Diez reglas para emitir **pólizas electrónicas en Colombia**

Héctor José García Santiago, director del Centro de Estudios en Derecho y Tecnologías de las Información y las Comunicaciones (CEDT) de la Pontificia Universidad Javeriana, actualmente presidente de la Sociedad Cameral de Certificación Digital, Certicámara S.A.

Las pólizas electrónicas deben cumplir estándares en seguridad técnica y jurídica para ser consideradas como tal. La autenticidad e integridad de la póliza son los atributos de seguridad que deben garantizarse en entornos electrónicos.

El SOAT electrónico:

A propósito del «SOAT electrónico», una cosa es el reporte en línea y tiempo real de los datos de la póliza SOAT al RUNT por parte de las aseguradoras, lo cual fue regulado por el Ministerio de Transporte mediante la Resolución 5886 de 2015, y otra muy distinta es expedir pólizas electrónicas.

Para el caso puntual de este seguro, debe precisarse que sin que se haga un reporte en línea de los datos de la póliza SOAT al RUNT, la validación de la información por parte de las autoridades competentes se torna imprecisa e inexacta, desvirtuando las bondades que permiten las tecnologías de la información y las comunicaciones.

Sin perjuicio de la suerte que corra la Resolución 5886, es posible que hoy en día se expidan pólizas electrónicas, siempre y cuando se garanticen unas condiciones mínimas.

A continuación se plantean diez reglas a tener en cuenta para expedir pólizas electrónicas:

1. Teniendo en cuenta que el contrato se celebra por medios electrónicos, y bajo el entendido de que nos encontramos frente a contratos de adhesión (Ley 1480 de 2011, artículo 37), es preciso que la información, condiciones y el contenido del contrato de seguro sean informados de forma previa, clara y expresa al adherente (tomador del seguro), lo que precisa habilitar un sistema de aceptación de estas condiciones de manera inequívoca y expresa. Este sistema debe garantizar la integridad de la información y el consentimiento

Héctor José García Santiago
Presidente de Certicámara S.A.

irrefutable en señal de aceptación por parte del tomador.

2. Debe verificarse de manera inequívoca la identidad del tomador del seguro, a fin de tener certeza sobre si su actuación es a nombre propio o de un tercero, bajo el entendido de que el seguro puede ser contratado por cuenta de un tercero determinado o determinable (artículo 1039 del Código de Comercio) y con el objetivo de que la declaración de asegurabilidad sea fiable, esto es, que se tenga certeza sobre la persona y su condición frente a los hechos y circunstancias que determinan el estado del riesgo a través de un cuestionario previamente definido. Esta validación de la identidad del tomador del seguro debe hacerse a través de mecanismos técnicos robustos como la validación de identidad consultando la base de datos biográfica y biométrica de la Registraduría Nacional del Estado Civil, Resolución 5633 de 2016, y mediante el uso de mecanismos de firma digital o firma electrónica certificada como la huella, la voz, el iris o el rostro. (Artículo 30 de la Ley 527 de 1999 modificado por el artículo 161, numeral 1), del Decreto 019 de 2012).

3. Debe asegurarse la integridad del contenido de la póliza (artículo 1047, Código de Comercio), esto es, garantizar que los datos de la póliza sean inmodificables a través del uso de funciones hash y técnicas de cifrado que permitan determinar el momento exacto de expedición de la póliza.

"Es posible que hoy en día se expidan pólizas electrónicas, siempre y cuando se garanticen unas condiciones mínima".

4. Debe habilitarse un sistema para firmar electrónicamente las pólizas de seguro por las partes; tanto el asegurador como el tomador deben firmar la póliza. La firma manuscrita se presume auténtica (artículo 1052 del Código de Comercio), la firma electrónica que goza de esa autenticidad es la firma digital (artículo 28, Ley 527 de 1999) y la firma electrónica certificada (artículo 161, Decreto Ley 019 de 2012). Lo recomendable es que el asegurador haga uso de una firma digital y el tomador de una firma electrónica certificada.

5. Se deben preservar los elementos esenciales del contrato de seguro, (artículo 1045 del Código de Comercio), lo que se traduce en que el interés asegurable, el riesgo asegurable, el valor de la prima y la obligación condicional del asegurador deben permanecer inalterables, lo cual implica garantizar la integridad del documento a través de técnicas de cifrado certificado. (Artículo 9, Ley 527 de 1999).

6. Se debe realizar el envío del documento original al tomador con fines exclusivamente probatorios, dentro de los quince días siguientes a la celebración del contrato, para lo cual debe tenerse en cuenta que los documentos que se transmitan deben garantizar su autenticidad, integridad y no repudio, tanto en su firma como en su contenido. En este punto cobra especial relevancia el principio de equivalencia funcional de original (artículo 8, Ley 527 de 1999) en virtud del cual es posible la presentación de un original en formato digital.

   Así mismo, se debe garantizar la transmisión segura de la información. Para certificar el envío seguro se recomienda el uso de protocolos de seguridad como el Secure Socket Layer (SSL), así como el empleo de un correo elec-

trónico certificado que dé certeza del envío y recepción del mensaje de datos.

7. Se requiere habilitar un mecanismo que permita validar la identidad de la persona para notificar al asegurador los hechos o circunstancias no previsibles que sobrevengan con posterioridad a la celebración del contrato, donde se pueda determinar con exactitud la fecha y hora en la cual se realizó dicha notificación (artículo 1060 del Código de Comercio). Del mismo modo, este mecanismo debe servir para dar aviso del siniestro, para lo cual es imperioso el uso de sellos de tiempo para verificar la fecha exacta de estas manifestaciones.

8. Deberá habilitarse un mecanismo de pago que permita confirmar dicha obligación en el domicilio electrónico de la aseguradora y acreditar el pago al tomador del seguro. Existen múltiples opciones en el mercado para pagos electrónicos, incluyendo monederos a través de sistemas de micropagos multipropósito, sistemas de pagos electrónicos, (EPS), incluso y terminales en puntos de venta (TPV) que hacen uso de la red bancaria a través de medios de pago tradicionales como las tarjetas débito o crédito.

9. Se debe habilitar un sistema de cesión de pólizas donde el riesgo a mitigar es la suplantación de identidad. Se requiere un sistema robusto de validación de identidad, que permita identificar a las partes, cedente y cesionario, de manera inequívoca y remota. La biometría certificada es la tendencia mundial de más alta seguridad para validar remotamente la identidad de las personas. (Decreto 2364 de 2012 y artículo 161, numeral 1), Decreto 019 de 2012).

10. Se debe contar con un mecanismo de almacenamiento seguro de la póliza y sus anexos que permita su consulta en cualquier momento, con la garantía de preservación de la integridad del contrato de seguro y de sus anexos de estos documentos. (artículo 161, numeral 8), Decreto 019 de 2012).

> "Uno de los pilares fundamentales es la validación de la identidad del tomador del seguro y la firma de la póliza. Colombia es pionera en la región".

Las Aseguradoras que quieran expedir pólizas electrónicas deben garantizar un ambiente que permita preservar los atributos de seguridad jurídica propia de los documentos electrónicos, tales como la autenticidad, integridad, no repudio, conservación y consulta, a través del uso de mecanismos y estándares internacionales como los señalados por la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional (CNUDMI) (Leyes Marco de Comercio Electrónico y Firmas Electrónicas) adoptados por el Gobierno de Colombia mediante la Ley 527 de 1999, en los que uno de los pilares fundamentales es la validación de la identidad del tomador del seguro y la firma de la póliza. Colombia es pionera en la región, en la implementación de procesos de validación de identidad mediante el acceso a la base de datos biométrica y biográfica de la Registraduría Nacional del Estado Civil y a través de procesos de firma de documentos con patrones biométricos como la voz, la huella, el rostro o el iris.