FIRMA ELECTRONICA EN EL CONTEXTO DEL GOBIERNO DIGITAL

Dr. Jorge Enrique Romero Pérez (*)
Profesor emérito de la Universidad de Costa Rica

(Recibido 07/06/16 • Aceptado 21/11/16)

(*) Investigador del Instituto de Investigaciones Judiciales. Universidad de Costa Rica.
jorgerp10@gmail.com . Tels. 00-506 2250 1160; 00-506 2259 4844
Apartado postal: 1264, Y Griega 1011, San José. Costa Rica

Resumen: De acuerdo con el desarrollo de la ciencia y la tecnología, la firma digital o electrónica , ha permitido su uso en los sectores privados y en el público.
Mostraremos varios aportes normativos de Costa Rica, Colombia, México, España y la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil, a modo de ejemplo, con el fin de visualizar la regulación de esta firma y sus efectos respectivos.
También, se deja constancia de un glosario útil; y, la bibliografía respectiva.

Palabras Clave: contrato electrónico, documento electrónico, firma digital, repositorio, sistema de información

Abstract: In line with the development of science and technology, the digital or electronic signature has allowed its use in both private and public realms.
We will present several policy inputs of Costa Rica, Colombia, Mexico, Spain, and the United Nations Commission on International Trade Law, by way of example, with the purpose of viewing the regulation of this signature and its subsequent effects.
Additionally, this paper provides a useful glossary and the respective bibliography.

Keywords: Electronic contract, electronic document, digital signature, repository, information system.

Índice

Introducción

De acuerdo con el desarrollo de la ciencia y la tecnología, la firma digital o electrónica , ha permitido su uso en los sectores privados y en el público.

Mostraremos varios aportes normativos de Costa Rica, Colombia, México, España y la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil, a modo de ejemplo, con el fin de visualizar la regulación de esta firma y sus efectos respectivos.

Asimismo, dejaremos indicado un glosario útil y la bibliografía correspondiente.

I.- Gobierno digital

Líneas de acción para establecer un gobierno más transparente, productivo, competitivo y capaz de proporcionar mejores servicios para la sociedad (MIDIPLAN, 2010):

Calidad de Servicio:

- Mejora de la calidad de los servicios
- Centralización del proceso (una sola ventanilla)
- Servicio oportuno
- Disponibilidad de servicios
- Ahorro en costos y tiempo
- Promoción del acceso a los canales municipales

Transparencia y participación:

- Visibilidad de los asuntos públicos
- Conocimiento de la administración gubernamental
- Responsabilidad
- Nuevos canales que faciliten la participación ciudadana y el control social
- Fácil interacción y retroalimentación

Eficiencia del Gobierno:

- Información de calidad, oportuna y normalizada
- Interoperabilidad de las entidades
- Racionalizando los recursos
- Restablecimiento de procesos y procedimientos
- Efectividad del gobierno

Acceso:

- Interconexión de las instituciones por medio de banda ancha
- Integración de los servicios
- Disponibilidad del Internet para toda la población
- Normalización de registros (ciudadanos, productos, firmas entre otros)

Administración y políticas:

- Monitorear el impacto de las acciones
- Regulación de los procedimientos y las tecnologías
- Interoperabilidad
- Publicación y capacitación
- Administración del proyecto

II.- Ley No. 8454 del 30 de agosto del 2005, de certificados, firmas digitales y documentos electrónicos. Costa Rica. Comentarios

Artículo 1.- Ambito de aplicación.

Esta ley se aplicará a toda clase de transacciones y actos jurídicos públicos o privados (…).

El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Comentario:

Esta ley tuvo como finalidad regular el uso y el reconocimiento jurídico de la firma digital, dándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que implique la manifestación de la voluntad, así como autorizar al Estado o administración pública en su conjunto, para su uso práctico y efectivo (Monge, p. 10).

Artículo 8.- Alcance del concepto firma digital (primer párrafo):

Entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Artículo 8.- Alcance del concepto firma digital certificada (segundo párrafo):

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Comentario:

En estos numerales se define lo que es una firma digital y la firma digital certificada.

Para la existencia de una real seguridad transaccional es necesario que el documento sea válido: que la transacción sea segura y que produzca los efectos jurídicos pretendidos para las partes; y, además, que sea válida la asunción de obligaciones, realizadas por los medios electrónicos (Monge, p. 29).

Artículo 9 . Valor equivalente.

Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Los documentos públicos electrónicos deberán llevar la firma digital certificada.

Comentario:

Se define normativamente que la firma digital o electrónica y la firma hecha a mano, tienen jurídicamente un valor equivalente para todos los efectos ; a la vez que se instaura que los documentos públicos electrónicos tienen que llevar la firma digital certificada.

Una de las funciones primordiales de la firma digital, es la de mostrar la identidad, autenticidad, y a la vez acreditar la integridad del contenido del documento electrónico (Monge, p. 32).

III.- Reglamento a la ley de certificados, firmas digitales y documentos electrónicos ,decreto ejecutivo No. 33018 – MICIT (Ministerio de Ciencia y Tecnología) del 20/03/2006. Costa Rica: . Comentarios

Artículo 2, definiciones:

Iinciso 24: *la firma digital es el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor del documento.*

Artículo 2, inciso 25: *la firma digital certificada es la firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado.*

Comentario:

En este numeral, relativo a las definiciones, lo que debe entenderse por firma digital y por firma digital certificada.

Por su parte, el artículo 3 manda:

Aplicación al Estado. A los efectos del párrafo segundo del numeral 1 de la ley, los Supremos Poderes, el Tribunal Supremo de Elecciones, los demás órganos constitucionales y todas las entidades públicas podrán adoptar separadamente las disposiciones particulares que requiera su ámbito específico de competencia o la prestación del servicio público, incluyendo la posibilidad de fungir como certificador respecto de sus funcionarios.

Comentario:

El tema de la firma digital aplicada a la administración pública o Estado, se establece que cada una de las entidades de derecho público, pueden adoptar disposiciones concretas al tenor de la competencia de cada uno de ellos y de la respectiva prestación de servicios públicos; agregando que además, pueden llevar a cabo la tarea de certificador de sus agentes públicos.

El artículo 4, Incentivo de los mecanismos de gobierno electrónico, dispone:

Con excepción de aquellos trámites que necesariamente requieran la presencia física del ciudadano, o que éste opte por realizarlos de ese modo, el Estado y todas las dependencias públicas incentivarán el uso de documentos electrónicos certificados y firmas digitales para la prestación directa de servicios a los administrados, así como para facilitar la recepción, tramitación y resolución electrónica de sus gestiones y la comunicación del resultado correspondiente.

Comentario:

Se establece que hay un deber de motivación y de incentivación para todo el Estado para la utilización de documentos electrónicos y de firmas digitales, dentro del contexto del gobierno digital.

IV.- Normativa de Colombia:

a) Ley 527 del 18 de agosto de 1999 y sus reformas

Artículo 2.- Definiciones.

Presenta 6 definiciones, las cuales se han incorporado al glosario, bajo la identificación de LCo (ley Colombia).

Artículo 5º. Reconocimiento jurídico de los mensajes de datos.

No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

Comentario:

Se le da fuerza y efectos jurídicos al mensaje de datos.

Artículo 9º. Integridad de un mensaje de datos.

Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Comentario:

Se parte del supuesto de que la información que se encuentre en un mensaje de datos es íntegra; pero, se establecen requisitos y límites para que esa presunción sea efectiva.

Artículo 14. Formación y validez de los contratos.

En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Comentario:

En materia contractual, la oferta y su aceptación, se puede manifestar a través de uno o varios mensajes de datos.

Artículo 28. Atributos jurídicos de una firma digital.

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Comentario:

Se establece la presunción de que si la firma digital se ubica en un mensaje de datos, el suscriptor tuvo la intención de acreditar el mensaje y de vincularse al mismo.

b) Reglamento al artículo 7 de la ley No. 527 de 1999 (decreto No. 2364 del 22 de noviembre del 2012). Comentario

Presenta 4 definiciones, que se han incluido en el glosario con la identificación: RCo (reglamento Colombia).-

Artículo 7. *Firma electrónica pactada mediante acuerdo. Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica según el caso, que acuerden utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica.*

Comentario:

Para proteger el uso de la firma electrónica, se parte del supuesto de que se cumple con los requisitos para su utilización; indicándose "salvo prueba en contrario".

V.- Código de Comercio de México, en su numeral 89, define la firma electrónica así:

Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo por cualquier tecnología, los cuales son utilizados para identificar al firmante en relación con el mensaje de datos que signa, y es indicativa que el firmante aprueba la información contenida en el mensaje de datos y produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio (García, p. 104, 2016).

Comentario:

Se dan estos elementos fundamentales derivados del concepto:

1. Medio de identificación del firmante autor del mensaje, formado por un conjunto de datos, ajenos al mensaje de datos signado, adjuntados o asociados a éste último,

2. Es la aprobación o autorización del firmante de la información que contiene el mensaje de datos o documentos electrónico que signa,

3. Es un equivalente funcional a la firma autógrafa, pues tiene los mismos efectos,

4. Sirve como prueba en el juicio correspondiente (García, pp. 105 y 106, 2016).

VI.- Ley de firma electrónica No. 59 del 19 de diciembre del 2003, España . Comentario

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. *La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

2. *La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*

3. *Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

4. *La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.*

5. *Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.*

6. *El documento electrónico será soporte de:*

   a) *Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.*

   b) *Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.*

   c) *Documentos privados.*

7. *Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.*

8. *El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.*

9. *No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.*

10. *A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.*

Comentario:

En este numeral 3, se definen la firma electrónica, firma electrónica avanzada y firma electrónica reconocida.

Igualmente se define el documento electrónico y se indica de cuáles elementos se considera soporte. Asimismo, se establece el valor jurídico de los documentos electrónicos y de la firma digital en un proceso judicial, lo cual vale también en un proceso administrativo.

Artículo 4. Empleo de la firma electrónica en el ámbito de las administraciones públicas.

1. *Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.*

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

Comentario:

Se establece el uso de la firma electrónica al interior del Estado y entre éste y el sector privado.

En los procedimientos administrativos públicos, el Estado podrá establecer condiciones adicionales al uso de la firma digital. Podrá hacer uso de la fecha electrónica, que se entiende como el conjunto de datos electrónicos, usados para la constatación del momento de actuación en relación a otros datos digitales a los cuales estén asociados.

2. *Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.*

Comentario:

Las condiciones adicionales deben cumplir con lo que dispone el numeral 45 de la Ley de régimen jurídico de las administraciones públicas y del procedimiento administrativo común; y, además cumplir con ciertos requisitos que se señalan.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Comentario:

Las citadas condiciones generales adicionales para el uso de la firma electrónica ante el Estado, deben ser propuestas por los Ministerios de Administraciones Públicas y de Ciencia y Tecnología, mediante un previo informe del Consejo Superior de Informática y para el impulso de la Administración electrónica . Estos requisitos de funcionamiento los considero adecuados respecto de la buena utilización de la firma digital.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

Comentario:

Las citadas condiciones adicionales deben cumplir con los requisitos de ser objetivas, proporcionadas, transparentes, no discriminatorias y no deben ser un obstáculo al servicio de certificación a las personas.

VII.- Ley modelo sobre las firmas electrónicas, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. 12/12/ 2001. Comentario.

Su artículo 2, se refiere a las definiciones de acuerdo a los fines de la presente Ley. Están incorporadas en el glosario bajo la letra C (Comisión).

Su artículo 3, regula la igualdad de tratamiento de las tecnologías para la firma.

Ninguna de las disposiciones de la presente ley, con la excepción del numeral 5 (las partes podrán establecer excepciones a la presente ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable), será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 (cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica, que a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje) *o que cumpla de otro modo los requisitos del derecho aplicable.*

Comentario:

Esta ley modelo, manda que lo que ella establece tiende a proteger la firma electrónica .

Conclusión

En el plano del gobierno digital, el tema de la firma electrónica es clave para la modernización del funcionamiento del Estado; y, el cumplimiento entre otros aspectos como la rendición de cuentas de los empleados y funcionarios públicos (agentes públicos) y de la transparencia de la actuación del sector público.

La Asociación Bancaria Costarricense, (ABC), pide a la Superintendencia General de las Entidades Financieras (SUGEF) más tiempo para exigir a sus clientes la firma digital . La SUGEF puso como plazo el 31 de diciembre del 2017 para que el 100 % de sus clientes usara la firma digital en sus transacciones en línea. La ABC solicitó

a la SUGEF un plazo mayor para la utilización de la firma digital, debido a la complejidad operativa y el costo. Para la Cámara de Bancos, exigir la firma digital traerá limitaciones a los usuarios de la banca electrónica (Oscar Rodríguez, La Nación, sábado 30/04/16, p. 27 A).-

Definiciones o glosario

(**Nota:** si la definición está tomada del libro de García 2016, pp. 125 a 129, se indica con una **G**; si se toma del Reglamento de Costa Rica, se le coloca una **R**; si es de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: **C**; si es la ley No. 527 de 1999, de Colombia: **LCo**; si es del reglamento al artículo 7 de esta ley No. 527 de 1999, decreto No. 2364 del 22 de noviembre del 2012: **RCo**).

Acuerdo sobre el uso del mecanismo de firma electrónica: acuerdo de voluntades mediante el cual se estipulan las condiciones legales y técnicas a las cuales se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos. **RCo**

Autenticación: *verificación de la identidad de un individuo.*

a. En el proceso de registro, es el acto de evaluar las credenciales de la entidad final (por ejemplo, un suscriptor) como evidencia de que realmente es quien dice ser.

b. Durante el uso, es el acto de comparar electrónicamente las credenciales y la identidad enviada (Ej., código de usuario y contraseña, certificado digital, etc.) con valores previamente almacenados para comprobar la identidad. **R**

Autenticación mutua*:* proceso mediante el cual dos entidades verifican su identidad en forma recíproca. **R**

Autenticidad: la veracidad, técnicamente constatable, de la identidad del autor de un documento o comunicación. La autenticidad técnica no excluye el cumplimiento de los requisitos de autenticación o certificación que desde el punto de vista jurídico exija la ley para determinados actos o negocios. **R**

Autoridad de registro (ar): entidad delegada por el certificador registrado para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados digitales. Representa el punto de contacto entre el usuario y el certificador registrado. **R**

Bitácoras de auditoria: registro cronológico de las actividades del sistema, que son suficientes para habilitar la reconstrucción, revisión, y la inspección de la secuencia del entorno y las actividades secundarias o primarias para cada evento en la ruta de una transacción desde su inicio hasta la salida del resultado final. **R**

Certificación: proceso de creación de un certificado de llave púbica para un suscriptor . **R**

Certificado: se define como todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica. **G**

Se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma. **C**

Certificado digital: una estructura de datos creada y firmada digitalmente por un certificador, del modo y con las características que señalan este Reglamento y su anexo, cuyo propósito primordial es posibilitar a sus suscriptores la creación de firmas digitales, así como la identificación personal en transacciones electrónicas. Sin perjuicio del concepto anterior, la Dirección de certificadores de firma digital, podrá autorizar a los certificadores registrados la generación de certificados con propósitos diferentes o adicionales a los indicados. **R**

Certificado suspendido: cesación temporal o interrupción de la validez de un certificado. **R**

Certificado válido: se refiere a aquel certificado que se encuentra activo, que ha sido emitido por un certificador registrado. **R**

Certificador: la persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales. **R**

Certificador raíz: el nodo superior autocertificante de la jerarquía nacional de certificadores registrados. **R**

Certificador registrado: el certificador inscrito y autorizado por la Dirección de Certificadores de Firma Digital. **R**

Certificador padre: certificador registrado que se encuentra en la posición inmediata superior con respecto a otro certificador registrado, en la jerarquía de certificadores. **R**

Certificador subordinado*:* certificador registrado que se encuentra en la posición inmediata inferior con respecto a otro certificador registrado, en la jerarquía de certificadores. **R**

Comercio electrónico: comprende todas aquellas transacciones comerciales, nacionales e Internacionales, que se realizan por intercambio electrónico de datos y por otros medios de comunicación electrónica. **G**

Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera. **LCo**.

Compromiso: violación de la seguridad de un sistema, por haber ocurrido una divulgación no autorizada de información sensible. **R**

Contrato electrónico: es el celebrado sin la presencia física de las partes, prestando éstas su consentimiento en origen y destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, concretados por medio de cable, radio, medios ópticos o cualquier medio transmisor en vía electrónica, con la ficción jurídica, de que su

celebración debe tenerse como si se realizase entre sujetos físicamente presentes. **G**

Control múltiple: condición mediante la cual dos o más partes, separada y confidencialmente, tienen la custodia de los componentes de una llave particular, pero que individualmente no tienen conocimiento de la llave resultante. **R**

Datos de activación*:* valores de datos (que no son las llaves), que son requeridos para operar los módulos criptográficos y que necesitan ser protegidos (ejemplo: PINs, frase clave, biométricos o llaves distribuidas manualmente). **R**

Datos de creación de firma: son los datos únicos, como códigos o claves criptográficas privadas, que el firmante genera de manera secreta y utiliza para crear su firma electrónica, logrando un vínculo entre ésta y su persona. Esta definición determina los elementos de confidencialidad y de vinculación entre su creador y la propia firma. G

Datos de creación de la firma electrónica: datos únicos y personalísimos, que el firmante utiliza para firmar. **RCo**

Datos de verificación de firma: son los datos, consignados como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica. **G**

Derecho a la autodeterminación informativa: facultad de la persona de determinar quien puede conocer, almacenar, usar y transmitir sus datos personales. **G**

Declaración de las prácticas de certificación *(dpc):* declaración de las prácticas que utiliza el certificador para la emisión de los certificados (define el equipo, las políticas y los procedimientos que el certificador utiliza para satisfacer los requerimientos especificados en las políticas del certificado que son soportados por él). **R**

Destinatario: es la persona designada por el emisor para recibir el mensaje de datos, que no actúa a título de intermediario con respecto a dicho mensaje. **G**

Dirección de certificadores de firma digital *(dcfd):* dependencia del Ministerio de Ciencia y Tecnología, encargada de la administración y supervisión del sistema de certificación digital. **R**

Dispositivo de creación de firma: es un programa o un aparato informático que sirve para aplicar los datos que se hayan generado para crear la firma. **G**

Dispositivo de verificación de firma: es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma. **G**

Dispositivo o modulo seguro de creación de firmas *(mscf)*: dispositivo que resguarda las claves y el certificado de un suscriptor, utilizado para generar su firma digital y que, al menos, garantiza:

a. Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;

b. Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior; y,

c. Que los datos empleados en la generación de la firma pueden ser protegidos de modo fiable por el firmante legítimo, contra su utilización por cualesquiera terceros. **R**

Dispositivo seguro de creación de firma: es un de creación de firma y es necesario:

1. Que garantice que los datos utilizados para la firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2. Que exista seguridad razonable para que dichos datos no puedan dan ser derivados de los de verificación de firma o de la propia firma y que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3. Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma. **G**

Documento electrónico: cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático. **R**

Emisor: es toda persona que al tenor del mensaje de datos, haya actuado a nombre propio o en cuyo nombre se haya generado y enviado ese mensaje antes de ser archivado, y que no haya actuado a título de intermediario. **G**

Ente costarricense de acreditación (eca): la dependencia pública a que se refiere la "Ley del Sistema Nacional para la Calidad", número 8279 de 2 de mayo del 2002. **R**

Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.**LCo**

Entidad final: suscriptor del certificado. **R**

Firma digital: conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento. **R**

Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. **LCo**

Firma digital certificada: una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado. R

Firma electrónica: se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos. **C**

Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente. **RCo**

Firmante: se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa. **C**

Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa. **RCo**

Es la persona que posee los datos de creación de firma y actúa a nombre propio o de la persona que representa, o signatario que es la persona física que cuenta con un dispositivo de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

Puede ser cualquier persona la firmante, al no hacer distinción alguna respecto de que ésta sea física o moral, ya que no existe ningún impedimento legal para que una persona moral sea titular de firma electrónica, máxime que se utiliza fundamentalmente en las operaciones de comercio empresarial, por lo que los Datos de creación de firma, son generados por persona física debidamente facultada por ésta, para realizar actos de representación de la corporación mediante la citada firma.

La posesión de la firma, como ya se ha indicado, se refiere al de Datos que la contiene, esto a su codificación, es lo que del uso exclusivo del firmante, como es el caso de la firma autógrafa o manuscrita en papel, en este caso lo que se posee o tiene por su creador o autor, como

sería su nombre o firmas propias, quien solo debe tener el dispositivo de creación por ser la creó, y que lo identifica de manera exclusiva. **G**

Infraestructura de llave pública (pki por sus siglas en inglés): Se refiere a una estructura de hardware, software, personas, procesos y políticas que emplean tecnología de firma digital para proveer una asociación verificable entre una llave pública y un suscriptor específico que posee la llave privada correspondiente. **R**

Integridad: propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión, o bien que -habiendo sido alterados posteriormente- lo fueron con el consentimiento de todas las partes legitimadas. **R**

Habeas data: significa en términos generales un recurso pronto y expedito para lograr que un dato que obre en archivos, registros, bases de datos sea complementado, actualizado, corregido, bloqueado, destruido, o bien que una sede de datos, sean incluidos en esos mismos registros, archivos, bancos o bases además que permita accesar a los mismos. **G**

Intercambio Electrónico de Datos *(EDI)*. La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto. **LCo**

Intermediario: es toda persona que actuando por cuenta de otra, envía, recibe o archiva sus mensajes de Datos, o presta algún servicio a dicho respecto. **G**

Ley: La Ley de Certificados, Firmas Digitales y Documentos electrónicos, Ley número 8454 del 30 de agosto del 2005. **R**

LGAP: La Ley General de la Administración Pública. Costa Rica **R**

Lineamientos técnicos: el conjunto de definiciones, requisitos y regulaciones de carácter técnico-informático. **R.**

LRC: Lista de revocación de certificados. **R**

Mensaje de datos: es la información generada, enviada, da o archivada por medios electrónicos, ópticos o cualquier tecnología. **G**

Se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax. **C**

La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax **LCo**

Mecanismo en línea para verificar el estado del certificado: mecanismo mediante el cual se permite a las partes que confían, consultar y obtener, la información del estado de un certificado sin requerir para ello el uso de una LRC. **R**

Oficina de tarjetas (card bureau): agente del certificador registrado o de la autoridad de registro que personaliza la tarjeta de circuito integrado (o tarjeta inteligente), que contiene la llave privada del suscriptor (como mínimo). **R**

Parte confiante: se refiere a las personas físicas, equipos, servicios o cualquier otro ente que confía en la validez de un certificado emitido por un certificador específico. **R**

Parte que confía: es la persona que siendo o no el destinario, actúa sobre la base de un certificado o de una firma electrónica, es decir, es toda aquella persona que no siendo un destinatario específico acepta el mensaje de datos, y debe diferenciarse de la parte confiable que es el sujeto que funge como intermediario. **G**

Se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica. **C**

Políticas del certificado (pc): conjunto de reglas que indican la aplicabilidad del certificado a una comunidad particular y/o clase de aplicaciones con los requerimientos comunes de seguridad. **R**

Prestador de servicios de certificación: es la persona moral, institución pública, notario o corredor público, que presta servicios relacionados con firmas electrónicas y que expide los certificados respecto de éstas. Es la persona física o moral que expide certificados, pudiendo

prestar, además, otros servicios en relación con la firma electrónica, sólo pueden ser prestadores de estos servicios: los corredores o notarios públicos, de acuerdo con el artículo 100 del Código de Comercio de México. **G**

Se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas. **C**

Productor de bases de datos: es el que recoge las informaciones desde diversas fuentes y las somete a un tratamiento que permita su consulta a través de medios automatizados. **G**

Protocolo en línea para determinar el estado del certificado *(ocsp por sus siglas en inglés)*: protocolo suplementario para determinar el estado actual de un certificado. **R**

Recuperación de llaves: capacidad de restaurar la llave privada de una entidad a partir de un almacenamiento seguro, en el caso de que se pierda, corrompa o que por cualquier otra razón se convierta en no utilizable. **R**

Re-emisión de llaves del certificado: proceso por medio del cual una entidad con un par de llaves y un certificado previamente emitidos, luego de la generación de un nuevo par de llaves, recibe un nuevo certificado y una nueva llave pública. **R**

Reglamento: este reglamento. **R**

Renovación del certificado: proceso donde una entidad emite una nueva instancia de un certificado existente, con un nuevo período de validez. **R**

Repositorio: sistema de almacenamiento y distribución de certificados e información relacionada (Ej., almacenamiento y distribución de certificados, almacenamiento y recuperación de políticas de certificación, estado del certificado, etc.). **R**

Rol de confianza: función de trabajo que permite ejecutar labores críticas. Si dichas labores se ejecutan de una forma insatisfactoria puede ocurrir un impacto adverso, que dará como resultado una degradación en la confianza que provee el certificador. **R**

Sello de garantía (tamper evident): características de un dispositivo que proveen evidencia de que existió un intento de ataque sobre él. **R**

Servicios de validación de certificados: servicios provistos por el certificador registrado o sus agentes que ejecutan la tarea de confirmar la validez del certificado a una tercera parte que confía. **R**

Servidor: es el que administra uno o más servicios o productos informáticos existentes en el mercado, a través de alguno de los sistemas de telecomunicaciones disponibles (telefonía, satelitales, cables). Cuenta para ello con una estructura técnica adecuada (puertas o portales) que le permiten organizar eficientemente las entradas de los múltiples usuarios a los diversos servicios de consulta o transacción. **G**

Sistema de información: es todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma de mensaje de datos. **G**

Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. **LCo**

Suscriptor: la persona física a cuyo favor se emite un certificado digital y que lo emplea para los propósitos señalados en este reglamento, en conjunto con las claves, contraseñas y/o dispositivos necesarios al efecto y de cuya custodia es responsable. **R**

Titular del certificado: es la persona a cuyo favor se expide el certificado. **G**

Transportador: es el organismo público o privado que dispone o mantiene alguna red de telecomunicaciones, sea en régimen de propiedad (entes estatales), o en carácter de permisionario (empresas, entidades mixtas). **G**

Usuario: es el beneficiario del servicio, que lo utiliza a través de una terminal , conectado al servidor de la información (banco de datos) o gestor de transacciones (transferencias, telecompras, mensajerías, entre otros). **G**

Verificación de firma: Con relación a la firma digital, significa determinar con precisión:

(1) que la firma ha sido creada durante el período operacional de un certificado válido, utilizando la llave pública listada en el certificado; y,

(2) que el mensaje no ha sido alterado desde que la firma fue creada. Rutilización concreta de la firma electrónica relativa a información clasificada, seguridad pública o defensa nacional, será regulada por la respectiva normativa . Se trata de una excepción a la normativa general. **R**

Bibliografía

Barahona, Juan Carlos (dirección) (2015) *Evaluación de la calidad de la prestación de servicios públicos por medios digitales en Costa Rica* (Alajuela, Costa Rica, Instituto Centroamericano de Administración de Empresas, INCAE, www.incae.edu)

Campoli, Gabriel (2004) *Firma electrónica en el régimen comercial mexicano* (México: Porrúa)

Domínguez-Macaya, Jaime (2011) *Claves para una contratación pública electrónica eficaz*

(Madrid: El consultor de los ayuntamientos- La Ley)

García, Raquel (2016) *La firma electrónica, desde el punto de vista jurídico* (México: Porrúa)

Laborde, Carolina (2010) *Electronic Signatures in International Contracts* (Berne: Peter Lang Press; European University Studies)

León, Soyla et al (2009) *La firma electrónica avanzada*

(México: Oxford University Press)

Micó, Javier (2007) *La firma electrónica de notarios y registradores y el documento público electrónico* (Valencia, España: Tirant lo Blanch)

Mason, Stephen (2012) *Electronic Signatures in Law*

(UK: Cambridge University Press)

MIDIPLAN (Ministerio de planificación nacional y política económica) (2010) *Plan maestro de gobierno digital de Costa Rica*

(San José, Costa Rica, www.midiplan.go.cr)

Monge, Ignacio (2009) *Ley de certificados, firmas digitales y documentos electrónicos. Comentada y concordada*

(San José: Editorial Investigaciones Jurídicas)

Moreno, José Antonio (2015) *El nuevo derecho de la contratación pública de la Unión europea.Directivas* 2014

(UK: Chartridge Books Oxford)

Pérez, Pablo (dirección) (2011) *Guía sobre licitación y contratación pública electrónica* (Madrid: Ministerio de Industria, Turismo y Comercio-Instituto Nacional de Tecnologías de la Comunicación, www.av-asesores.com)

Reyes, Alfredo (2003) *La firma electrónica y las entidades de certificación* (México: Porrúa)

Romero-Pérez, Jorge Enrique (2013) *Contratación electrónica del Estado.* Costa Rica (San José: Editorial Universidad de Costa Rica)

(2012) *Derecho Internacional de las Contrataciones públicas electrónicas.* (San José: Editorial Universidad de Costa Rica)

Schellekens, M H M (2004) *Electronic Signatures: Authentication Tecnology from a Legal Perspective* . (The Hague: T M C Asser Press)