvil en Colombia y el apoyo a nuevos negocios auxiliares, tales como el aseguramiento del teléfono, y la autenticación segura, con dos factores, basada en el dispositivo móvil.

En última instancia, una implementación exitosa del registro debe basarse en un enfoque analítico que requiera el almacenamiento de múltiples fuentes de datos, incluyendo los datos de registro del dispositivo en las redes del operador de telefonía móvil por largos períodos. Dada la naturaleza sensible de estos datos, se deben implementar las mejores prácticas para mantener los datos separados de acuerdo a la parte contribuyente de los mismos y al acceso a una auditoría, a fin de prevenir el abuso en la utilización de los datos y asegurar que la privacidad de los ciudadanos y las empresas colombianas quede debidamente protegida.

Finalmente, deberían tomarse en consideración herramientas que permitan a los ciudadanos de Colombia verificar y certificar que los dispositivos disponibles para la venta no hayan sido robados o de cualquier otra manera ilícitamente importados al país. Un esquema con un buen funcionamiento debería apoyar una forma de seguro para el usuario referente al dispositivo móvil, a bajo costo para los suscriptores móviles en el mercado, para un dispositivo móvil nuevo o revendido, a fin de reducir el riesgo de mantener el mercado para estos dispositivos.

La experiencia de Telcordia

Para abordar este desafío emergente sobre la información, Telcordia ha diseñado un Registro centralizado de información sobre dispositivos (CDIR) a fin de reemplazar la implementación tradicional del EIR y hacer frente a los riesgos emergentes que plantea la clonación, la reprogramación, la falsificación y la producción e importación ilícitas de dispositivos móviles. El CDIR incrementa las bases de datos de suscriptores del operador independiente con un ecosistema centralizado para recolección de datos, análisis, informes y cumplimiento de regulaciones para dispositivos móviles dentro de un país, alimentado por los datos recogidos por los fabricantes, proveedores de plataformas, importadores y operadores.

Mediante la consolidación en un contexto común de la recolección de datos en tiempo real y en tiempo diferido, el CDIR puede enfrentar no solamente los desafíos tradicionales para los dispositivos móviles, tales como antirrobo viable, bloqueo de dispositivo no válido y detección de clonación, sino que también proporciona la semántica del ciclo de vida de los dispositivos y suscriptores móviles en varios puntos centrales de datos (IMEI, IMSI, MSISDN, identificador de la plataforma, etc.), constituyéndose en una valiosa fuente de información para los fabricantes, operadores, reguladores nacionales, aduanas e impuestos, y las organizaciones para la aplicación de la ley y para la seguridad nacional.

Telcordia considera que un enfoque integral, tal como el propuesto, puede contribuir a que Colombia cree un marco sostenible para la cooperación entre todas las partes interesadas, ofreciendo incentivos para cada actor que tome parte en el programa.

II- Comentarios de Telcordia al borrador del Proyecto de Resolución

Este documento tiene por objeto hacer aportes adicionales por parte de Telcordia a los artículos del proyecto de resolución, ya sea para abordar preocupaciones específicas, o para sugerir mejores prácticas o enfoques alternativos para los objetivos de la regulación.

Al Artículo 1
Telcordia sugiere que los objetivos que la norma persigue sean más amplios, y que por tanto haga mención de la necesidad de abordar la prevención de la clonación, la falsificación, la reprogramación y la importación ilegal de dispositivos no declarados y sin certificar, además de la redacción haciendo referencia exclusivamente al alcance en cuanto a dispositivos robados o perdidos. En la medida que todos estos factores están relacionados entre sí en el resto del borrador del Proyecto de Resolución, nos parece que un lenguaje más amplio daría cabida a amplias facultades para la recolección de los datos adecuados, sobre los cuales basar un ecosistema operativo para el registro.

Además, creemos que la tecnología moderna para el registro no debería tener ningún problema en la identificación de los dispositivos robados que operan en las redes móviles domésticas en Colombia, sin importar la procedencia de la red anfitriona del suscriptor. Sugerimos que los objetivos del Registro centralizado incluyan el bloqueo de cualquier dispositivo considerado como ilícito o robado según las reglas propuestas por la CRC.

Artículo 2
Telcordia sugiere la adición del término "único a nivel mundial" a la definición del IMEI, y la exigencia de que dicho IMEI sea asignado por un organismo reconocido a nivel mundial. En este momento, el único proveedor de tales números IMEI a nivel mundial es la GSMA.

Artículo 9
Telcordia sugiere que a cualquier persona sindicada de reprogramación, clonación o de cualquier otra manipulación de un dispositivo móvil sin el permiso expreso del fabricante responsable del móvil le sea suspendida la reventa de dispositivos móviles; a los condenados se les debe revocar la licencia.

Por otra parte, a las instalaciones legítimas certificadas por el fabricante que sigan las instrucciones del mismo se les debe permitir la reparación, el alistamiento para otro dueño y la actualización de los dispositivos móviles, sin temor a perder su licencia para la venta.

Artículo 15
En la sección 15.10, la CRC sugiere un régimen de notificación y aceptación para el uso de dispositivos móviles importados. Dado que un dispositivo puede satisfacer requerimientos específicos, tales como la activación a través de un sistema de activación por fabricante o plataforma y el uso de un número de IMEI único, este proceso podría ser automatizado y controlado a través de un diálogo alternativo, incluso a través de SMS. Para los dispositivos que presentan comportamientos sospechosos, tales como la presencia de un IMEI que no sea único o que no cumpla con las normativas colombiana en cuanto a salud, seguridad o certificación, se sugiere que una Persona autorizada para la venta de Equipos Terminales Móviles debería certificar en persona el dispositivo para su uso en el país y que tales afirmaciones sean auditadas y seguidas de acuerdo con la autoridad licenciada.

Proponemos una nueva sección 15.18 de la siguiente manera: "15.18. Tener el equipo necesario y suficiente y los medios de transmisión disponibles para la comunicación desde la red de señalización del PRSTM a la BDA".

Esto es con el fin de soportar los sondeos en tiempo real necesarios para la detección de patrones en la BDA, como por ejemplo para la detección avanzada de clones y la detección de la excesiva movilidad de la SIM, tal como se describe en forma más detallada en los comentarios de Telcordia sobre el Documento de soporte, sección 3.1.3.1.

Artículo 16
En la sección 16.3, Telcordia sugiere que todos los productos importados tengan un Código de homologación asignado por la GSMA y que cumplan las normas colombianas para la certificación funcional del dispositivo móvil, ya sea como lo documente un proceso independiente o mediante la aceptación del régimen de certificación de otra jurisdicción (la FCC de los Estados Unidos, CE, etc.).

Artículo 17
Proponemos una nueva sección 17.9, que exija a los Fabricantes de dispositivos proporcionar datos si han recogido información bajo los regímenes de activación y registro de dispositivos móviles que involucren suscriptores dentro de la jurisdicción colombiana, incluyendo nombre completo, dirección, información demográfica, IMEI, IMSI, MSISDN, e identificador único de plataforma (tal como un nombre de usuario funcional o dirección de correo electrónico vinculada con el suscriptor) dentro de los ocho días de la activación o del registro, así como proporcionar un medio para consultar estos datos en tiempo real cuando los dispositivos ingresen en su jurisdicción en forma demostrable, haya sido originalmente vendido o no el dispositivo dentro de sus fronteras.

Artículo 18
En la sección 18.4, se sugiere aclarar que deben utilizarse estándares abiertos cuando estén disponibles. Pero en los casos en que estas interfaces o normas no existan, el administrador de la BDA establecerá requisitos comunes para estas interfaces, de acuerdo con las mejores prácticas del sector.

En la sección 18.10, proponemos que la CRC requiera la disponibilidad del registro centralizado con el objetivo a lo largo de todo el sistema de 99,95 % anual, con las excepciones por mantenimiento programado, en vez de la disponibilidad del 100% asignada por el requerimiento enumerado.

En la sección 18.12, estamos de acuerdo con la necesidad de asegurar la privacidad de los datos en el esquema, pero para el artículo 23 sugerimos poner a un lado a los usuarios aprobados por la CRC. La totalidad de estos usuarios requerirán la aprobación por separado por parte de la CRC luego de la evaluación del administrador de la BDA. Como ejemplos de tales usuarios se pueden citar los fabricantes de dispositivos, los distribuidores autorizados, los revendedores de equipos usados, los centros de reparación y las empresas que tramitan solicitudes de seguros. Los ejemplos de utilización son el aseguramiento de la importación por parte del fabricante del dispositivo, la garantía de la validez del dispositivo en el país y la validación de su legítima cadena de custodia.

Proponemos una nueva sección 18.18 del siguiente modo: "**18.18.** Se encargará de actualizar la información de IMEI contenida en la BDA con la información en la IMEIDB de la GSMA y otras bases de datos sectoriales, nacionales y regionales que sean aprobadas por la CRC". Esta propuesta haría que la BDA, en lugar de los PRSTMs, tuviera la obligación de conectarse a la IMEIDB de la GSMA y a otras bases de datos sectoriales, nacionales y regionales que sean aprobadas por la CRC. La centralización de la función, en lugar de su descentralización sobre la base de cada PRSTM, promueve (1) una estructura reducida de costos industriales por PRSTM y la totalidad de la industria, a ser establecida, operada y ampliada con el paso del tiempo, (2) la uniformidad, integridad y seguridad de los datos de acuerdo con los requerimientos del sector, (3) la evolución oportuna a medida que cambian los requisitos del sector, (4) la pro actividad por parte del ABD para llevar a cabo las mejoras.

Artículo 20
Los pares IMEI-IMSI en la base de datos negativa deberían permanecer prohibidos indefinidamente a partir de la fecha del informe, a menos que sean trasladados a la base de datos positiva, ya que es probable que cualquier identificador llevado a la lista negativa seguirá siendo un problema persistente y no se puede asignar para su reutilización de acuerdo con las normas actuales de la GSMA.

Los datos históricos sobre el emparejamiento IMEI-IMSI se mantendrán en la BDA durante un extenso período; se sugiere, como mínimo, tres años para el almacenamiento de estos emparejamientos. Estos datos soportarán los análisis para la detección de clonación, reprogramación y otras actividades ilícitas, así como proporcionarán un medio mediante el cual probar la propiedad y la identidad de cada uno de los dispositivos móviles en caso de su recuperación.

Además, sugerimos que la CRC permita el seguimiento histórico de los abonados móviles dentro de los PRSTMs individuales, ya sea mediante el par IMEI-IMSI o la tripleta IMEI-IMSI-MSISDN, a opción de la BDA, con el acceso a la consulta de los HLRs del PRSTM para la resolución de IMSI a MSISDN, sin costo alguno, en los casos en que el PRSTM sea incapaz de proporcionar la tripleta. Esto es para asegurar que la función analítica apropiada a través de los operadores y los abonados no resulten bloqueados accidentalmente durante los procesos de portabilidad de número, así como para proporcionar un medio por el cual la BDA pueda ponerse en contacto con los suscriptores cuando los dispositivos estén bloqueados o designados como no válidos, y para servicios de restitución de calidad basados en SMS, tales como la recuperación de derechos de importación o del IVA por parte del gobierno.

Artículo 21
Telcordia cree que las bases de datos positiva y negativa serán derivadas de los datos recogidos y procesados a través de un marco analítico, y podrían variar dependiendo de la parte que consulta y el propósito de la consulta. Ya que el contexto de la consulta podría impartir una respuesta positiva o negativa, sugerimos que la delimitación entre las bases de datos positiva y negativa pueda requerir una separación virtual, en vez de física, de las dos listas.

Como la lista positiva no tendría ningún impacto funcional sobre el registro de dispositivos móviles en el PMNS, sugerimos que cualquier implementación activa de bloqueo en un PRSTM podría requerir sólo de la generación de una base de datos negativa para la ejecución en tales sistemas.

Artículo 22
Telcordia preferiría ver una descripción más funcional en cuanto a lo esperado, los métodos utilizados y los datos recogidos por el esquema del Modelo Único de Ingresos, Servicio y Control Automatizado - MUISCA existente, a fin de entender mejor la interfaz y eficacia de este sistema con miras a los objetivos buscados en la propuesta regulatoria.

Artículo 23
Telcordia propone una visión más amplia sobre el acceso a los datos recogidos y gestionados dentro de la BDA para los usuarios autorizados por la CRC. La totalidad de estos usuarios requerirán la aprobación por separado por parte de la CRC luego de la evaluación del administrador de la BDA.

Como ejemplos de tales usuarios se pueden citar los fabricantes de dispositivos, los distribuidores autorizados, los revendedores de equipos usados, los centros de reparación y las empresas que tramitan solicitudes de seguros.

Un ejemplo de uso es el acceso a los datos de dispositivos anónimos solicitado por los fabricantes de dispositivos móviles al auditar sus propios procesos de importación para la investigación de robos de dispositivos a granel y de la importación del mercado gris, o por parte del PRSTM al analizar la distribución de los dispositivos de abonados. Otro ejemplo de uso es el asegurar la validez del dispositivo en el país y validar su legítima cadena de custodia.

Telcordia sugiere un proceso, con costo, de revisión de la privacidad por parte del proveedor de la BDA y la revisión por parte de la CRC de tales solicitudes, en lugar de la restricción amplia de las mismas, para hacer frente a tales solicitudes legítimas de datos, así como cargos transaccionales que cubran el costo del procesamiento y suministro de los datos.

Artículo 24
Telcordia propone una sección adicional para permitir que los fabricantes de dispositivos y los terceros distribuidores mayoristas informen los dispositivos robados al ABD para su inserción en la BDA. Un registro tal puede involucrar el robo de grandes cantidades de dispositivos. Esta regulación debería permitir este tipo de informes a fin de que la BDA mantenga una lista negra efectiva.

Artículos 24 y 25
Telcordia cree que debería existir espacio para la detección activa, la restricción y, en algunos casos, el bloqueo de los dispositivos móviles que cumplan con los requerimientos específicos establecidos por la CRC. Los casos candidatos incluyen dispositivos prohibidos, IMEI inválido, múltiples IMEIs clonados operando en forma simultánea posiblemente a través de múltiples PRSTMs, evaluaciones inválidas de IMEI y masificación ("churning") de SIM. Esta regulación debería permitir dicho bloqueo y proporcionar un medio por el cual el operador de la BDA pueda proponer y hacer aprobar este proceso alternativo.

También sugerimos que el plazo para el bloqueo sea de 30 minutos tanto en el Artículo 24 como en el Artículo 25 para la resolución de las listas negativas y positivas a fin de tener en cuenta el retraso inherente a los sistemas distribuidos, y para prevenir el impacto de la actualización sobre las redes del PRSTM durante las horas pico de utilización.

Telcordia también sugiere que en los dispositivos con múltiples identificadores de IMEI, tales como los teléfonos con SIM doble, el bloqueo de un número de IMEI en un único dispositivo físico, debería también demandar la obstrucción de todos los IMEI asociados con ese dispositivo físico.

Artículo 27
Una vez más creemos que la opción de la tripleta IMEI-IMSI-MSISDN, o alternativamente el par IMEI-IMSI con acceso al HLR del PRSTM para la resolución del MSISDN, es un factor crítico en el éxito de la seguridad cruzada entre PRSTMs.

En la sección 27.4, la experiencia nos ha demostrado que el proporcionar la prueba de propiedad de los dispositivos móviles comprados en el extranjero es a la vez engorroso y difícil de hacer cumplir activamente por varias razones, incluyendo la facilidad de falsificación de los recibos, las barreras idiomáticas y la declaración inconsistente del IMEI en las listas de materiales. En lugar de exigir la prueba de la venta, Telcordia sugiere un régimen de registro obligatorio, ya sea soportado con los datos de activación del fabricante o a través de un proceso manual a ser definido por la BDA y aprobado por la CRC.

Además, el ABD podría verse obligado a recaudar los derechos de importación del abonado a través del proceso de restitución del PRSTM con base en la justa valoración de mercado del dispositivo móvil antes de que el dispositivo sea completamente aceptado en la lista de dispositivos aprobados a nivel nacional. Esta práctica ya está en marcha manualmente en Turquía, aunque Telcordia sugiere que un proceso automatizado es más adecuado.

En la sección 27.7, recomendamos que la CRC investigue la legislación que castiga la clonación, la reprogramación y la importación de equipos con números de IMEI inválidos o que no sean únicos a nivel mundial, similar a la legislación del Reino Unido sobre la clonación. El alcance debe incluir a aquellos que crean, distribuyan y comercialicen equipos y software que se utiliza para cambiar el IMEI. También se recomienda la prohibición de dispositivos sin ningún tipo de número de IMEI, en forma similar a la legislación aprobada por la India en 2009 a raíz de los atentados terroristas de 2008 en Mumbai.

Artículo 28
Ya que el operador de BDA puede ser el único participante que visualice múltiples instancias de un IMEI, por ejemplo, si se producen a través de múltiples PRSTMs, se sugiere que el operador de BDA y los PRSTMs trabajen conjuntamente para identificar y eliminar los dispositivos que no cumplen, durante el período de transición.

Artículo 33
Teniendo en cuenta el esfuerzo para obtener con precisión la "huella digital" de las redes móviles nacionales, establecer los suministros de datos para las fuentes de datos colombianas y del fabricante, implementar mecanismos comunes para recolección de datos y para la aplicación en las redes de PRSTM, y realizar una desactivación ordenada de los dispositivos que no cumplen, Telcordia sugiere que la ventana de implementación para su pleno funcionamiento sea ampliada a nueve meses después de

la adjudicación del contrato para el proveedor de la BDA, con hitos incrementales a ser acordados entre el proveedor de la BDA y la CRC, a fin de lograr las metas de cumplimiento.

Artículo 34
Dado el gran número de dispositivos móviles activos hoy en día en Colombia, Telcordia sugiere la aplicación de "derechos adquiridos" a los dispositivos móviles identificados durante la reimplementación, para los que se determine que estén utilizando IMEIs únicos antes de una fecha determinada, con el fin de minimizar las interrupciones durante la ventana de activación y poner restricciones más amplias sobre los dispositivos nuevamente activados después de esa fecha. Los dispositivos que coincidan con los patrones de clonación, reprogramación u otros ilícitos, o a los que les falten por completo los números de IMEI requerirían la certificación de acuerdo con el proceso propuesto en esta sección.

Comentarios sobre la documentación de soporte

Telcordia entiende que la documentación de soporte existe para aclarar y articular aún más la intención de la regulación subyacente sin sobrecargar la propia regulación con lenguaje innecesariamente complejo o requerimientos técnicos inflexibles. Sin embargo, Telcordia quisiera una orientación adicional sobre si la documentación es de carácter consultivo o si los requerimientos incluidos en la documentación son de carácter obligatorio para cualquier administrador futuro, pues desde ya Telcordia quisiera poder participar en cualquier proceso a llevarse a cabo para desarrollar o implementar las listas positivas o negativas, y administrar dicha base de datos. Aunque muchos de los requerimientos y procesos coinciden con las soluciones que hemos desarrollado, hay varios métodos alternativos para cumplir con los objetivos de políticas similares que con gusto podemos poner a su disposición para efectos de una futura contratación del administrador de la base de datos.

Sección 3.1.1.1

Telcordia tiene entendido que los modelos, tal como se presentan en esta sección y las subsecciones siguientes, son solamente para fines ilustrativos y no representan una arquitectura obligatoria para la implementación.

Telcordia sugiere que la BDA, en lugar de los PRSTMs, sea la que tenga la obligación de conectarse a la IMEIDB de la GSMA y a otras bases de datos sectoriales, nacionales y regionales que sean aprobadas por la CRC. Los datos descargados en Colombia por la BDA se integrarían con los datos distribuidos a los PRSTMs de acuerdo con los convenios del sector en Colombia. Los datos cargados desde Colombia por la BDA a la IMEIDB de GSMS y a otras partes potenciales seleccionadas estarían de acuerdo con los convenios del sector en Colombia. La centralización de la función, en lugar de su descentralización sobre la base de cada PRSTM, promueve (1) una estructura reducida de costos industriales por PRSTM y la totalidad de la industria, a ser establecida, operada y ampliada con el paso del tiempo, (2) la uniformidad, integridad y seguridad de los datos de acuerdo con los requerimientos del sector, (3) la evolución oportuna a medida que cambian los requisitos del sector, (4) la pro actividad por parte del ABD para llevar a cabo las mejoras.

Sección 3.1.1.2.1

La lógica booleana que soporta la consulta propuesta tanto a una base de datos positiva de ~45M registros y a la base de datos negativa durante el registro de cada dispositivo representa una sobrecarga sobre la red móvil. Teniendo en cuenta que un resultado positivo no tendría ningún impacto en el registro del dispositivo, Telcordia sugiere que sólo se requiera a los PRSTMs el comparar contra la lista negativa al registrar el dispositivo.

Además, la capacidad para consultar la infraestructura del EIR varía entre los fabricantes de MSC; la aclaración de que el objetivo final consiste en que la consulta a la base de datos negativa antes del registro inicial exitoso sea permitida por el PRSTM debería constituir un umbral adecuado para el cumplimiento.

Sección 3.1.1.2.1

El proceso de comprobación del PRSTM sobre su BDO cubre también el escenario de los eventos de inserción de la SIM. De ese modo se comprobará el cambio resultante de IMSI para el mismo IMEI.

Sección 3.1.2.1

Proponemos como objetivo para todo el sistema una disponibilidad del 99,95 % anual, con la sustracción adecuada para los intervalos aprobados en cuanto a mantenimiento y actualización.

Sección 3.1.3.1
Telcordia sugiere la aplicación de una sonda de recolección de datos, según lo especificado por el administrador de BDO, que se colocará en cada red de PRSTM para facilitar mecanismos de recopilación de datos persistentes y normalizados en tiempo real, a través de todas las redes participantes. Esto se puede hacer de una manera que no resulte molesta y afecte mínimamente a los entornos de red del PRSTM. Tengan en cuenta que las sondas son pasivas y no están activas en las consultas desde MSC/SGCN a la BDO.

Este mecanismo puede ser utilizado durante el período de transición para detectar y registrar la actividad real del dispositivo en las redes de PRSTM. Esto proporciona un método proactivo, basado en los hechos y económico para poblar inicialmente la BDA en forma cruzada entre PRSTMs.

Este mecanismo debería seguir utilizándose después del período de transición para detectar y registrar la actividad real del dispositivo en las redes de PRSTM. Esto proporciona un mecanismo proactivo, basado en los hechos, para llevar a cabo la recopilación de datos normalizados desde las redes PRSTM para complementar otros aportes, tales como los provenientes de la BDO del PRSTM, de los fabricantes y ensambladores nacionales, la base de datos de importación MUISCA, y la GSMA. Como resultado, se pueden implementar algunas detecciones avanzadas, tales como:

> Detección avanzada de clones. Esto ocurre cuando un dispositivo y una tarjeta SIM, con un par IMEI-IMSI en la lista blanca y que no están en la lista negra, han sido clonados. Un enfoque consiste en analizar de forma proactiva los registros de actividad del dispositivo con marca de tiempo para detectar la potencial concurrencia de pares IMEI-IMSI duplicados a través de múltiples PRSTMs.
> Detección de patrones sospechosos de comportamiento con posible problema de seguridad. Un ejemplo es la masificación ("churning") de la SIM" en la cual, llamada por llamada, una persona usa y descarta tarjetas SIM en el mismo dispositivo, potencialmente a través de múltiples PRSTMs. Un enfoque consiste en analizar de forma proactiva los registros de actividad del dispositivo con marca de tiempo para detectar la utilización secuencial prácticamente coincidente de múltiples IMSIs para un determinado IMEI.

Sección 3.1.3.1.1

Error tipográfico para el Caso 1: En vez de "no menos de" deberá decir "no más de".

Casos 2 y 4: El número de clones podría estar en el rango de decenas, centenas o miles, de tal modo que informar a todos los usuarios y descubrir el usuario válido podría ser impracticable. Sería más apropiado bloquear el IMEI, a pesar de que esto interrumpa la operación del usuario válido.

Sección 3.2.1

Telcordia sugiere que el marco temporal sea normalizado con los requerimientos de los Artículos 23 y 24.

Sección 3.2.2

Telcordia sugiere que los usuarios dispongan de un método, sujeto a pago, para confirmar la legitimidad de un dispositivo central en la BDA centralizada.