ORGANIZACIÓN MUNDIAL DEL COMERCIO

JOB/GC/115, JOB/CTG/3
JOB/SERV/247, JOB/IP/20
JOB/DEV/41

21 de diciembre de 2016

(16-6995) Página: 1/5

Original: inglés

Consejo General
Consejo del Comercio de Mercancías
Consejo del Comercio de Servicios
Consejo de los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio
Comité de Comercio y Desarrollo

PROGRAMA DE TRABAJO SOBRE EL COMERCIO ELECTRÓNICO

FIRMAS ELECTRÓNICAS

Comunicación de la Argentina, el Brasil y el Paraguay

La siguiente comunicación, de fecha 15 de diciembre de 2016, se distribuye a petición de las delegaciones de la Argentina, el Brasil y el Paraguay.

1.1. La firma electrónica abarca una amplia gama de soluciones digitales encaminadas a garantizar la autenticidad, integridad y privacidad de las transacciones y comunicaciones internas y transfronterizas que se realizan en línea. En la firma electrónica se emplean datos electrónicos que permiten comprobar la identidad del remitente de un correo electrónico o del comprador de un servicio en línea. En su forma básica, la firma electrónica no precisa de la certificación de una entidad oficial que actúe como tercero independiente.

1.2. En su versión más sofisticada, la firma electrónica, llamada firma electrónica avanzada o firma digital, se basa en un archivo electrónico (un certificado digital avanzado) que constituye una verdadera identidad digital y permite la identificación segura e inequívoca del autor de un mensaje electrónico o de una transacción digital. El certificado digital debe ser expedido por un tercero fiable -una autoridad de certificación oficial o acreditada-, que asociará toda persona física o jurídica a un par de claves criptográficas. El certificado digital no solo permite identificar claramente a una persona en la Web, sino que también asegura la validez jurídica de toda operación digital en que se emplee. Los certificados digitales se están convirtiendo en una herramienta fundamental para el comercio electrónico, los contratos electrónicos, las operaciones bancarias, y las iniciativas de gobierno electrónico, entre otros usos. Por ejemplo, cuando un correo electrónico se envía con un certificado digital, se asegura la identidad del remitente y la integridad del mensaje, y también que su contenido no se ha alterado en modo alguno.

1.3. Ya se ha señalado que la cuestión de la firma electrónica y la autenticación es una cuestión pertinente en el marco de los debates relativos al Programa de Trabajo sobre el Comercio Electrónico (documentos JOB/GC/97/Rev.3 y JOB/GC/98).

1.4. Con el fin de seguir alimentando el debate, la Argentina, el Brasil y el Paraguay desean dar a conocer a los Miembros la Resolución GMC 37/06, que trata esta cuestión en el ámbito del MERCOSUR. Los copatrocinadores están convencidos de que la firma electrónica será un elemento fundamental en todas las cuestiones relacionadas con el comercio electrónico que se examinen en el futuro en la OMC.

MERCOSUR (Resolución GMC 37/06)

Artículo 1 - Ámbito de aplicación

La presente Resolución tiene por finalidad reconocer, en las condiciones previstas en la presente norma, la eficacia jurídica de los documentos electrónicos, de la firma electrónica y de la firma electrónica avanzada en el ámbito del MERCOSUR, contribuyendo a su utilización.

La presente normativa no regula otros aspectos relacionados con la celebración y validez de los actos jurídicos cuando existan requisitos de forma establecidos en las legislaciones nacionales, ni afecta a las normas y límites contenidos en las legislaciones nacionales que rigen el uso de documentos.

La presente normativa no habilita la libre circulación de servicios de certificación digital en el ámbito del MERCOSUR. En lo atinente a la prestación de servicios de certificación digital, los Estados Partes observarán las disciplinas establecidas en el Protocolo de Montevideo sobre Comercio de Servicios del MERCOSUR y en sus Listas de compromisos específicos.

Artículo 2 - Principios

Los Estados Partes observarán los siguientes principios:

1. Autonomía operativa y coordinación permanente entre las infraestructuras nacionales.

2. Interoperabilidad basada en estándares internacionales.

3. Intercambio de información y documentación digital entre los Estados Partes en condiciones técnicas seguras, con validez legal y valor probatorio.

4. Transparencia en la gestión de la certificación digital.

5. Tratamiento neutro en las leyes nacionales con relación a las diversas tecnologías utilizadas en las actividades previstas en la presente Resolución, de modo de permitir la adaptación al ritmo del desarrollo tecnológico inherente a esas actividades (neutralidad tecnológica).

6. Interpretación funcional de los términos y conceptos, a fin de asegurar que no sean negados efectos jurídicos a un proceso o tecnología utilizado por un Estado Parte, por el solo hecho de que se le atribuye una nomenclatura distinta a la prevista en la presente Resolución.

Artículo 3 - Definiciones

A efectos de la presente Resolución, se entenderá por:

1) "**Firma electrónica**": los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados por el firmante como medio de identificación.

2) "**Firma electrónica avanzada**": la firma electrónica que cumple los requisitos siguientes:

a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;

b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

c) ser susceptible de verificación por terceros;

d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable; y

e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.

3) "**Firma digital**": utilizada indistintamente con "firma electrónica avanzada" a los efectos de la presente Resolución.

4) "**Firmante**": la persona física o jurídica que utiliza legalmente un dispositivo para la creación de firma electrónica.

5) "**Documento electrónico**": representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

6) "**Documento digital**": utilizado indistintamente con "documento electrónico" a los efectos de la presente Resolución.

7) "**Certificado digital**": documento electrónico firmado digitalmente que vincula unos datos de verificación de firma con su titular y confirma su identidad.

8) "**Certificado reconocido**": certificado digital emitido por un prestador de servicios acreditado que cumple con los requisitos establecidos por la legislación nacional.

9) "**Certificado avanzado**": utilizado indistintamente con "certificado reconocido" a los efectos de la presente Resolución.

10) "**Prestador de servicios de certificación**": persona física o jurídica, conforme a la legislación nacional, que expide certificados o presta otros servicios en relación con la firma electrónica.

Artículo 4 - Efectos legales de los documentos electrónicos y de las firmas electrónicas

Los Estados Partes reconocen que los documentos electrónicos satisfacen los requerimientos de escritura. En virtud de ello, en cualquiera de los Estados Partes los documentos electrónicos tendrán los mismos efectos jurídicos que los documentos escritos, salvo excepciones contempladas en las legislaciones nacionales.

Los Estados Partes reconocerán efectos jurídicos a la firma electrónica cuando la misma fuese admitida como válida por las Partes que la utilizan o fuese aceptada por la persona a quien fuese opuesto el documento a ella vinculado.

Los Estados Partes asegurarán que no sean negados efectos probatorios a un documento electrónico por el solo hecho de que este no esté vinculado a una firma electrónica avanzada, si por algún medio inequívoco se pudiese demostrar su autenticidad e integridad.

Se respetará la libertad de las Partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas, conforme a su legislación nacional.

En caso de ser desconocida la firma electrónica por una de las Partes, corresponde a la otra Parte probar su validez.

Artículo 5 - Firma electrónica avanzada: Reconocimiento mutuo

Con el objetivo de alcanzar el reconocimiento mutuo de las firmas electrónicas avanzadas y de los certificados digitales, los Estados Partes podrán celebrar, entre sí, acuerdos de reconocimiento mutuo. A tales efectos, el GMC aprobará las Directrices para la celebración de dichos acuerdos. Dichas Directrices reflejarán el estado de la materia al momento de su aprobación y podrán ser actualizadas a propuesta del SGT Nº 13, de manera de acompañar la evolución de las tecnologías a ellas relacionadas.

A través de los acuerdos de reconocimiento mutuo se otorgará a las firmas electrónicas avanzadas, que cumplan con las condiciones dispuestas en ellos, el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas.

Los Estados Partes reconocerán la autenticidad e integridad de un documento electrónico firmado con una firma electrónica avanzada, admitiéndola como prueba documental en procesos judiciales, conforme lo que se disponga en los Acuerdos de Reconocimiento Mutuo.

Los Estados Partes indicarán, en el ámbito del SGT Nº 13, cuáles serán los organismos competentes habilitados para suscribir Acuerdos de Reconocimiento Mutuo.

Artículo 6 - Certificados digitales reconocidos

Los Acuerdos de Reconocimiento Mutuo establecerán las condiciones bajo las cuales los certificados digitales expedidos en un Estado Parte de ese Acuerdo tendrán la misma validez jurídica en los demás Estados Partes que suscriban el Acuerdo.

Dichas condiciones deberán contemplar, como mínimo, que los certificados digitales:

a) sean emitidos por un prestador de servicios de certificación bajo el sistema nacional de acreditación y control previsto en el artículo 7;

b) respondan a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación de cada Estado Parte;

c) respondan a los criterios mínimos establecidos en las Directrices mencionadas en el artículo 5; y

d) contengan como mínimo, los datos que permitan:

    1. identificar indubitablemente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

    2. ser susceptible de verificación respecto de su estado de revocación;

    3. diferenciar claramente la información verificada de la no verificada incluidas en el certificado digital;

    4. contemplar la información necesaria para la verificación de la firma;

    5. identificar la política de certificación bajo la cual fue emitido.

Artículo 7 - Prestación de servicios de certificación

Los Estados Partes no sujetarán a acreditación previa la prestación de servicios de certificación, excepto en aquellos vinculados a una firma electrónica avanzada, de conformidad con los términos de la presente Resolución.

Los Estados Partes asegurarán la creación de un sistema adecuado de acreditación y control de los prestadores de servicios de certificación que emitan certificados reconocidos que permitan la verificación de firmas electrónicas avanzadas, establecidos en sus respectivos territorios.

Los Estados Partes podrán supeditar el uso de la firma electrónica y la firma electrónica avanzada en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y solo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas prescripciones no deberán obstaculizar los servicios transfronterizos.

Artículo 8 - Responsabilidades

Los Estados Partes asegurarán como mínimo que un prestador de servicios de certificación acreditado en los términos del artículo 7, sea responsable por los daños y perjuicios causados a cualquier persona física o jurídica que confíe razonablemente en el certificado digital por él emitido, en lo que respecta a:

a) la inclusión de todos los campos y datos requeridos por las respectivas infraestructuras nacionales para el certificado reconocido y a la exactitud de los mismos, al momento de su emisión;

b) que al momento de emisión de un certificado reconocido por parte del prestador de servicios de certificación acreditado, la firma en él identificada obedece a los datos de creación de firma correspondientes a los datos de verificación incluidos en el certificado reconocido del prestador, con el objeto de asegurar la cadena de confianza;

c) los errores u omisiones que presenten los certificados reconocidos que emitan, o por la inobservancia de los procedimientos de certificación establecidos a partir de los Acuerdos de Reconocimiento Mutuo;

d) el registro en tiempo y forma de la revocación de los certificados reconocidos que haya emitido, cuando así correspondiere.

Corresponde al prestador de servicios de certificación acreditado demostrar que no actuó ni con culpa ni con dolo.

Los Estados Partes asegurarán que el prestador de servicios de certificación acreditado en los términos del artículo 7, pueda indicar en un certificado reconocido de forma identificable por terceros, los límites de su utilización.

El prestador de servicios de certificación acreditado en los términos del artículo 7, no será responsable por los perjuicios resultantes de la utilización de un certificado reconocido por él emitido, que exceda el alcance definido en su política de certificación. Tampoco responderá por eventuales inexactitudes en el certificado reconocido que resulten de la información verificada facilitada por el titular, siempre que el prestador de servicios de certificación acreditado pueda demostrar que ha cumplido todas las medidas previstas en sus políticas y procedimientos de certificación.

Artículo 9 - Protección de datos personales

Los Estados Partes deberán prever que un prestador de servicios de certificación que emite certificados reconocidos destinados al público, solo pueda recolectar los datos personales directamente de la persona a quien esos datos se refieren, después de haber obtenido su consentimiento expreso y solo en la medida en que los mismos sean necesarios para la emisión y mantenimiento del certificado. Los datos no podrán ser obtenidos o utilizados para otro fin, sin el consentimiento expreso del titular de los datos.

Los Estados Partes garantizarán la confidencialidad de los demás datos personales requeridos para la emisión del certificado reconocido y que no figuren en él, en los términos dispuestos por el presente artículo.

_____