# Boletín del Grupo Internacional de Trabajo "Nuevas Tecnologías, Prevención y Seguro"

Nº 1-2007

*Este Boletín responde a la necesidad, detectada por los miembros del Grupo de Trabajo, de recoger, describir, analizar y relacionar con el objeto del mismo aquellos aspectos de las Nuevas Tecnologías (NT) que inciden, de manera directa o indirecta, en las pólizas de seguros, en lo que afecta a la delimitación de los riesgos, a sus exclusiones o a las medidas preventivas para evitar o aminorar el siniestro.*

*El Boletín NTPS es un foro abierto a los miembros del Grupo, a todos los asociados de AIDA y a cualquier otra persona interesada, por lo que cualquier tipo de comunicaciones es bienvenido.*

*Las personas que nos envíen aportaciones pueden hacerlo también en inglés, alemán, francés, italiano o portugués.*

**Abstract:**

A questionnaire, prepared by the Group, was submitted last year to national sections in order to collect information regarding certification services providers, as one of the main research area of the Group (NTPI). The results of the consultation may be summarized as follows. The level of response ranges from a few countries providing wide information and useful additional documentation; to other countries that, albeit the lack of completion of the questionnaire, has drafted an informative note outlining the domestic situation. The study of the replies and the reasons alleged to explain the lack of response or its difficulties reveals several appealing conclusions. The level of domestic development may be classified in two categories: emerging and intermediate. The referred development affects to a set of elements: the market of certification services, the society of information services, the legislative recognition, the commercialization of insurance policies regarding certification services. Whereas some countries assert that the limited development of the information society services explains a narrow offer by the insurance companies and a poor demand of insurance policies related to certification services; other countries, namely European countries, has reached a reasonable level of technological evolution that justifies a regulation in detail and a stronger market. In particular, the case of Spain deserves to be mentioned, where the digital sign has been incorporated to the official identity documents (eDNI).



Redactores: Joaquín Alarcón, Sandra Camacho y Teresa Rodríguez de las Heras.

Email: seaida @seaida.com

To sum up, the replies show that the disparity in the development is significant and concerns four legislative areas and practical matters: regulation on electronic commerce; regulation on electronic signature; specific rules on services providers' liability and, in particular, certification services providers; rules or practices regarding the insuring of this activity.
Apart from the matters just mentioned, the Group is interested in considering the following topics: the evidential value of the electronic document; the use of computer at work for private purposes and its effects on insurance; the biomedical progress and its impact on insurance law.

## 1. Informe del Grupo sobre los prestadores de servicios de certificación

El año pasado se sometió a las diversas secciones nacionales un cuestionario sobre el tema referenciado, objeto de investigación del Grupo. Como resumen podemos indicar lo siguiente:

1.1. Varios países han contestado al cuestionario remitido y otros nos han suministrado valiosísima documentación que comprende textos de pólizas, cuestionarios, legislación y útiles informaciones adicionales (Sudáfrica, España, Suiza y Chile) que nos permiten clarificar el escenario; determinados países a los que nos hemos dirigido no han contestado ni enviado póliza; sin embargo, nos han remitido una nota informativa de la situación en su país que permite hacerse una idea aceptable de la situación en los países respectivos.

1.2. Niveles de desarrollo

1.2.1. Nivel de desarrollo preliminar**.** La falta de desarrollo del sector y consecuentemente de los servicios relacionados es el factor predominante que incide en la falta de respuesta concreta al cuestionario en determinados países. Ciertamente puede afirmarse que en muchos países la prestación de servicios de certificación de firma electrónica y, por tanto, el aseguramiento de esta actividad, se encuentra en un estado todavía embrionario. Más aún, no son pocos los países en los que este estado preliminar de desarrollo puede extenderse en general al sector de las tecnologías de la información y la comunicación. En consecuencia, es razonable encontrar que en estos países la demanda de pólizas relacionadas con servicios y actividades tecnológicas sea notablemente baja y la respuesta de las aseguradoras ante tales riesgos extraordinariamente limitada e incluso inexistente. El diagnóstico que de las respuestas de nuestros corresponsales puede extraerse para explicar este limitado o, en ocasiones, emergente desarrollo de la Sociedad de la Información se basa en los siguientes parámetros:

- la ausencia de norma legislativa que acepte, autorice o regule la prestación de servicios a través de medios informáticos, esto es, la prestación de servicios de la sociedad de la información (Paraguay, Serbia)

- la inexistencia de pólizas comercializadas relativas a la prestación de servicios de la sociedad de la información y, en particular, de servicios de certificación de firma electrónica (Paraguay, Serbia). Este contexto de baja o nula comercialización de pólizas, viene lógicamente marcado, como pone de manifiesto nuestro corresponsal de Serbia, de un lado, por una falta de demanda de seguro relativo, en especial, a servicios de carácter tecnológico y, de otro, por una lenta y escasa respuesta de las aseguradoras locales para atender esta demanda cuando la misma se produce.

Conviene hacer notar, en este punto, la expresa solicitud recibida de estos países para recibir nuestra ayuda con objeto de fomentar el sector y completar la normativa legal, contribuyendo de esta manera al desarrollo del derecho de seguros en los mismos.

1.2.2. Nivel de desarrollo intermedio. En países que podríamos considerar algo más avanzados, como pueden ser los pertenecientes a un determinado entorno europeo, la regulación legal existente sobre la prestación de servicios de la sociedad de la información está en una etapa de desarrollo intermedia, sometida a continuos cambios motivados por la necesaria consolidación de las reglas adoptadas y también por la evolución tecnológica. En este contexto normativo y negocial el uso de la firma electrónica, en sus diversas modalidades, se está extendiendo para transacciones públicas y privadas. De hecho, en aquellos países que cuentan con una legislación más o menos completa y depurada de la sociedad de la información, la legislación sobre firma electrónica representa una de las piezas básicas de esta disciplina. Más aún, en algunos países, como el caso de España, se ha procedido incluso a la incorporación de soluciones de firma electrónica en los documentos de identidad oficiales.

El proyecto eDNI (Documento Nacional de Identidad electrónico) se encuentra en proceso de implantación en España. En la actualidad, las oficinas de expedición se localizan en 36 ciudades de 22 provincias españolas, se han expedido hasta el momento 240.000 DNI electrónicos con el objetivo de que se implante progresivamente en el resto de las provincias para que a finales de 2007 se expida en toda España. El DNI electrónico trata de ofrecer un instrumento eficaz para acreditar la personalidad de los usuarios en las transacciones electrónicas e incorporar una firma electrónica mediante un dispositivo seguro de creación de firma que le otorga idénticos efectos que la firma manuscrita. Ello permite hacer una serie de transacciones públicas (es aceptado por todas la Administraciones públicas y Entidades de Derecho público vinculadas o dependientes de las mismas) y privadas en un entorno de confianza y seguridad.

**1.3.- La operativa básica del servicio: obligaciones legales y tecnología empleada.**

1.3.1. Obligaciones legales del prestador de servicios de certificación de firma. Con respecto a los prestadores de servicios de certificación de firma electrónica, los mismos están sometidos a una **serie de obligaciones** consistentes, a título de ejemplo, en comprobar la identidad del solicitante, oferta de un amplio servicio de información (relativo a las condiciones, consecuencias del mal uso de la firma, medidas referentes a la confidencialidad y protección de los datos personales), comprobación de la exactitud de los datos relativos a la constitución de la personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante, mantenimiento de directorios actualizados, empleo de personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos, procedimientos de seguridad, publicación de sus prácticas de certificación, etc.

1.3.2. Tecnología empleada. Las soluciones de firma disponibles en el mercado y reconocidas por la legislación van desde las más simples contraseñas o nombres de usuario (firma simple), hasta sofisticadas técnicas biométricas de reconocimiento del iris, de la huella digital o de voz. Es preciso asumir esta variedad de técnicas como natural pues su elección en cada caso ha de responder a un adecuado balance entre la fiabilidad de la firma y el riesgo de la operación. Por ello, legislaciones como la española no desconocen efectos jurídicos a las firmas más simples, pero optan por dotar de los mismos efectos que la firma manuscrita a una determinada


Redactores: Joaquín Alarcón, Sandra Camacho y Teresa Rodríguez de las Heras.

modalidad de firma basada en la técnica de criptografía asimétrica. Se construye así el concepto de "equivalente funcional", de modo que la firma digital basada en tal tecnología es el equivalente funcional de la tradicional firma de puño y letra.
La certificación de la firma electrónica, se hace, en Europa y en parte en Asia, principalmente mediante un sistema mencionado, denominado "PKI" (*Public Key infrastructure*), criptografía asimétrica o de clave pública. La firma electrónica se basa en el empleo de dos claves, una clave privada de creación de firma bajo el control del titular y una clave pública de verificación de firma a disposición del destinatario. Estas claves son algoritmos matemáticos relacionados entre sí pero irreversibles, de modo que desde la clave pública no pueda obtenerse la privada.
El usuario dispone de una llave o clave criptográfica, es decir, de datos electrónicos únicos; es una llave privada que permanece secreta y permite firmar los documentos electrónicos; la llave pública permite al receptor de los mismos comprobar la firma electrónica del que envía el documento; si la comprobación es positiva ello indica: la identidad del firmante, el no repudio y la no alteración del mensaje firmado. La llave pública es la que se contiene en o viene acompañado de un certificado electrónico emitido por el prestador de servicios de certificación y cuya función principal consiste el asociar un par de llaves o, en concreto, la clave pública con una persona concreta, física o jurídica (certificado de identidad), o con determinados atributos del firmante (certificado de atributos) con lo que el receptor del documento conoce la identidad del que lo envía.

El sector asegurador no está muy animado a otorgar cobertura para estos supuestos. Los riesgos ciertamente pueden resultar imprevisibles y difíciles de determinar previamente, lo que complicaría su asegurabilidad. Téngase en cuenta que, en relación con las diversas obligaciones asumidas, el prestador de servicios de certificación se enfrenta a varios escenarios de riesgo: en la fase de identificación del solicitante (etapa que actualmente se realiza de forma presencial pero que pronto podrá ejecutarse a distancia gracias a la implantación de documentos electrónicos de identidad y acceso remoto a los registros públicos); en el proceso de uso de la firma al deber garantizar la seguridad y fiabilidad del sistema; en el proceso de verificación de la firma al deber actuar diligentemente para publicar los certificados suspendidos, caducados o cancelados. Más aún, en la medida que las soluciones de firma se emplean vinculadas a las más diversas transacciones, la previsión de los daños es prácticamente imposible.

Por otro lado, muchas empresas se debaten, en estos momentos, ante la cuestión de qué sea mejor si crear un propio sistema de PKI o bien adquirirla en el sistema de prestación de servicios.

### 1.4. Riesgos y cobertura

En la actualidad empresas de *software* de seguridad y *Solutions* en el ámbito de la seguridad apenas si pueden obtener cobertura de responsabilidad civil, pues un fallo de dichos productos es lo que causaría el daño objeto de indemnización.

Esta falta de cobertura actúa en cascada en las pólizas de los prestadores, que suelen excluir todo lo relacionado con virus o con fallos de seguridad en general, con lo que las coberturas se devalúan considerablemente. Las exclusiones se formulan de manera diferente, por lo general se excluyen *Security Breach* y *Theft of Data* (en América) o se dan incluso exclusiones específicas respecto a las PKI (pólizas de AIG).

A veces se cubren dichos supuestos mediante sublímites. Interesante es también destacar que en determinados países (Suiza, Alemania o Francia) aquellos programas de seguro que incluyen daños patrimoniales primarios incluyen, aun sin quererlo, dichas


Redactores: Joaquín Alarcón, Sandra Camacho y Teresa Rodríguez de las Heras.

coberturas; ello se debe, al parecer, a que los suscriptores locales no analizan las actividades ni sus correspondientes exposiciones por falta de conocimientos.

Respecto a la siniestralidad, la verdad es que se conocen pocos casos de violaciones o quiebras (*Security Breaches*), aunque son cada vez más frecuentes y aparecen ilustrados en la prensa, con indicación del recurso a la vía judicial. En la práctica interna de las aseguradoras y reaseguradoras apenas se conocen casos de grandes siniestros asegurados y pagados.

1.5. Estado de la cuestión: análisis comparado

Un análisis comparado de la cuestión, con base en las respuestas al cuestionario recibidas, nos permite identificar cuatro niveles legislativos y prácticos pertinentes: regulación del comercio electrónico o de los servicios de la sociedad de la información, en general; regulación de la firma electrónica; legislación específica sobre la responsabilidad de los prestadores de servicios y, en particular, sobre los prestadores de servicios de certificación de firma electrónica; reglas o prácticas sobre el aseguramiento de la actividad.

1.5.1. Regulación sobre comercio electrónico

Respecto a los cuestionarios, de cuyas respuestas disponemos ya, cuatro países (Grecia, España, Sudáfrica y Hungría) tienen legislación reguladora del comercio electrónico y de la prestación de servicios de la sociedad de la información y especialmente de la firma electrónica, en sus diversas modalidades.

Los países europeos adaptan su legislación a las correspondientes Directivas de la UE en materia precisamente de comercio electrónico y servicios de la sociedad de la infromación (Directiva 2000/31/CE) y firma electrónica (Directiva 1999/93/CE).

1.5.2. Regulación sobre firma electrónica

Como mencionábamos anteriormente, de los países que han enviado sus respuestas, cuatro (Grecia, España, Sudáfrica y Hungría) disponen también de legislación reguladora de la firma electrónica. Igualmente, por efecto de las Directivas comunitarias, los Estados miembros de la Unión Europea han debido transponer a sus ordenamientos la regulación comunitaria sobre firma electrónica (básicamente la Directiva 1999/93/CE).

En Uruguay existe un Proyecto de Ley del año 2000 y otro más actual en estudio de las comisiones parlamentarias, a fin de regular la firma electrónica y, más específicamente, la digital.

1.5.3. Regulación específica de la responsabilidad de los prestadores de servicios

En algunos países existe una regulación específica de la responsabilidad de los prestadores de servicios y, en concreto, de los prestadores de certificación, en otros no. Con respecto a su responsabilidad, por influencia de la Directiva comunitaria (Directiva 2000/31/CE), se mantiene en los ordenamientos europeos una regulación específica para los prestadores de servicios de intermediación (proveedores de acceso, prestadores de servicios de alojamiento de datos, prestadores de servicios de copia temporal, y en algunos casos como el español, buscadores y enlaces). En la normativa general de comercio electrónico no suele, sin embargo, incluirse una referencia a los prestadores de servicios de certificación de firma electrónica, si bien no dejan de ser un tipo de prestador de servicios de la sociedad de la información. Los supuestos de responsabilidad se detallan en su legislación específica (aunque nos referimos en particular al caso español, esta dualidad normativa se produce ya en sede comunitaria).
La responsabilidad por hechos propios está basada en la culpa, bien, como

decíamos, por regulación específica, bien por regulación general. La responsabilidad por hechos o contenidos ajenos tiene, en algún país, previsiones legales específicas y en otros no. La tendencia del Derecho comparado se dirige precisamente a proponer un principio de no responsabilidad por los contenidos y hechos ajenos que libere a los prestadores del elevado riesgo de su actividad (así artículos 14 a 17 de la ley española 34/2002 sobre comercio electrónico, artículos 12 a 15 de la Directiva 2000/31/CE y también Section 512 de la estadounidense *Digital Millenium Copyright Act*).

1.5.4**.** Seguro de responsabilidad civil

Donde las respuestas al cuestionario son más moderadas es en el apartado dedicado al seguro de responsabilidad civil. Respecto al seguro la gama varía desde la obligación para los prestadores de servicios de certificación de contratar una póliza de responsabilidad civil (España, Hungría), incluso con indicación de sumas (3.000.000 de euros en España), a la ausencia de previsión legal al respecto. Ello se debe a la ausencia de obligatoriedad del mismo, a la escasez de mercado o también a falta de dominio del escenario respecto al tratamiento que se debe dar a los deberes del asegurado.

Los aspectos relacionados con la prevención del riesgo o aminoración del siniestro están tratados en las pólizas de manera marginal, o no están tratados, o se tratan como un deber de comunicar los cambios materiales bien mediante la imposición de una gerencia o control del riesgo, sin distinguir exactamente entre los deberes del asegurado precontractuales, contractuales o después del siniestro, faltando precisión o bien no existiendo regulación de las consecuencias jurídicas en caso de infracción de dichos deberes.

De lo expuesto podemos ver que el Grupo de Trabajo tiene un amplio campo de actuaciones ante sí, relacionadas con la regulación de la responsabilidad y, especialmente, con la estructuración de unas coberturas adecuadas al riesgo.

1.6. Actuaciones previstas

A. Cuestionario y trabajos relacionados

1.6.1. Contestar/completar el cuestionario
1.6.2. Completar el archivo de pólizas
1.6.3. Resumen de los aspectos específicos de la responsabilidad (carencias, diferencias, coincidencias)
1.6.4. Resumen de la existencia de una obligatoriedad de asegurarse

B. Modelo de póliza

1.6.5 Elaboración de un borrador de póliza modelo que atienda, en particular, las siguientes cuestiones:

. Incluido- Excluido (delimitación cualitativa)
. Delimitación cuantitativa, temporal y geográfica
. Delimitación del concepto de daño (material o no)
.Medidas de prevención/aminoración y consecuencias jurídicas en caso de no observancia

C. Material de apoyo

1.6.6 Obtener y recopilar material de apoyo a la investigación

- Recopilación de daños frecuentes y sus causas (ej. cibervandalismo por virus que infectan el ordenador por hechos internos o externos) y su tratamiento en las pólizas

- Catálogo de medidas de prevención/aminoración para evitar o minimizar los incidentes (por ejemplo, equipo técnico de apoyo, apoyo de la Dirección, protecciones físicas contra el cibervandalismo, su actualización, directrices

escritas frente al mal uso de los empleados, política de claves de acceso de los empleados, sistemas de protección de la información personal de clientes, controles pre-contratación, su formación inicial y continua, existencia de un generador *backup*, sistema general de respuestas a los incidentes etc.) y su tratamiento en las pólizas.

D. Divulgación del informe

Divulgación del informe en las Secciones Nacionales de AIDA, asociaciones de seguros de los mercados y Autoridades

## 2. Próximos números del Boletín NTPS

Junto a los temas indicados más arriba, en los próximos números del Boletín los miembros del Grupo tienen varios temas para someter a análisis, entre los cuales podemos citar los siguientes:

- la realidad legislativa de la validez de un documento de soporte electrónico en juicio. La seguridad de las pruebas. La autenticidad del documento (el saber de dónde sale, cómo se ha obtenido y su veracidad). La valoración pericial y judicial.

- la utilización del ordenador de la empresa para fines privados (envío de correos, acceso a Internet en general, instalación de programas): repercusiones prácticas en el seguro de RC privada y en la póliza de RC Empresas (casos concretos).

- la investigación biomédica en el tratamiento y prevención de enfermedades: las técnicas de transferencia nuclear, prohibición o no de la creación de embriones destinados a la investigación, la realización de cribados genéticos para detectar enfermedades o el riesgo grave de padecerlas con el fin de realizar un tratamiento precoz de su desarrollo o prevenirlas, derecho del individuo a ser o no ser informado. Incidencia en los seguros de Vida, Salud o Accidentes en cuanto a selección de riesgo y gestión del siniestro ocasionado por padecer una enfermedad genética determinada.



Redactores: Joaquín Alarcón, Sandra Camacho y Teresa Rodríguez de las Heras.

Email: seaida @seaida.com