ARTICULO 7o. FIRMA.

Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ARTICULO 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.

ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS.

Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

1 Notas de Usuario Crear nota

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ARTICULO 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS.

Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1 Notas de Usuario

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y

3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

ARTICULO 13. CONSERVACIÓN DE MENSAJES DE DATOS Y ARCHIVO DE DOCUMENTOS A TRAVÉS DE TERCEROS.

El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

ARTICULO 28. ATRIBUTOS JURIDICOS 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.

PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.

2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.

5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

ARTICULO 29. CARACTERÍSTICAS Y REQUERIMIENTOS DE LAS ENTIDADES DE CERTIFICACIÓN.

< Artículo modificado por el artículo 160 del Decreto 19 de 2012. El nuevo texto es el siguiente: > Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional. El Organismo Nacional de Acreditación de Colombia suspenderá o retirará la acreditación en cualquier tiempo, cuando se establezca que la entidad de certificación respectiva no está cumpliendo con la reglamentación emitida por el Gobierno Nacional, con base en las siguientes condiciones:

a. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

b. Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;

c. Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

ARTICULO 30. ACTIVIDADES DE LAS ENTIDADES DE CERTIFICACION.

< Artículo modificado por el artículo 161 del Decreto 19 de 2012. El nuevo texto es el siguiente: > Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país , podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje d datos y de documentos electrónicos transferibles.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a l documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.

4. Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepci de mensajes de datos.

6. Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.

7. Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.

8. Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónic transferibles.

9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.

ARTICULO 35. CONTENIDO DE LOS CERTIFICADOS.

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.