

## LEGISLACION INFORMATICA

### PROYECTO DE LEY REGULADORA DE LOS DATOS PERSONALES INFORMATIZADOS EN EL ECUADOR

Por:

**Libardo Orlando Riascos Gómez**  
**Doctor en Derecho**  
**2003**

**NOTA:** El Proyecto Ley tiene la estructura y contenido de la Ley reguladora de datos personales de España, conocida como la **LORTAD de 1992, derogada** por la [Ley 15 de 1999](#), Diciembre 13, "Protección de datos de carácter personal". Igualmente del Convenio Europeo de Estrasburgo de 1981, Sobre la protección de las personas relativas a la protección de los datos personales automatizados.

## ECUADOR

### PROYECTO DE LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS.

#### TITULO PRELIMINAR

##### **Artículo 1 : Ambito de aplicación:**

Esta Ley regula la eficacia y valor jurídico de los documentos electrónicos, el uso de la firma electrónica, la prestación de servicios de certificación, el manejo de bases de datos y la protección a los usuarios del comercio electrónico.

Las disposiciones contenidas en esta Ley se complementarán y se regirán por los principios generales establecidos en la Constitución y las Leyes.

##### **Art. 2.- Glosario de Términos:**

**Mensajes de Datos:** Toda aquella información generada por medios electrónicos, digitales o similares que puede ser almacenada o intercambiada por cualquier medio. Podrán ser mensajes de datos sin que esta enumeración limite su definición los siguientes: Documentos Electrónicos, Correo electrónico, páginas web, telegrama, telex, fax, facsímile e Intercambio electrónico de datos.

**Documento Electrónico:** Documento en formato electrónico con información electrónica o digital que se genera o almacena por cualquier medio.

**Comercio Electrónico:** Toda transacción civil, comercial o financiera, contractual o no, que se efectúe a través del intercambio de mensajes de datos o medios similares.

**Firma Electrónica:** Dato en formato electrónico asignado a un documento electrónico o mensaje de datos por el autor del mismo, su representante o mecanismo autorizado por él y que permitirá certificar su autenticidad e integridad a través de procedimientos técnicos de comprobación.

**Intercambio Electrónico de Datos:** Intercambio normalizado de datos entre dos o más sistemas.

**Mecanismo de emisión:** Instrumento físico o lógico utilizado por el signatario de un documento para crear mensajes de datos o una firma electrónica

**Mecanismo de comprobación:** Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o un documento creado con una firma electrónica.

**Certificado electrónico de Identidad:** Documento electrónico que vincula a un mecanismo de comprobación con una persona natural o jurídica y confirma su identidad.

**Proveedor del servicio de certificación:** Persona natural o jurídica que está legalmente en capacidad de emitir certificados de identidad y proporcionar servicios relacionados con comercio y firma electrónica y para lo cual debe cumplir con los requisitos determinados en esta Ley y sus Reglamentos, deberá disponer de las herramientas físicas y lógicas necesarias y acordes al tipo de servicio a prestar.

**Emisor:** Persona natural o jurídica que firma y origina un mensaje de datos. Se entenderá como emisor aun cuando no genere el mensaje por sí mismo o lo haga a través de terceros o de

mecanismos automatizados de cualquier tipo siempre y cuando éstos se encuentren debidamente autorizados.

**Destinatario:** Persona natural o jurídica a quien va destinado el mensaje de datos. Se entenderá como Destinatario aun cuando no reciba el mensaje por si mismo o lo haga a través de terceros o de mecanismos automatizados de cualquier tipo siempre y cuando éstos se encuentren debidamente autorizados.

**Signatario:** Se entenderá la persona que consigna, o en cuyo nombre se consigne una firma electrónica.

**Suscriptor:** Será el Destinatario que hubiere aceptado las condiciones de un contrato preestablecido siguiendo las instrucciones contenidas en un mensaje de datos.

**Fedatario Público Electrónico:** Serán los Notarios que de acuerdo con la Leyes que regulan su actividad, cumplan los requisitos señalados en ésta ley para certificar firmas electrónicas.

**Sistema de información:** Se entenderá como sistema de información, a todo sistema utilizado para enviar, recibir, procesar o archivar de cualquier forma mensajes de datos.

**Criptografía:** Es la codificación de mensajes de datos ilegibles y que mediante un uso de algoritmos matemáticos o señales autorizadas puede ser devuelto a su forma original o legible.

**Usuario:** Toda persona que utilice sistemas de información o comunicación electrónica. Este podrá estar suscrito o no a un Proveedor de Servicios de Certificación y en base al uso de un certificado o al manejo de claves o códigos entregados por el emisor, podrá acceder a la información intercambiada.

**Quiebra técnica:** Es la incapacidad temporal o permanente del proveedor de servicios de certificación que impida garantizar el cumplimiento de los requisitos establecidos para la firma electrónica.

## **TITULO PRIMERO**

### **CAPITULO I**

#### **PRINCIPIOS GENERALES**

**Art. 3 .- Efectos de la Ley.-** Se reconoce la fuerza jurídica y la validez de los mensajes de datos, cualquiera sea su forma, así como la información que estos contengan. Los mensajes de datos, su información y contenido tendrán igual

valor jurídico que los documentos públicos y privados y su eficacia y valoración se someterán al cumplimiento de lo establecido en esta Ley.

**Art.4 .- Interpretación.-** La interpretación de esta Ley se someterá a los métodos de interpretación del Código Civil y demás leyes concordantes. La interpretación de aquellos casos no determinados en esta Ley se basarán en el uso normalmente conocido de los términos relacionados con el Comercio Electrónico o en su aplicación técnica de uso general, en las Normas, Acuerdos y Tratados Internacionales que sobre la materia se hubieren celebrado.

**Art. 5 .- Propiedad Intelectual.-** Todos la información relacionada con los mensajes de datos o transmisión de datos por cualquier forma o medio, sea esta dentro o fuera del Comercio Electrónico, estará sometida a las Leyes, Reglamentos y Acuerdos Internacionales relativos a la Propiedad Intelectual.

**Art. 6 .- Confidencialidad.-** El principio de la confidencialidad regirá para los mensajes de datos, cualquiera sea su forma medio o intención. Toda violación a este principio será sancionado conforme a lo dispuesto en el Código Penal, Ley de Propiedad Intelectual y demás leyes que rijan la materia.

**Art. 7.- Información escrita.-** Cuando las Leyes requieran que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.

**Art. 8 .- Información original.-** Cuando la Ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si siendo requerido conforme a la Ley, existe garantía fidedigna de que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.

Se considera que un mensaje de datos permanece íntegro si se mantiene completo e inalterable, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

**Art. 9 .- Conservación de los mensajes de datos.-** Cuando la Ley requiera que ciertos documentos, registros, o informaciones sean conservados, ese requisito quedará satisfecho

mediante la conservación de los mensajes de datos, siempre que se cumplan las siguientes condiciones:

- a). Que la información que contengan sea accesible para su ulterior consulta;
- b). Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada o recibida; y
- c). Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

La obligación de conservar ciertos documentos, registros o informaciones no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

Toda persona podrá recurrir a los servicios de un tercero para observar o verificar los requisitos señalados en éste artículo.

**Art. 10 .- Obligatoriedad de Firma.-** Cuando la Ley exija la firma de una persona, ese requisito quedará satisfecho en un mensaje de datos, si se utiliza un método seguro y fiable para identificar al titular de esa firma electrónica de acuerdo a lo establecido en esta Ley.

**Art. 11. - Protección de datos.-** Para la elaboración de bases de datos obtenidas en la transmisión de mensajes de datos, se requerirá de la autorización expresa y afirmativa del usuario, el mismo que podrá seleccionar la información a compartirse con terceros.

Las bases de datos obtenidas como resultado del intercambio de mensajes de datos, serán protegidas de acuerdo con los derechos de propiedad intelectual vigentes, su uso y disposición estarán sometidos a la autorización expresa de su titular.

Los datos obtenidos con el consentimiento y voluntad de una persona responderán a los principios de privacidad e intimidad garantizados por la Constitución de la República y podrán ser utilizados o transferidos únicamente con su autorización u orden de autoridad competente.

Toda persona tiene derecho al libre acceso a los datos públicos o privados que contengan información relacionada con su persona, para lo cual ejercerá su derecho al habeas data consagrado en la Constitución vigente o en las leyes que regulen la institución.

## **CAPITULO II**

### **FIRMAS ELECTRONICAS**

**Art. 12.- Efectos de la firma electrónica.** La firma electrónica, tendrá igual validez y se le reconocerá los mismos efectos jurídicos que a una firma manuscrita. Deberá reunir los requisitos determinados en esta Ley, guardar concordancia con el cuerpo de Leyes ecuatoriano y cumplir con las reglamentaciones que para el efecto se dictare.

**Art. 13.- Requisitos de la firma electrónica:** Para tener validez, la firma electrónica reunirá como mínimo los siguientes requisitos:

- a).- Ser individual, única o vinculada exclusivamente a su titular, y capaz de ser mantenida bajo el estricto control de la persona a quien pertenece y usa.
- b).- Disponer de las seguridades necesarias que garanticen su integridad.
- c).- Ser verificable inequívocamente mediante mecanismos técnicos de comprobación, establecidos por la Ley, los Reglamentos o el acuerdo de las partes.

Cualquier requisito adicional a los aquí señalados, deberá constar expresamente determinado en la Ley.

**Art. 14 .- La firma electrónica en un mensaje de datos:** Debe ser parte integrante del mensaje de datos, enviarse en un mismo acto y ser inalterable, de tal forma que si se cambia el documento o la firma, ésta se invalide. Cumplidos los requisitos de seguridad e inalterabilidad, se presumirá la integridad del mensaje de datos.

Cuando se fijare la firma electrónica en un mensaje de datos, salvo prueba en contrario, se presumirá que éste conlleva el acuerdo de voluntad del Emisor y se someterá al cumplimiento de las obligaciones o contratos de acuerdo a lo determinado en la presente Ley y demás Leyes pertinentes.

**Art. 15 .- Obligaciones vinculadas a la firma electrónica:** La firma electrónica, mientras el certificado no sea revocado, suspendido o cancelado vincula al titular o a su representado en sus obligaciones frente a terceros de buena fe.

Frente al tercero de buena fe no cesará la eficacia de la firma electrónica por muerte, incapacidad, liquidación, quiebra o cualquier otra causa restrictiva de la capacidad de la persona a quien se impute los efectos de la firma electrónica.

**Art. 16.- Obligaciones del titular de la firma electrónica:**

a). Actuar con diligencia para evitar toda utilización no autorizada de su firma.  
b). Notificar al proveedor de servicios o a los interesados, por cualquier medio, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y pueda utilizarse para falsificar su firma electrónica.

c). Asegurar la exactitud de sus declaraciones en todos sus actos.  
d). Cumplir con las obligaciones derivadas del uso ilegal de su firma si no ha obrado con la debida diligencia para impedir la utilización no autorizada de su firma y para evitar que el destinatario confíe en ella, salvo que el destinatario supiera o hubiera debido saber que la firma no era autorizada.

**Art. 17 .- Duración de la firma electrónica:** Esta duración estará sujeta a la voluntad del titular de dicha firma, de acuerdo a lo que se estableciere en la Ley y sus reglamentos.

**Art. 18 .- Revocación de la firma electrónica:** La revocación de la firma electrónica se producirá a solicitud del titular de la misma y el proveedor del servicio de certificación está obligado a proceder a la revocación inmediata y a su publicación de acuerdo con ésta Ley..

La revocación de la firma electrónica no exime a su titular de las obligaciones previamente contraídas.

**Art. 19 .- Cancelación y suspensión de la firma electrónica:** El proveedor del servicio de certificación podrá suspender de modo temporal o cancelar el certificado de firma electrónica cuando:

- a). Sea solicitado por autoridad competente de acuerdo a la legislación vigente.
- b). Se compruebe que alguno de los datos del certificado es falso.
- c). Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación y el Usuario.
- d). El proveedor del servicio de certificación cese en sus actividades y los certificados vigentes ya emitidos por el mismo servicio de certificación no sean asumidos por otro servicio de certificación.
- e). El proveedor del servicio de certificación está en la obligación de publicar inmediatamente dicha cancelación, de acuerdo con el literal i) del artículo 25 de esta Ley.
- f). Se produzca una quiebra técnica del sistema de seguridad del proveedor del servicio de certificación que afecte a la integridad y confiabilidad del certificado.

En los casos de suspensión temporal, la misma podrá ser levantada una vez desvanecidas las causas que la originaron, en cuyo caso igualmente el proveedor del servicio de certificación está en la obligación de habilitar de inmediato el certificado de firma electrónica.

### **CAPITULO III**

#### **CERTIFICADOS DE FIRMA ELECTRÓNICA**

**Art. 20.- Funciones:** Los certificados de firma electrónica buscarán dar mayor seguridad y confianza a los mensajes de datos y a las transacciones dentro del comercio electrónico, su uso y validez serán regulados por esta ley o por el acuerdo de las partes.

**Art. 21 .- Requisitos de los Certificados de firma electrónica:**

Los certificados deberán contener como mínimo los siguientes requisitos para considerarse válidos:

- a). Identificación del proveedor del certificado.
- b). Datos del domicilio legal del proveedor del certificado.
- c). Código de proveedor del certificado asignado por el respectivo órgano de control.
- d). Los atributos específicos del titular del certificado que permitan su ubicación e identificación, códigos, nombres, domicilio del titular y, adicionalmente, el número de la persona natural o jurídica asignado por el Registro de firmas electrónicas del órgano de control respectivo.
- e). El método de verificación de que el dispositivo de verificación de firma se corresponde con el dispositivo de creación de firma controlado por el titular del certificado
- f). El procedimiento para comprobar la revocación o cancelación de un certificado.
- g). Las fechas de inicio y fin del periodo de validez del certificado.
- h). El identificador del certificado, que deberá ser único, y;

i). La firma electrónica del proveedor del servicio de certificación debidamente acreditado por el órgano de control respectivo.

j). Cualquier limitación que contenga, sea de uso, responsabilidad o montos de transacciones del certificado en caso de tenerlas y de responsabilidad del proveedor de certificaciones.

**Art. 22.- Requisitos adicionales:** Cualquier requisito adicional a los aquí señalados, deberá constar expresamente determinado en la Ley.

**Art. 23 .- Tratados Internacionales:** Aquellos Acuerdos internacionales, bilaterales, multilaterales o comunitarios suscritos por el Estado Ecuatoriano buscarán la unificación de normas para la validez y reconocimiento de los certificados entre los países miembros.

## **CAPITULO VI**

### **PROVEEDORES DE SERVICIOS DE CERTIFICACION**

**Art. 24 .- Control:** El control, supervisión, vigilancia y sanción de los Proveedores de Servicios de Certificación será ejercido por el Superintendente de Telecomunicaciones.

**Art.- 25.- Proveedores de Servicios de Certificación:** Toda persona puede contratar al Proveedor de Servicios de Certificación de firma electrónica que desee, el mismo que deberá estar debidamente acreditado ante el órgano de control respectivo. Los proveedores deberán cumplir los siguientes requisitos:

a). Encontrarse legalmente constituidos.

b). Justificar la confiabilidad y probidad necesarias para ofertar servicios de certificación.

c). Ser entidades con independencia financiera.

d). No haber sido condenados previamente en proceso judicial,

e). Contar con un servicio de suspensión y revocación rápido y seguro.

f). Mantener el personal técnico adecuado con conocimiento especializado en la materia y experiencia para el servicio a prestar

g). Utilizar sistemas técnicamente confiables para los servicios a prestar tanto en el uso de software como de hardware.

h). Mantener sistemas de resguardo y respaldo de la información relativa a los certificados.

i). Mantener una publicación en internet u otros medios determinados en el contrato de suscripción, en la cual conste la información relativa a los procedimientos, reglamentos, prácticas aplicadas a los contratos celebrados con los Usuarios y los certificados suspendidos o cancelados.

j). Estar inscritos y habilitados en el Registro de Servicios de Certificación del órgano de control respectivo.

k). Verificar por los medios establecidos en la ley la identidad y capacidad de actuar de la persona natural o jurídica sobre la cual emiten un certificado.

l). Utilizar herramientas de firma electrónica que estén protegidas contra la modificación de las mismas, de tal forma que no puedan realizar funciones distintas a aquéllas para las que han sido diseñadas. Deben utilizar productos de firma electrónica que bajo estándares internacionales garanticen la seguridad técnica y criptográfica de los procesos de certificación soportados por los productos.

m). Adoptar medidas para evitar la falsificación de certificados, y, en el caso de que el Proveedor de Servicios de Certificación intervenga en la generación de claves criptográficas privadas, garantizar la seguridad y confidencialidad durante el proceso de generación de dichas claves.

n). Mantener recursos financieros suficientes para actuar en conformidad con los requisitos establecidos en la presente ley, especialmente garantizar la responsabilidad por daños y perjuicios.

o). Almacenar toda la información relevante relativa a un certificado por un periodo mínimo de 10 años, especialmente a efectos de prueba en procedimientos judiciales. El almacenamiento podrá ser realizado por medios electrónicos.

p). No almacenar o copiar las claves criptográficas privadas de firma electrónica de la persona a la cual el proveedor del servicio de certificación ofrezca servicios de administración de las claves, a menos que la persona lo solicite expresamente

q). Informar a los consumidores antes de iniciar una relación contractual, por escrito utilizando un lenguaje entendible y un medio duradero de comunicación, acerca de los términos precisos y condiciones para el uso del certificado, incluyendo cualquier limitación sobre responsabilidad, la existencia de una acreditación voluntaria y los procedimientos existentes para resolver cualquier conflicto.

r). Mantener la confidencialidad de la información y proteger la información frente a terceros.

- s). Transferir a un Notario para su archivo confidencial las claves, revocaciones y la documentación que las justifique, en caso de liquidación o cese de las actividades.
- t). Garantizar la integridad, disponibilidad y entrega de la información y documentos a su cargo a fin de que puedan ser usados como medio de prueba.

**Art. 26 . Responsabilidades de los proveedores de servicios de certificación:**

El proveedor de servicio de certificación será responsable por:

- a. Adoptar las medidas necesarias para determinar la identidad del titular de la firma y la exactitud de sus certificaciones.
- b. La validez, vigencia y legalidad del certificado emitido.
- c. Certificar que la información contenida en el certificado era exacta en el momento en el que fue emitido, a no ser que el proveedor del servicio de certificación hubiera establecido otra cosa en el certificado,
- d. Asegurar que el titular del certificado tenía, en el momento de creación del mismo, el instrumento de generación de firma correspondiente al instrumento de verificación del mismo reseñado o identificado en el certificado, y
- e. Asegurar que en los casos en los que el proveedor del servicio de certificación generara los instrumentos de creación y comprobación de firma, ambos instrumentos funcionaran juntos de una forma complementaria.
- f. Almacenar y garantizar la seguridad de las claves criptográficas de firmas electrónicas que se le solicitara expresamente.
- g. La Correspondencia de funcionamiento entre la clave pública y privada de acuerdo con el certificado expedido.
- h. Proporcionar a los titulares de firmas un medio para dar aviso de que una firma electrónica tiene riesgo de uso indebido, en cuyo caso el titular deberá solicitar la suspensión de la firma electrónica.
- i. Mantener un listado de las firmas suspendidas, canceladas o revocadas.

Todo Proveedor de Servicios de Certificación será responsable del incumplimiento de sus obligaciones. En todos los casos, la responsabilidad del proveedor del servicio de certificación deberá constar claramente establecida tanto en el contrato con los usuarios como en el certificado de firma electrónica concedido y su omisión no será eximente de responsabilidad.

**Art. 27 .- Los Proveedores de Servicios de Certificación en el archivo, uso y manejo de datos obtenidos en función de su trabajo, garantizarán:**

- a). Privacidad, protección y confidencialidad de la información y datos que manejen,
- b). Obtener información únicamente con el consentimiento y voluntad de la persona relacionada con dicha información.
- c). La no divulgación de la información obtenida por cualquier medio,
- d). La protección frente a terceros de la información y datos obtenidos por cualquier medio, y
- e). Otros requisitos establecidos en las leyes y reglamentos que regulen la materia.

Los Proveedores de Servicios de Certificación bajo pena de cancelación de su calidad de tales, y otras consecuencias legales establecidas en la presente ley recopilarán datos personales o particulares únicamente de los propios sujetos o sus representantes legalmente acreditados y sólo en la medida que sean necesarios para la emisión de un certificado. Los datos no pueden ser recopilados o procesados para fines distintos o distribuidos sin el consentimiento expreso del titular de los mismos.

En caso de que una persona natural o jurídica recopile información por medios fraudulentos, cedere bajo cualquier modalidad datos fuera de los casos permitidos por la Ley y en general vulnerase el derecho a la confidencialidad de los individuos o instituciones, se prohibirá su actividad y funcionamiento y se comunicará del efecto al Superintendente de Compañías para que proceda a su inmediata liquidación y será reprimido con multa de 500 a 2.500 UVCs y prisión de dos meses a dos años sin perjuicio de la acción de daños y perjuicios.

## **TITULO II**

### **CAPITULO I**

#### **CONTRATOS**

**Art. 28 .- Formación de un contrato electrónico:** La elaboración, envío y aceptación de un contrato podrá ser efectuada mediante mensajes de datos. Estos mensajes de datos gozarán de

completa validez y fuerza jurídica, sea que se trate de una oferta, la aceptación de la misma o cualquier otra forma que genere obligaciones entre las partes.

**Art. 29.- Contratos de adhesión:** En los contratos en los cuales las condiciones se encuentren preestablecidas, bastará que el suscriptor cumpla con las instrucciones de adhesión establecidas en el mensaje de datos para crear obligaciones entre emisor y suscriptor.

**Art. 30 .- Perfeccionamiento de los contratos electrónicos:** Los contratos concluidos electrónicamente se entenderán perfeccionados cuando la declaración de voluntad del aceptante llegue a conocimiento del Oferente.

Se entenderá como el lugar de perfeccionamiento del contrato el que acordaren las partes, en caso de no fijarlo, será el lugar de envío o recepción del mensaje de datos.

**Art. 31 .- Aceptación de un contrato electrónico:** Si alguna de las partes solicitare que previa a la aceptación legal de un documento electrónico, se deba confirmar su recepción y conformidad, se entenderá que el documento electrónico no surtirá sus efectos legales mientras no se cumpla dicho requisito.

**Art. 32.- Recepción y Aceptación:** En caso de que cualquiera de las partes solicitare confirmación de recepción o aceptación de un documento electrónico, sin especificar el medio, se considerará haberse emitido dicha confirmación cuando:

- a). Expresa.- Se hubiere enviado un mensaje por cualquier medio electrónico haciendo referencia a dicho documento o su conformidad con el mismo.
- b). Tácita.- Se hubiere enviado un mensaje electrónico por cualquier medio, en el cual se entienda por el sentido del mismo, que se recibió dicho mensaje o su conformidad con el contenido.
- c). La confirmación de la recepción de un mensaje, indicando que éste ha cumplido los requisitos técnicamente reconocidos o acordados, no implicará presunción de aceptación de su contenido.

**Art. 33.- Tiempo de validez:** A Criterio del Emisor, el mensaje de datos enviado y condicionado a confirmación de recepción o aceptación, podrá tener un tiempo de validez durante el cual generará obligaciones para las partes.

En caso de no señalarse tiempo de validez, éste será de cinco días hábiles, luego de los cuales se deberá ratificar las condiciones establecidas y aceptadas por las partes para proceder a la ejecución del contrato.

**Art. 34 .- Procedencia e identidad de un mensaje datos:** Se entenderá que un mensaje de datos proviene de quién lo envía y autorizará a quién lo recibe a actuar conforme al contenido de dicho documento, cuando de la verificación acordada entre las partes, exista concordancia entre la identificación del envío y la recepción del mensaje de datos, sea por si mismo, por interpuesta persona o por cualquier medio u orden.

**Art. 35 .- Excepciones:** Lo señalado en el artículo anterior se entiende que no surte efectos cuando:

- a). Se hubiere dado aviso que el mensaje de datos no provenía de quién lo suscribe electrónicamente. Este aviso se lo deberá hacer antes de que quién lo recibe actúe conforme a dicho mensaje. En caso contrario deberá justificar plenamente que el mensaje no se inició por orden suya o que el documento fue alterado.
- b). Si el Destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o si hubiera hecho caso omiso de su resultado.

**Art. 36 .- Envío y recepción de un mensaje de datos:** Salvo pacto en contrario, se presumirán los siguientes:

1.- Tiempo:

- a). Se tendrá como expedido cuando entre en un sistema de información que no esté bajo control del Emisor, de quién éste autorizara o del medio programado para el efecto.
- b). Se considerará momento de recepción cuando ingrese al sistema de información señalado por el Destinatario. En caso enviarse a otro sistema de información o de no haber señalado un lugar preciso de recepción, el momento de recepción será cuando el Destinatario recupere el mensaje de datos en cualquier sistema de información.

2.- Lugar: Se considerará como lugar de envío y recepción, el domicilio que conste en el certificado de firma electrónica del Emisor y del Destinatario. Si por errores en el certificado, no se pudiere establecer el domicilio, será el lugar de trabajo o donde desarrollen el giro principal de sus negocios o del negocio relacionado con el mensaje de datos.

**Art. 37 .- Duplicación del mensaje de datos:** Cada mensaje de datos se presume diferente, de acuerdo al negocio entre las partes. En caso de duda el Destinatario deberá solicitar la confirmación del nuevo mensaje. Todo mensaje lleva implícita la obligación de verificar técnicamente la autenticidad del mismo.

**Art. 38 .- Modificación contractual:** Las disposiciones señaladas en este capítulo podrán ser modificadas por el acuerdo de las partes.

## **CAPITULO II**

### **DE LOS DERECHOS DEL USUARIO DE CONSUMO**

**Art. 39.- Protección al usuario:** Se garantizan los derechos de los usuarios de servicios de certificación y de quienes actúen intercambiando mensajes de datos, o efectuando transacciones de cualquier tipo relacionadas con el acceso a Internet, Comercio Electrónico, otros medios de comunicación y Tecnologías de Información.

**Art. 40 .- Información:** El Oferente en internet deberá informar al usuario, en forma objetiva, veraz y en detalle lo que se está adquiriendo, para que sirva y como utilizarlo.

**Art. 41.- Contratos de consumo:** Luego de celebrados estos contratos, el Usuario o adquirente tiene el derecho de desistir del contrato veinte y cuatro horas después de suscrito el mismo. Dentro de éste término el Usuario será responsable por los gastos que hubiere ocasionado al Oferente por ese contrato. En caso de no notificar dicho desistimiento dentro del término señalado el Usuario será responsable del pago o de los daños y perjuicios que le cause al Oferente.

**Art. 42.- Privacidad:** Como privacidad del usuario se entiende el derecho a la intimidad y el derecho a no recibir información o mensajes no solicitados. Para el envío o recepción de mensajes o información directamente o mediante cadenas, el usuario deberá haber suscrito una autorización expresa al iniciador o emisor del mensaje de datos.

El usuario podrá solicitar en cualquier momento su exclusión de cadenas de mensajes o de bases de datos en las cuales conste inscrito. En caso de violarse el derecho a la privacidad, el usuario podrá iniciar las acciones que le concede la Ley y el iniciador o emisor del mensaje de datos será condenado al pago de la respectiva indemnización por daños y perjuicios.

**Art. 43 .- Prohibición de oferta:** Una vez rechazado una oferta electrónica por parte del Destinatario del mensaje, el Oferente no podrá seguir enviando mensajes si hay oposición para recibirlos. En caso de incumplimiento, el Oferente será condenado a cumplir con una indemnización por daños y perjuicios de acuerdo a lo determinado por la autoridad competente.

## **CAPITULO III**

### **DOCUMENTOS PUBLICOS**

#### **Artículo.- 44 .- Documentos públicos electrónicos.-**

a). Los documentos escritos que se transformen en documentos electrónicos en presencia de un Notario se considerarán copias electrónicas auténticas. Lo mismo sucederá a la inversa.

c). La afirmación hecha por un Notario o autoridad competente acerca de que la firma electrónica ha sido puesta o reconocida en presencia del mismo por su titular será considerada una legitimación de la firma electrónica, la misma que deberá cumplir con los requisitos técnicos y legales establecidos

d). Cuando una declaración de voluntad sea transmitida telemáticamente por un Notario o autoridad competente, la actuación de éste acreditará la realización de la comunicación del hecho, su lugar y fecha.

e). Los Fedatarios Públicos deberán cumplir los mismos requisitos que los Proveedores de Servicios de Certificación para dar fe sobre mensajes de datos.

f). Los documentos electrónicos expedidos por Notario o autoridad competente y firmados electrónicamente por ellos tienen los mismos efectos jurídicos que los documentos escritos de su misma clase.

**Artículo.- 45 .- Delegación de firmas:** La delegación de firmas electrónicas se regirá de acuerdo a lo dispuesto en los siguientes literales:

a). La solicitud de una firma electrónica ante los proveedores acreditados de servicios de certificación no podrá realizarse a través de representante voluntario.

b). La solicitud de una firma electrónica ante los proveedores acreditados de servicios de certificación, para usarla en nombre de otra persona por el apoderado, tendrá que ser realizada por el poderdante y el apoderado.

c). Para la delegación de firmas se cumplirá con los demás requisitos exigidos por la Ley.



### TITULO III CAPITULO I

**Art. 46 .- Jurisdicción:** Las partes libremente pueden acordar los términos y condiciones bajo los cuales establecen relaciones electrónicas.

En caso de no acordar el lugar de resolución de controversias, se aplicarán las normas señaladas en la Sección Segunda del Título Primero, del libro Primero del Código de Procedimiento Civil.

Para la identificación de la procedencia de un mensaje se utilizarán los medios tecnológicos disponibles y se aplicarán las normas señaladas en esta Ley y en las Leyes relacionadas con el proceso judicial.

**Art. 47 .- Notificaciones:** En las controversias derivadas de la aplicación de esta Ley, también se deberá citar y notificar al demandado a su dirección de correo electrónico, con todas las providencias que se dictaren en el transcurso de la litis.

### CAPITULO II

**Art. 48 .- Medio de prueba:** El mensaje de datos, cualquiera sea su procedencia o generación, será considerado medio de prueba con todos los efectos legales que tienen los principios probatorios determinados en las Leyes que regulan la materia.

**Art. 49.- Presunción:** Existe presunción legal sobre un documento electrónico presentado como prueba, siempre y cuando la firma electrónica hubiere sido certificada por un Proveedor de Servicios de Certificación que cumpla con los requisitos señalados en la Ley. En este caso se presumirá que:

- a). Los datos no han sido alterados desde su firma.
- b). La firma electrónica pertenece al suscribiente.
- c). Fue añadida al documento con la intención de manifestar su voluntad.

En caso de que alguna de las partes niegue la validez del contrato deberá justificar conforme a la Ley que el contrato electrónico adolece de uno o varios vicios que lo invalidan. Entre otros pueden ser:

- a). Que el procedimiento de seguridad, incluyendo los medios, utilizados para verificar la firma no pueden ser reconocidos técnicamente como seguros.
- b). Insuficiencia del procedimiento empleado.
- c). Adulteración técnica.
- d). Los demás establecidos en la Ley.

**Artículo.- 50 .- Pruebas:** Para la validez de la prueba se deberán respetar los principios procesales consagrados en la Constitución y en la Ley. Las partes deberán seguir las siguientes normas para el uso de la prueba.

- a). Siempre que se presente un documento firmado electrónicamente ante un Juzgado o Tribunal se deberá presentar junto al soporte informático la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura en claro y la verificación de la firma.
- b). Cuando la parte que se oponga a un documento firmado electrónicamente no reconozca su firma, la parte que haya presentado el documento deberá designar al proveedor del servicio de certificación en el que se encuentre el certificado, y solicitar del Juzgado que reclame dicho certificado y los documentos en los que se basó la solicitud del firmante.
- c). La información obtenida por medios electrónicos o por certificaciones de los proveedores o autoridades competentes, formarán parte del expediente al que se incorporen.
- d). El telegrama, telex, fax, facsímil en un documento escrito, deberá guardar su integridad, haber sido conservado conforme a lo prescrito en esta ley, cumplir los requisitos que les fueran aplicables y ser presentados cuando así lo solicite la Autoridad Competente.

**Art. 51 .- Valoración de la prueba:** La prueba será analizada bajo los principios determinados en la Ley y de acuerdo con la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió. Estos parámetros no son excluyentes y se ajustarán en base a la técnica y la tecnología.

Para la valoración de las pruebas, el Juez, Arbitro o Mediador competente que juzgue el caso deberá designar los peritos que considere necesarios para el análisis, perfecto conocimiento técnico e interpretación de las pruebas presentadas.

**Art. 52.- Infracciones:** Para el juzgamiento de las infracciones cometidas en el Comercio Electrónico, regirán las normas del Código Penal, la Ley de Propiedad Intelectual y demás leyes pertinentes.

La violación a la confidencialidad será sancionada en base a lo dispuesto por el capítulo V, del título II, del libro Segundo del Código Penal y a las normas de la Ley de Propiedad Intelectual. Cualquier alteración o falsificación de un mensaje de datos, será sancionado de acuerdo a lo dispuesto en el Capítulo III, del Título IV, del Libro Segundo del Código Penal.

**Art. 53 .- Artículo Final:** Esta ley entrará en vigencia a partir de su publicación en el Registro Oficial.

---

[Principio del documento](#)