

Informe de la 19ª Llamada de Consulta de la A2ii y la IAIS

Desafíos de la protección de datos en los seguros móviles

24 de noviembre de 2016



Las llamadas de consulta de la A2ii son organizadas junto con la IAIS para proporcionar a los supervisores una plataforma de intercambio de experiencias y lecciones aprendidas en la ampliación del acceso a los seguros.

La 19ª Llamada de Consulta, llevada a cabo el 24 de noviembre de 2016, se centró en explorar los desafíos de la protección de datos generados por los modelos de negocios de seguros móviles. Se realizaron cuatro llamadas: dos en inglés, una en francés y una en español.

Los expertos técnicos Dr. Nicola Jentzsch (consultora) y Andrea Camargo (Directora de Regulación y Protección al Consumidor de la de la Microinsurance Catastrophe Risk Organisation, MiCRO) exploraron riesgos importantes en la privacidad y protección de datos luego de aplicar análisis de Big Data a la oferta de seguros así como también consideraciones regulatorias para supervisores. Los expertos de país Eugene Du Toit (del Consejo de Servicios Financieros de Sudáfrica) y Ranferi Gómez (de la Comisión Nacional de Seguros y Finanzas de México) compartieron su experiencia en protección de datos y seguros móviles en sus respectivas jurisdicciones.

Introducción al seguro móvil

El seguro móvil, o la oferta de productos de seguros por el ecosistema de telefonía móvil, ha crecido rápidamente en todo el mundo. Para junio de 2015, la industria de seguros móviles ofrecía 120 servicios de pólizas de vida con 31 millones de pólizas activas en 33 mercados emergentes¹. La proliferación del seguro móvil, no solo en términos de escala sino también de cobertura, ha creado un mercado grande y creciente de enorme impacto potencial.

Tendencias de los seguros móviles en el mercado de microseguros

La industria de microseguros ha estado en constante crecimiento en los últimos años. La primera evaluación global² realizada en 2007 reveló que existían casi 80 millones de clientes de microseguros en el mundo. En 2013, esta cifra había crecido a más de 263 millones. Hoy en día, muchos expertos opinan que las cifras se han vuelto a duplicar. Gran parte de este crecimiento se debe a la propagación de productos de seguros móviles que pueden crecer muy rápidamente. Las tasas de crecimiento anual muestran que mientras los mercados maduros de seguros crecen a aproximadamente 2-4% al año y los mercados emergentes de seguros crecen en un aproximado de 10-12% anual, los mercados de microseguros móviles tienen un crecimiento anual del 100% o más. Por ejemplo, Tigo, un proveedor de servicios técnicos en Ghana, alcanzó un millón de clientes solo un año después de haberlos lanzado, y en Bangladesh, Grameenphone y MicroEnsure alcanzaron un millón de clientes en 30 días. La aplicación de la tecnología digital en seguros inclusivos ha cambiado drásticamente el panorama de esta última y se presenta prometedora para el futuro.

“ Se necesita solo un año para alcanzar un millón de pólizas de vida vía los ORM en comparación con los 40 años que toma en un mercado típico de aseguramiento ”

Accenture

¹ GSMA, 2015. *Mobile Insurance, Savings & Credit Report*. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf>

² Accenture, 2014, *Mobile Microinsurance (MMI): goes from experiential to exponential*. Presentación por Thomas Meyer en la Conferencia Internacional de Microseguros (CIM), México.

Figura 1.



Fuente: Inclusivity Solutions

Características de los modelos de negocios de seguros móviles

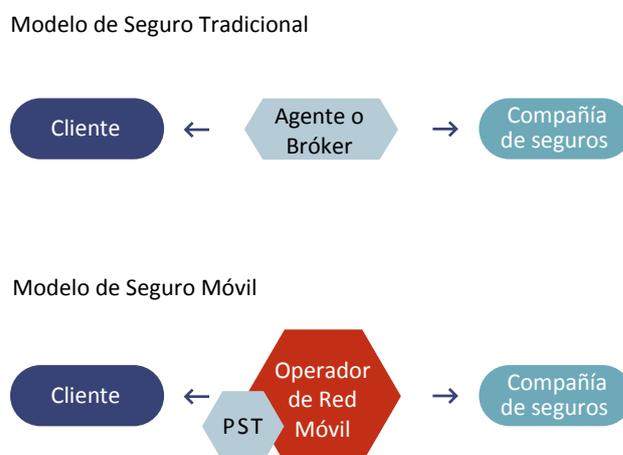
Un modelo de seguros móviles es un modelo de negocios de seguros que utiliza el canal telefónico móvil en cualquier momento del ciclo de vida del producto de seguros. El número y naturaleza de las nuevas entidades participantes, la digitalización de la cadena de valor de los seguros y la aplicación de análisis Big Data son las características principales que diferencian a los modelos móviles del negocio tradicional de seguros.

Surgimiento de nuevos actores

Una de las características definitorias de los modelos de seguros móviles es la introducción de nuevos actores en la cadena de valor de los seguros. Mientras que la estructura tradicional de modelos de seguros se caracteriza por contar con el cliente, la aseguradora y el agente o bróker intermediario, los modelos de seguros móviles introducen múltiples nuevos actores en la cadena de valor que tienen su origen fuera de la esfera de los seguros: operadores de redes móviles (ORM) u otras redes de apalancamiento de agregadores / comercializadores terciarios que potencian las redes y proporcionan seguros a un gran número de clientes pre-existentes, mientras que los proveedores de servicios técnicos (PST) actúan como intermediarios entre la aseguradora y los ORM proporcionando la infraestructura para la administración y pagos aunque también a veces participan en el diseño de producto. Cualquiera de las tres partes interesadas puede tomar la iniciativa de proporcionar seguros. Sin embargo, usualmente son los ORM los que toman la iniciativa. Un estudio reciente demostró que el 63% de los servicios de seguros móviles era dirigido por ORM³. Cuando una aseguradora toma la iniciativa, el ORM asume un rol principalmente pasivo, apoyando con las transacciones a través de su operador móvil y/o infraestructura monetaria móvil, mientras que la aseguradora, que es regulado por un supervisor de seguros, suscribe el producto. En modelos liderados por ORM, se permite a la aseguradora usar la data del ORM para captar e inscribir clientes. En este modelo el ORM aporta su considerable fuerza de marca para estimular la suscripción del seguro ya que el producto está incorporado al paquete que ofrece el ORM. Estos ofrecen seguros para aumentar la lealtad del cliente, reducir la rotación, crear reconocimiento de marca y/o aumentar el ingreso promedio por cliente. La inversión por parte de los ORM puede incluir el pago de primas a nombre de sus suscriptores, aprovechando su propia infraestructura, el uso de Big Data para identificar clientes objetivo, y/o cofinanciar el marketing y la publicidad. El ORM, como agregador, mantiene la base de clientes, y aporta una 'marca de confianza' y un mecanismo de recaudación de primas. Los ORM no están tradicionalmente bajo la jurisdicción de un supervisor de seguros.

³ GSMA, 2015. *Mobile Insurance, Savings & Credit Report*. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf>

Figura 2. Modelo de Seguro Tradicional | Modelo de Seguro Móvil



Estos nuevos actores junto con las alianzas orientadas a la tecnología están impactando la cadena de valor y el equilibrio de poder en el mercado de seguros, haciendo surgir desafíos particulares para los supervisores. Más aún, la inclusión de nuevos actores ajenos a la esfera de seguros podría desalinear los incentivos entre estos y las aseguradoras, condicionando las ventas y, potencialmente, distorsionando la percepción del seguro por el cliente, ejerciendo presiones a la baja en la demanda.

Digitalización de la cadena de valor de seguros

La penetración de nuevos modelos de negocios se debe en gran parte a la mayor eficacia y menores costos de transacción gracias al uso de las tecnologías de información en cada etapa de la cadena de valor de los seguros. El uso de datos de las redes móviles facilita en gran medida la captación de clientes, el diseño y distribución de productos, y el manejo de las relaciones con los clientes. El uso de tecnología en las alianzas de seguros móviles tiene el potencial de superar muchas de las barreras tradicionales que existen en el ciclo de vida de los seguros inclusivos, permitiendo en última instancia el crecimiento.

- **La generación de datos digitales, la comunicación y la analítica** se usan para que las aseguradoras conozcan los patrones de comportamiento y preferencias de los clientes. El procesamiento de grandes cantidades de información digital puede revelar la inclinación del cliente a tomar un seguro o estimar su disposición a pagar por el seguro. La analítica de datos digitales y la creciente integración de datos permiten a las empresas mejorar sus capacidades de predicción. Estos análisis pueden apalancarse para mejorar la focalización de los clientes, el marketing, el diseño de productos, para adaptar la distribución y para reducir la rotación.
- **Contratación digital.** Los teléfonos móviles ofrecen un canal de fácil acceso y bajo costo para comunicarse con posibles clientes y suscribir pólizas utilizando firmas electrónicas.
- Para **reducir costos de distribución**, los proveedores de seguros optan por aliarse con agregadores terciarios para facilitar la venta de productos y la recaudación de primas. Las empresas aseguradoras se montan sobre la base de clientes e infraestructura digital de sus socios para reducir costos y llegar a los clientes de bajos ingresos fuera de los puntos de distribución tradicionales.

- La **recaudación de primas** vía canales móviles es menos costosa para la aseguradora y más conveniente para el mercado objetivo donde los asegurados a menudo no están bancarizados. Frecuentemente, las primas se descuentan con tiempo de llamadas/datos de un ORM o usando la infraestructura de dinero móvil.
- **Liquidación de reclamos.** Los teléfonos móviles pueden facilitar los reclamos y su liquidación, por ejemplo cuando los pagos se hacen mediante billeteras electrónicas. Los problemas tradicionales de la liquidación de reclamos, tales como la falta de infraestructura o cuando los consumidores carecen de documentación apropiada, se superan gracias a los agregadores / comercializadores terciarios debido a que las relaciones ya existentes con los clientes y los flujos de pagos pueden aprovecharse para que permitan aceptar y liquidar las solicitudes de pago de siniestros.
- **Modelamiento de riesgos.** La aplicación de algoritmos sofisticados a grandes bases de datos puede ayudar a los proveedores a perfilar y modelar mejor el riesgo aceptado y aumentar la eficiencia del diseño de productos, selección de riesgos y fijación de precios de primas.

Análisis de Big Data

Al aprovechar la infraestructura móvil a través del análisis de Big Data, las aseguradoras tienen más oportunidades de abrir camino más rápidamente a nuevos productos para un mayor número de consumidores. El término Big Data se refiere a las grandes cantidades de información digital en forma de conjuntos estructurados y no estructurados de datos, cuyo uso aumenta la eficiencia y eficacia del proceso de aseguramiento en un grado sin precedentes. La información Big Data se caracteriza por las tres 'v': (i) volumen de datos muy grandes (tera y petabytes); (ii) velocidad de acumulación (usualmente en alta frecuencia en tiempo real); y (iii) variedad (patrones de llamadas de móviles, blogs, registros de los centros de llamadas, etc.)⁴. La transmisión de información computarizada ayuda en la recopilación en tiempo real de datos y permite a las aseguradoras establecer relaciones directas y no mediadas basadas en el acceso directo a datos no filtrados. Este mapeo de preferencias y patrones de comportamiento permite a las aseguradoras entender con mayor precisión quiénes son sus clientes y cómo cambian sus necesidades con el paso del tiempo y así poder hacerles propuestas personalizadas.

La implementación de nuevas tecnologías y el procesamiento mediante analítica en la infraestructura móvil amplían el entorno de interconexión e intercambio de información que, por su potencial de llevar los seguros a millones y millones de personas no aseguradas, crea nuevos desafíos en temas de privacidad, protección de datos y seguridad cibernética.

Creciente preocupación por la privacidad

A pesar de los potenciales beneficios de los seguros móviles, la creciente adopción del procesamiento de información generalizado y a veces invasivo ha aumentado las preocupaciones por la privacidad en todo el mundo. Un estudio reciente realizado por KPMG⁵ en más de 24 países indica que en 2016, el 55% de los consumidores a nivel mundial optó por no comprar nada en Internet debido a su preocupación por la privacidad. En la misma encuesta, 66% de los consumidores indicaron que no se sentían cómodos con que las aplicaciones ("apps") utilizaran su información personal. La mayor preocupación por la privacidad también afecta a muchos países en vías de desarrollo y mercados emergentes. Otra encuesta⁶ con más de 24.000 consumidores de 20 países reveló que el número de consumidores preocupados o muy preocupados por su privacidad ha aumen-

4 Watson, H.J. (2014). Tutorial: Análisis Big Data: Conceptos, Tecnologías y Aplicaciones, <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3785&context=asi>

5 KPMG (2016). Crossing the line: Staying on the right side of consumer privacy, <https://home.kpmg.com/content/dam/kpmg/au/pdf/2016/crossing-the-line.pdf>

6 2016 CIGI-Ipsos Global Survey on Internet Security and Trust, <https://www.cigionline.org/internet-survey-2016>

tado significativamente comparado al año anterior. Este aumento de la preocupación por la privacidad puede crear problemas de confianza, que si no se abordan debidamente, pueden impedir la adopción de servicios de seguros móviles en el futuro.

Protección de datos

La protección de datos suele abarcar medidas de política, legales, normativas y técnicas así como la formulación de protocolos para la protección de datos personales⁷. En general, la protección de datos incluye derechos individuales de protección (como el derecho al acceso a los datos, a corregirlos, etc.) y normalmente concierne a los individuos, no a las empresas. Dependiendo de la situación del país, existe una variedad de leyes aplicables a la protección de datos.

Los derechos fundamentales de la protección de datos de las personas usualmente incluyen reglas como la transparencia del procesamiento de datos, en otras palabras, las organizaciones que recopilan datos personales deben exponer abierta y claramente las cuestiones de procesamiento. Los datos personales deben ser recopilados para propósitos limitados y legales y no ser usados para otros propósitos ajenos a los indicados en el momento de su obtención. También debe especificarse la razón por la cual son revelados. En muchos regímenes normativos, los individuos cuentan con el derecho de dar su consentimiento para el procesamiento de sus datos lo cual es importante ya que aumenta la transparencia del proceso. Además, las leyes de protección de datos también incluyen medidas técnicas de seguridad y de procesamiento para evitar el acceso no autorizado a los datos. Entre otras disposiciones se incluye que los datos deben ser relevantes, exactos y actualizados y que el sujeto de los datos debe contar con el derecho de acceder a sus datos y corregirlos si es necesario.

Desafíos de la protección de datos en los seguros móviles

Propiedad de datos y responsabilidad

Uno de los principales desafíos que surgen de los modelos de seguros móviles es el problema de la propiedad de los datos y su distribución. Quién exactamente es el propietario de los datos del cliente y quién es responsable de su protección y/o difusión es un tema complejo que a menudo depende del modelo de negocio y de los acuerdos de servicio entre las entidades involucradas. Mientras que el Operador de Red Móvil (ORM) posee todos los datos del consumidor que se recopilan por medio de la red móvil, otras entidades como los PST pueden ser subcontratadas o asumir funciones por las cuales se les concede el acceso a los datos de los clientes en la base de datos de los ORM. Por ejemplo, se puede proporcionar a los PST datos con el fin de participar en la preselección de clientes para ofrecerles seguros. Esto permite a los PST contactar directamente al cliente a fin de establecer una relación y recopilar directamente información adicional sobre el cliente, información que se compartirá luego con un proveedor de seguros para intermediar un contrato. Este flujo libre de transferencia de datos resalta la importancia de las cuestiones de privacidad y protección de datos ya que este procesamiento se realiza a menudo de forma no transparente y sin el debido consentimiento de los consumidores.

⁷ Según la nueva Regulación General de Protección de Datos de la UE, los 'datos personales' se pueden definir como "... cualquier información relacionada con una persona natural identificada o identificable ('sujeto de datos'); una persona natural identificable que puede ser identificada, directa o indirectamente, en particular mediante un identificador tal como el nombre, número de identificación, localización, identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de la persona natural". Fuente: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

Cambios fundamentales introducidos por modelos de negocios de seguros móviles

Asimetrías de información

Los seguros móviles introducen un cambio fundamental en las asimetrías de información que existen en el mercado, no solamente entre clientes y firmas, sino también entre empresas y supervisores. Una vez que las empresas realizan análisis de Big Data, procesan la información de forma que en gran parte no es transparente para los consumidores. Cuando un cliente solicita un seguro, renuncia a la privacidad de su información personal que es proporcionada por sus datos digitales. A menudo los consumidores no tienen muy claro hasta qué punto ceden este activo intangible; es decir, el tipo de datos personales usados para la estimación y el tipo de análisis de datos que se lleva a cabo. Los clientes no pueden determinar cuál sería la compensación adecuada por dar su consentimiento informado ya que no queda claro cuánta información se procesa y analiza. La falta de conocimiento de los clientes plantea importantes preocupaciones de protección del consumidor relacionadas con la necesidad de preservar sus derechos básicos intrínsecamente asociados con la recopilación y procesamiento de información. Por otro lado, a menudo se capta clientes recurriendo a desequilibrios de poder que no les permiten acceder a otras formas de adquirir un seguro. En otras palabras, para tener el seguro, deben aceptar lo que se les ofrece.

En lo que se refiere a las firmas y supervisores, mientras que los supervisores tienen la tarea de monitorear las firmas que utilizan análisis de Big Data, estas empresas a menudo utilizan modelos sofisticados que complican la supervisión. El uso de máquinas inteligentes o algoritmos de aprendizaje automático, por ejemplo, incrementa la brecha de conocimientos entre las empresas y los supervisores, lo cual hace que para los supervisores sea muy difícil supervisar adecuadamente a estas empresas. Además, surgen nuevas complicaciones con la cuestión de quién es el responsable de regular a los diferentes actores involucrados. Si bien el regulador de telecomunicaciones supervisa a los ORM y el supervisor de seguros regula a las aseguradoras, el supervisor de seguros también debe coordinar con el regulador de telecomunicaciones para supervisar a los ORM y sus actividades, mientras que los PST están en un área gris. Esta dimensión adicional de la responsabilidad de supervisión aumenta los obstáculos reglamentarios que surgen debido al uso de tecnologías sofisticadas.

Expansión y saturación de mercado

El mercado de seguros suele pasar por dos fases tras la introducción de estos nuevos modelos de negocio. La primera es una fase de expansión del mercado seguida de una fase de saturación. En la fase de expansión del mercado, la caída de los costos de transacción permite a las empresas cotizar más clientes, lo que significa que más individuos que antes no tenían acceso a los seguros, ahora sí lo tendrán y, por lo tanto, aumenta el bienestar general del consumidor. Sin embargo, el mercado se satura por el aumento de la competencia. Las empresas compiten ferozmente por cuotas de mercado y comienzan a personalizar los precios y productos basados en la información que han reunido de cada cliente individual. Esta combinación de precios y productos personalizados provoca una disminución del bienestar de los consumidores, debido a que los proveedores de servicios empiezan a fijar el precio de los productos según la disposición de pago de los consumidores o el nivel máximo de asequibilidad⁸. Por otra parte, una vez que un producto o servicio se adapta a las preferencias de un individuo, es difícil para un individuo comparar ofertas alternativas debido a que otros productos no son comparables ya que tienen características diferentes. Estos incentivos empresariales cambian las estrategias competitivas de las empresas de maneras que pueden hacer que los consumidores estén expuestos a prácticas predatorias.

⁸ Ghose, A. y K.W. Huang (2009). Personalized Pricing and Quality Customization, *Journal of Economics & Management Strategy* 18 (4), 1095-1135. El modelo presentado en este artículo se aplica a los mercados saturados. En un mercado en expansión, el efecto neto en el bienestar de los consumidores puede ser positivo si es que se aumenta el bienestar general gracias a la incorporación de nuevos clientes por mecanismos de precios.

¿Revertir el acceso a los seguros? Saturación del mercado y relegación de los consumidores mediante fijación de precios

P. ¿La saturación del mercado significará que los individuos de bajos ingresos serán eventualmente relegados en el mercado?

Cabe señalar que durante la fase de saturación del mercado la personalización de los precios no es indicador de que automáticamente los clientes de bajos ingresos serán relegados en el mercado. Para maximizar sus utilidades, los restadores de servicios idealmente preferirían fijar el precio de un producto justo por debajo de la disposición a pagar de cada consumidor. Sin embargo, en la práctica esto no siempre sucede. Por ejemplo, si una empresa tiene clientes que han demostrado ser no rentables, la empresa establecerá un precio que los clientes no estarán dispuestos a pagar, por lo tanto, los relegarán. No se puede decir que en etapas posteriores del desarrollo del mercado todas las personas de bajos ingresos serán discriminadas y excluidas del mercado, ya que algunas de ellas podrían ser clientes rentables.

Estrategias competitivas de las firmas

Los modelos de negocio de seguros móviles también cambian las estrategias competitivas de las empresas, principalmente debido a que las compañías de seguros pueden aumentar la información que recopilan y analizan. El uso de procesamiento Big Data permite a las empresas micro-direccionar y pre-seleccionar clientes que presentarían una mayor propensión a responder a una oferta y convertirse en clientes rentables pagantes. Tras la elaboración de perfiles y el registro de clientes pre-seleccionados, las compañías de seguros tratarán de diseñar productos adaptados a las preferencias específicas de un consumidor individual. La no estandarización de estos productos disminuye su comparabilidad general y, por lo tanto, también incentiva a las empresas a aplicar precios individualizados.

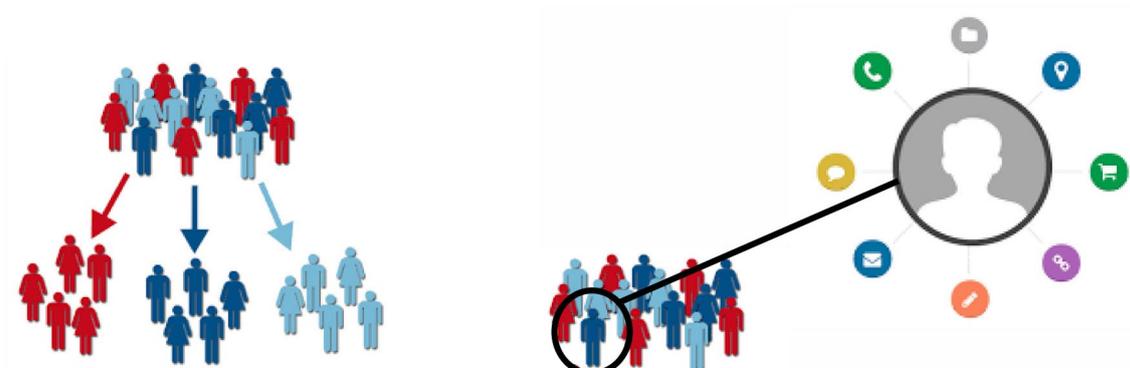
Privacidad: construyendo una visión 360° del consumidor

En los modelos de seguros tradicionales, las aseguradoras realizan segmentaciones del mercado según la demografía y los comportamientos observables de los consumidores, clasificando de manera efectiva a los individuos en diferentes tipos de clientes. Con los seguros móviles y el procesamiento de Big Data, sin embargo, las empresas pueden recurrir a una segmentación personalizada debido al gran volumen de información que recopilan sobre los clientes. La geolocalización de individuos, la duración y volumen de los patrones de llamadas, la duración y dirección de las llamadas son sólo unas cuantas de los cientos de variables utilizadas en el modelamiento de perfiles de consumidores. Estas variables revelan información de segmentación delicada, que abarca desde la red social de un individuo y sus ingresos hasta su estado de salud, sus patrones diarios de desplazamiento e incluso su religión. La información obtenida de la implementación de análisis Big Data se utiliza para construir una visión 360° del cliente que antes no era posible con la segmentación tradicional de mercado.

Consideraciones para supervisores

Con el creciente uso de tecnologías de la información para ofrecer seguros móviles, cada vez más actores del mercado recogen información financiera, geolocalizada y del estilo de vida de las personas. De esta transferencia sin precedentes de información surgen preocupaciones importantes acerca de la privacidad y el procesamiento y la distribución de datos personales, así como desafíos para la protección de los consumi-

Figura 3. Segmentación versus personalización de usuarios



dores derivadas de los cambios en las estrategias competitivas de las empresas. Sin duda existen oportunidades significativas que el seguro móvil ofrece para aumentar el acceso financiero y apoyar el desarrollo socioeconómico. No obstante, es importante que los supervisores aborden las cuestiones derivadas de los seguros móviles y se aseguren de que la regulación facilite el desarrollo del mercado de seguros inclusivos al tiempo que se protege a los asegurados y se mantenga el equilibrio de la estabilidad financiera.

Marco regulatorio

Las estrategias antes mencionadas y los cambios que nacen de estas nuevas configuraciones digitales crean una gran cantidad de preocupaciones para la protección del consumidor. No obstante, los supervisores pueden tomar la iniciativa para abordar estos desafíos mediante una regulación adecuada.

Mientras que en algunas jurisdicciones se está considerando emitir reglamentaciones específicas para seguros móviles, en otras, las normas que generalmente se aplican a los seguros inclusivos también se están aplicando a la reglamentación de seguros móviles y protección de datos. Regular los seguros móviles y los datos del consumidor es a menudo un proceso complejo que abarca muchas autoridades regulatorias y supervisoras, como autoridades de seguros, banca central, telecomunicaciones y protección de datos, entre otros. Varios órganos reguladores incluyen la protección de datos del consumidor entre sus responsabilidades. El panorama normativo de un país, por lo tanto, está conformado por todas o algunas de los siguientes elementos de legislación relevantes: una ley de telecomunicaciones, una ley de seguros, una ley de informe de créditos y una ley de protección de datos.

→ Ley de telecomunicaciones

Normalmente, una ley de telecomunicaciones no contiene extensas cláusulas o reglamentaciones detalladas sobre protección de datos, aunque pueden existir cláusulas dispersas de confidencialidad que requieran que las firmas mantengan la privacidad de los datos de los clientes y de los métodos comerciales. Esto se debe a que el objetivo principal de la ley de telecomunicaciones es reglamentar el mercado de telecomunicaciones, por ejemplo, encargándose de temas como otorgar licencias a empresas de telecomunicaciones y crear una autoridad para la regulación del sistema de telecomunicaciones. Las medidas de protección de datos no se encuentran explícitamente delineadas en la legislación de telecomunicaciones.

→ **Ley de seguros**

Ocurre lo mismo con la ley de seguros. La ley de seguros tiene como objetivo principal la supervisión de la industria de seguros con el fin de desarrollar y mantener mercados de seguros justos, seguros y estables para beneficio y protección de los asegurados. Al igual que con la ley de telecomunicaciones, en algunos países la legislación de seguros también contiene cláusulas de confidencialidad sobre los datos de los clientes; sin embargo, la ley de seguros no está completamente abocada a la preservación de la privacidad de los datos del cliente.

→ **Ley de protección de datos**

La normatividad que explícitamente incorpore la protección de datos y medidas de privacidad requiere la promulgación de una ley separada de protección de datos. Las disposiciones básicas sobre la recopilación, tratamiento y análisis de datos suelen ser reguladas por las leyes de protección de datos, que simultáneamente crean una autoridad encargada de la protección de datos con el objetivo de proteger los derechos fundamentales de los sujetos de datos. La estructura y el alcance de la legislación de protección de datos pueden variar considerablemente, por ejemplo, concentrándose únicamente en el sector privado o público, o para cubrir áreas específicas de un sector. En muchas jurisdicciones las leyes de protección de datos son elementos generales de legislación consagrados en la constitución del estado, pero no están específicamente diseñados como un subconjunto de la regulación de los seguros que trate específicamente con el ecosistema móvil.

→ **Ley de informes de crédito**

Algunas jurisdicciones también cuentan con una ley de informes de crédito. Las implicancias de una ley de informes de crédito en la protección de datos dependen del alcance de la ley en cada jurisdicción. Algunas leyes de informes de crédito designan ciertos grupos de instituciones para que informen a una agencia de informes de crédito; si una compañía de seguros forma parte de este grupo de instituciones designadas, entonces la firma de seguros informaría sobre sus asegurados y sus comportamientos de pago a la entidad de informes de crédito. Esta ley podría desempeñar un papel en términos de cómo se maneja y monitorea el intercambio de información en un país específico.

→ **Desafíos legales: estatus y cumplimiento de la norma por los nuevos actores**

Cada país tiene una legislación particular que podría plantear muchos desafíos en términos de protección y privacidad de datos. Las entidades no aseguradoras que participan en la cadena de valor del seguro están básicamente fuera de la jurisdicción tradicional de los supervisores de seguros (por ejemplo, los ORM son regulados por la autoridad de telecomunicaciones). Aun así, cuando estas entidades no aseguradoras se encuentran involucradas en el negocio de seguros, si no se supervisa debidamente sus acciones pueden presentar grandes riesgos de protección a los consumidores que forman parte de sus amplias bases de clientes. Más aún, suele ocurrir en muchas jurisdicciones que la legislación existente no tiene en cuenta los seguros móviles ni a los nuevos actores como los PST. Los PST generalmente participan en la cadena de valor del seguro apoyando diferentes actividades, pero asumen el liderazgo en la gestión de los datos de los consumidores; mientras que en algunas jurisdicciones los PST tienen que registrarse como agentes bajo la jurisdicción del supervisor de seguros, en otras escapan a la legislación vigente. Este vacío normativo se agrava si no se cuenta con ninguna ley de protección de datos que rijan el procesamiento de información personal. Es importante que los supervisores aclaren o adapten el marco legal que deben cumplir los PST, junto con otros intermediarios, para proteger a los consumidores de problemas derivados por el entorno de Big Data.

Es vital que el alcance de la supervisión esté en armonía con las buenas prácticas en supervisión de la protección de datos, y con cualquier nuevo requerimiento que tenga en cuenta los mandatos y reglamentos existentes. Es crítico que quede claro quién es responsable de proteger qué datos, a medida que terceros o intermediarios recolectan cada vez más datos que después usan las aseguradoras

u otros actores de los negocios relacionados con los seguros. Los supervisores de varias autoridades deben trabajar conjuntamente para preservar los derechos más fundamentales de los consumidores, especialmente en un entorno de Big Data caracterizado por la recolección generalizada e intrusiva de información personal. Se necesita una base legal para esta cooperación, idealmente codificada en un documento (por ejemplo, un Memorando de Entendimiento) que describa los procedimientos básicos para supervisar y regular a las diferentes entidades involucradas.

Legislación de Protección de Datos en los Seguros Móviles

Ley de Telecomunicaciones: cláusulas de confidencialidad para mantener la privacidad de los datos y asuntos comerciales del cliente

Ley de Seguros: cláusulas de confidencialidad para mantener la privacidad de los datos y asuntos comerciales del cliente

Ley de Protección de Datos: disposiciones para la protección de datos que tratan sobre la recolección, procesamiento, análisis y transferencia de datos personales, tareas para los controladores de datos y derechos de los sujetos de datos (individuos)

Ley de Informes de Créditos: disposiciones para la protección de datos así como también condiciones para la transferencia de datos del cliente de seguros a la agencia de informes de crédito

Estudios de caso: Sudáfrica y México

SUDÁFRICA

El seguro móvil no es un ámbito de supervisión regulado explícitamente en Sudáfrica. Más bien, las cuestiones transversales relativas a los seguros móviles y los desafíos de la protección de datos son supervisados más específicamente por una serie de órganos de supervisión y por el mandato general de la constitución sudafricana.

Estructuras y riesgos de asociaciones de ORM para seguros

Para entender los diferentes retos de regulación en el contexto sudafricano, es importante entender las estructuras de las asociaciones de ORM para los seguros y cómo operan dentro de la industria de seguros⁹.

- **Un asegurador registrado forma parte del grupo del ORM:** el ORM tiene su propia compañía de seguros creada como parte del grupo ORM y casi todo funciona internamente.
- **Acuerdo de celdas cautivas:** el ORM crea una entidad separada que se convierte en una célula dueña del riesgo asegurado adquiriendo una clase específica de acciones delimitadas dentro de una aseguradora registrada. A menudo se combina con un contrato vinculante o de subcontratación por el cual el ORM realiza varias funciones a nombre de la aseguradora (es decir, se encarga del negocio de seguros) y la aseguradora solo suscribe el riesgo.
- **Arreglos de marca:** la aseguradora registrada asume la responsabilidad total del seguro, aunque posiblemente existan acuerdos de intercambio de datos con el ORM a fin de obtener la base de clientes. El papel del ORM consiste en proporcionar datos sobre el cliente para que pueda agregar los productos que se va a distribuir a cambio de lo cual podría recibir una compensación gracias sus acuerdos de marca con la aseguradora (ya que la aseguradora apalanca el negocio que realiza el ORM con su propia marca).

Los principales riesgos identificados en el mercado de seguros móviles sudafricano son:

- **Las cuestiones sobre la protección de datos y privacidad de datos** surgen como consecuencia de la interconexión estructural entre entidades y las asimetrías de información resultantes, las cuales dan lugar al uso no autorizado de datos debido al libre flujo de información entre las distintas entidades. Por ejemplo, en los arreglos de celdas cautivas, a pesar de que el ORM actúa en nombre de la aseguradora, utiliza la información de su compañía matriz lo cual podría constituir una infracción a la ley de datos sudafricana.
- Se ha identificado numerosas **prácticas abusivas de marketing**, como la comercialización con opciones negativas¹⁰, la falta de identificación de la aseguradora y la falta de información fundamental sobre los términos del contrato.
- **Riesgos operacionales** específicamente relacionados con la tercerización de funciones y riesgos

⁹ Solo se menciona las tres estructuras más usuales. Sin embargo, la estructura de un ORM específico no se limita necesariamente a una de estas estructuras y podría consistir en una combinación de cualquiera de ellas.

¹⁰ Un ejemplo del marketing de opción negativa es una aseguradora que vende productos empaquetados, tales como seguro de sepelio gratuito por un período de tiempo dado para después deducir automáticamente primas sin que los clientes hayan solicitado retener la póliza.

de asociación. Incluye la falta de supervisión de la entidad que realiza el negocio de seguros en nombre de la aseguradora, lo cual da por resultado una protección inapropiada del consumidor durante todo el ciclo de vida del producto. Esto es particularmente prevaeciente en las estructuras de acuerdos de celdas cautivas y contratos vinculantes.

Marco regulatorio

El marco regulatorio que rige el seguro móvil y la protección de datos actualmente consiste en:

- **Constitución Sudafricana:** ley general que todo ciudadano de Sudáfrica debe cumplir. Todas las leyes sudafricanas deben estar de acuerdo con la Constitución. Una disposición en la Constitución establece que todo ciudadano tiene derecho a la privacidad. Aunque no es una legislación detallada, proporciona la base de otras leyes sobre la privacidad de los datos.
- La ley principal que rige la protección de datos en Sudáfrica es **Ley de Aplicación General** llamada **Ley de Protección de la Información Personal (LPIP)**. La LPIP crea un regulador de la información (que no es el supervisor de seguros) y le da amplios poderes para aplicar la Ley. La LPIP también se ocupa del procesamiento de datos y otorga ciertos derechos de privacidad a la conexión y análisis de datos de las personas en Sudáfrica. En consecuencia, es una ley general que se aplica a todas las aseguradoras, ya que actualmente no hay legislación de seguros que rijan específicamente la protección de datos¹¹.
- En las **Leyes de Aplicación General** también existe una **Ley de Protección al Consumidor**, que incluye disposiciones limitadas sobre privacidad. Sin embargo esta Ley de Protección al Consumidor no se aplica a funciones, actos, transacciones, bienes o servicios sujetos a las leyes sobre servicios financieros¹². Por consiguiente, la industria de servicios financieros cuenta con sus propias leyes de protección al consumidor que rigen su comportamiento.
- Existe también una **Ley de Comunicaciones y Transacciones Electrónicas que incluye algunas normas** sobre protección de datos.

En general, la principal ley que rige la protección de datos en Sudáfrica es la LPIP. El reto para el regulador de seguros es suscribir Memorandos de Entendimiento (MdE) apropiados con el regulador de información a fin de cooperar en el trato hacia las aseguradoras cuando incumplan con cualquier ley de protección de datos.

Acciones de mitigación de riesgo tomadas por la Junta de Servicios Financieros

Propuestas de enmiendas a la legislación

Actualmente, la Ley de Seguros a Largo Plazo y la Ley de Seguros a Corto Plazo, que rigen los seguros en Sudáfrica, no contienen requisitos específicos ni sobre protección de datos ni sobre seguros móviles. No obstante, la JSF está elaborando una legislación subordinada para abordar los problemas relacionados a la privacidad de los datos y la protección del consumidor. Si bien estas enmiendas no tienen un enfoque específico en el seguro móvil, por su propia naturaleza se aplican al análisis de Big Data y al seguro móvil. Una enmienda importante abarca varias cuestiones relacionadas con la gestión de datos, lo que supondrá introducir requisitos importantes para que las aseguradoras cuenten con

¹¹ Aunque se ha promulgado la LPIP, todas las secciones importantes sobre procesamiento y privacidad de datos aún no entran en vigencia. Hasta el momento, solo se encuentran vigentes las secciones de naturaleza administrativa (por ejemplo, la creación del regulador de la información). No queda claro en qué momento entrarán en vigencia las secciones sustantivas, aunque se prevé que ocurra en 2017

¹² Sección 28(2)(b) de la Ley de la Junta de Servicios Financieros.

un marco de gestión de datos para el análisis de Big Data. Esto abordaría las preocupaciones acerca de los acuerdos de tercerización haciendo responsable a la aseguradora y fijando requisitos estrictos sobre supervisión, diseño de productos y monitoreo. Se aplican requisitos similares a otros temas importantes como la divulgación, la publicidad y la comercialización con opciones. Estos requisitos son neutrales para todos los medios, lo cual significa que la legislación se aplica a cualquier plataforma, móvil o no. Todas estas políticas, si bien generales, tendrán un impacto significativo en el seguro móvil.

Si bien no ha tenido como resultado incorporar sólidas leyes sobre privacidad o protección de datos como parte de las normas de seguros, la JSF está elaborando enmiendas que indirectamente darán al regulador de seguros la capacidad de actuar cuando se produzcan violaciones en materia de protección de datos¹³. La JSF también tendrá que suscribir un MdE con el regulador de la información para fomentar la cooperación y toma de acciones cuando se considere necesario.

Enfoque de supervisión focalizada

Para complementar la legislación, la JSF está considerando adoptar un estilo de supervisión focalizada para regular las cuestiones de seguro móvil y protección de datos. Ello podría implicar concentrarse en los proveedores de seguros móviles y asegurar que cumplan con la legislación preexistente.

RÉGIMEN DE PROTECCIÓN DE DATOS DE MÉXICO

El régimen de protección de datos personales de México está compuesto por una constelación de normas constitucionales. La Constitución establece que toda la información concerniente a la vida privada y la información personal de los ciudadanos está protegida bajo los términos establecidos en la legislación y se la reconoce como derecho fundamental garantizado. Se garantiza su cumplimiento a través de un organismo federal autónomo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), encargado de proteger los datos personales de todos los ciudadanos mexicanos. La autoridad supervisora de seguros, la Comisión Mexicana de Seguros y Valores, no tiene el mandato de regular la protección de datos.

A continuación se presentan las principales leyes y disposiciones que regulan la protección de datos en México.

Ley General de Transparencia y Acceso a la Información Pública

- Crea el *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos de Personales (INAI)*, organismo independiente de supervisión del uso de datos personales
- El acceso a la información personal solo se permite a sus legítimos propietarios, representantes o funcionarios autorizados

¹³ Incluye una propuesta de modificación según la cual la aseguradora debe cumplir con todas las leyes relevantes sobre confidencialidad, privacidad, seguridad y retención de datos o información.

- Los titulares de datos personales deben proteger sus datos y sólo permitir el acceso a la información confidencial con el consentimiento de los propietarios legítimos de dicha información
- Establece una instancia de apelación ante el INAI

Ley Federal de Transparencia y Acceso a la Información Pública

- Define la estructura y rol del INAI
- Establece Comités de Transparencia dentro del gobierno federal a fin de respaldar el procesamiento transparente de datos

Ley Federal de Regulación de Particulares en Posesión de Datos Personales

- Los administrados incluyen individuos y entidades que obtienen, utilizan, difunden o almacenan datos personales
- Obliga a las entidades que tratan con datos personales a obtener dicha información sin engaño y utilizarla con el consentimiento explícito de sus propietarios. Estas entidades deben informar a sus propietarios que se está obteniendo información y los fines de la misma mediante una advertencia de privacidad
- Permite a las entidades en posesión de datos personales transferir estos a terceros sin el consentimiento del titular cuando dicha transferencia se realice a filiales u otras empresas bajo el control de la entidad responsable
- Establece que los titulares de datos personales gozan de derechos de acceso, corrección, cancelación y oposición

Ley de Regulación de Grupos Financieros

- La empresa en posesión de datos personales y cualquier otra entidad financiera que pertenezca a un grupo financiero podrá compartir información relacionada a los servicios prestados por cada entidad con sus clientes, sin que esto constituya una infracción de la confidencialidad, siempre y cuando la naturaleza del documento compartido implique la obligación de confidencialidad

Ley de Protección y Defensa de Usuarios de Servicios Financieros

- La Comisión Nacional de Protección y Defensa de los Usuarios de Servicios Financieros creará y actualizará un Registro de Usuarios que no deseen que su información sea utilizada para fines de marketing y publicidad
- Se prohíbe a las instituciones financieras usar la información contenida en las bases de datos de sus clientes con fines de marketing o publicidad y para enviar anuncios a aquellos clientes que han declarado explícitamente que no desean recibir dicha publicidad o que se han inscrito en el Registro de Usuarios.

Ley de Instituciones de Seguros y Valores

- Las instituciones de seguros pueden compartir información para fortalecer las medidas de prevención e identificación de las operaciones que involucran asociación con fines delictivos siempre y cuando no se infrinja las obligaciones de confidencialidad de la información.

Preguntas y debate

¿El consumidor promedio de bajos ingresos no suele ser consciente de que tiene derechos que puede defender. ¿Existen medidas para sensibilizar a las personas acerca de qué derechos de los consumidores pueden ser violados con respecto a cuestiones de protección de datos?

Esto depende mucho del país. En algunos países, bajo la ley de protección de datos, y no de la ley sobre seguros, las empresas que recogen y procesan datos personales tienen que informar a los consumidores de sus actividades; los consumidores tienen derechos específicos para comprobar la exactitud de los datos recogidos y para que cualquier discrepancia sea rectificada. No obstante, esto no está prescrito universalmente así que los clientes a menudo no son conscientes de sus derechos. Los consumidores se enteran generalmente de los abusos a través de los medios de comunicación.

¿Qué pueden hacer los supervisores si no existe una ley general de protección de datos en el marco regulatorio? ¿Qué es lo que se puede hacer con una ley de seguros?

Esto depende mucho del alcance de la ley de seguros que exista y de la capacidad del supervisor para aplicar las medidas de protección del consumidor que aparezcan en las disposiciones conexas. Si existe la posibilidad, es importante que los supervisores exijan al asegurador ser responsable por los datos y la privacidad. Las normas básicas de protección de datos que se podrían aplicar mejorarían el conocimiento del cliente acerca de la recopilación, el tratamiento y el uso de los datos.

¿Es la falta de reclamos sobre el tema de la protección de datos realmente un indicador de la ausencia de abusos? ¿O los abusos a menudo quedan ocultos al consumidor que no sabe dónde puede haber vacíos, por ejemplo en la protección de su privacidad?

La cuestión de la falta de reclamos se asocia con la falta de transparencia del entorno de Big Data. La imposibilidad de comparar y la heterogeneidad de los servicios electrónicos ponen a los clientes en una posición en la que les es difícil detectar cualquier tipo de discriminación. Desde el punto de vista regulatorio, la falta de quejas no es un indicador ideal. Sin embargo, en algunas jurisdicciones, para los reguladores de seguros esto puede que no sea un enfoque primordial ya que puede existir una legislación general sobre protección de datos que da a otra autoridad la responsabilidad de proteger al consumidor. Los supervisores de seguros deben cooperar con otros reguladores para abordar de manera proactiva estas cuestiones, ya sea a través de un enfoque de supervisión específicamente dirigido al seguro móvil o mediante una aplicación más general.

¿Qué efectos competitivos deberían tener en cuenta los supervisores para el futuro?

La configuración del modelo de negocio de seguros móviles tiende a producir efectos competitivos verticales complicados. Por ejemplo, los ORM suelen verse estratégicamente impulsados a comprometerse con las aseguradoras y PST con el fin de proporcionar seguros para aumentar la fidelidad de sus clientes, reducir la rotación, crear conciencia de marca y/o aumentar el ingreso promedio por cliente. A su vez, los PST están incentivados a participar en negocios de seguros, debido a que reciben una retribución por los acuerdos en que actúan como intermediarios. Estos incentivos pueden crear desequilibrios de poder en el mercado y dar lugar a estrategias para aprovechar la oportunidad de un negocio lucrativo para las partes involucradas, en lugar de asegurar que los productos y precios sean apropiados para el consumidor final. Los supervisores deben ser cuidadosos con los incentivos perversos de mercado y deben ver si los servicios están agrupados y si los consumidores tienen la alternativa de tomar un seguro del PST o de una aseguradora en particular. Si los consumidores no tienen alternativa, pueden ser captados sin quererlo por la compañía de seguros que domina el mercado.

¿De qué manera los supervisores de seguros pueden regular a los intermediarios de seguros móviles para asegurarse de que sean canales responsables de distribución de seguros?

Existe una gran variedad de enfoques y requisitos que adoptan los supervisores para regular a los intermediarios de seguros móviles. En algunos países, los PST están registrados como corredores o agentes de suscripción de seguros. Sin embargo, en otros, el ORM se considera como el canal de distribución y, por lo tanto, se debe registrar como agente, poniéndolo efectivamente bajo el ámbito de supervisión. Por último, cómo se debe registrar el intermediario y qué regulación debe cumplir depende en gran medida de las funciones específicas que lleve a cabo. También se debe definir la tercerización, además de las funciones de valor. Por ejemplo, si un asegurador terceriza una función a otra entidad, la aseguradora debe aceptar cualquier responsabilidad que tenga el organismo que emite el seguro en su nombre.

¿Cómo se distribuyen las responsabilidades de propiedad de los datos entre el ORM, la aseguradora y el PST y cómo se pueden establecer estas responsabilidades, por ejemplo, mediante la reglamentación, un Memorando de Entendimiento o mediante otras medidas?

Generalmente, un ORM, una compañía de seguros y un PST determinarían estas responsabilidades en sus propios contratos mutuos. Dependiendo del régimen regulatorio, y suponiendo que existe una ley general de protección de datos, cada una de las instituciones que recolectan información es responsable de esa información. Cuando una entidad recopila datos, cae bajo la ley de protección de datos y, por lo tanto, debe cumplir con las normas establecidas en la legislación. Dicho esto, si una compañía de seguros terceriza una función crítica como la suscripción o la administración, entonces la compañía de seguros suele ser responsable por la entidad con la que ha tercerizado esta función, incluyendo todos los problemas de procesamiento de información derivados.

¿Es el uso del crédito en el servicio móvil (tiempo de llamada) para pagar primas considerado como una forma de transferencia de dinero electrónico (e-money)? ¿Ha habido ejemplos de conflictos con la legislación sobre transferencia de dinero electrónico?

Esta es una pregunta difícil que depende del contexto del país. Mientras que algunos países emergentes y en desarrollo tienen leyes o reglamentos sobre dinero electrónico, en otros, el tiempo de llamada no se considera un sistema de pago electrónico o la situación no está definida. Por ejemplo, en Sudáfrica, las transferencias de dinero electrónico no han sido incluidas en el marco regulatorio porque no se ha planteado como un problema prevaleciente en el mercado. La cuestión de si el tiempo de llamada puede considerarse una forma de dinero es todavía un tema que muchos bancos centrales siguen discutiendo.

¿Existen problemas de confidencialidad en el modelo “freemium” en el que pueden usarse los datos del cliente sin su consentimiento?

Esto depende de la manera en que está implementado el modelo. Si los clientes no están específicamente de acuerdo en compartir sus datos entonces existiría un problema de protección de datos. Debe existir una manera simple, transparente y fácil de entender para que los clientes estén informados sobre lo que sucede con sus datos y cómo se usan. Las maneras de dar consentimiento (o denegarlo) deben ser simples y si alguien no está de acuerdo en compartir sus datos, entonces debe respetarse su decisión. Además de los modelos, también es importante el marco regulatorio. En algunos países existe un enfoque de “exclusión voluntaria”, es decir, los datos y toda la información pueden compartirse a menos que el consumidor declare explícitamente que los datos no pueden ser utilizados. Esto podría plantear problemas para los clientes. Por el contrario, si la regulación requiere que los datos no pueden ser compartidos a menos que el consumidor consienta explícitamente compartir/usar los datos, el consumidor estará mejor protegido.



La Iniciativa de Acceso a Seguros
 Patrocinado por Proyecto de GIZ para el Sector
 Enfoques de los Sistemas Financieros al Seguro

Deutsche Gesellschaft für Internationale
 Zusammenarbeit (GIZ) GmbH
 Dag-Hammarskjöld-Weg 1-5
 65760 Eschborn, Alemania

Teléfono: +49 61 96 79-1362
 Fax: +49 61 96 79-80 1362
 Correo electrónico: secretariat@a2ii.org
 Internet: www.a2ii.org

La Iniciativa es posible gracias al esfuerzo conjunto de las siguientes instituciones.



Patrocinado por:

