REPORTE TEMÁTICO N.° 176/2024-2025

FIRMA DIGITAL
Legislación comparada

Lima, 27 de mayo de 2025

Plaza Bolívar, Av. Abancay s/n – Lima, Perú
Central Telefónica: 311-7777
www.congreso.gob.pe

PRESENTACIÓN

El Departamento de Investigación Parlamentaria, a través del Área de Servicios de Investigación y Seguimiento Presupuestal, ha elaborado el Reporte Temático N.º 176/2024-2025-ASISP/DIP, referido a la firma digital en la legislación comparada.

Para la elaboración se ha consultado la información disponible en fuentes oficiales sobre la materia; cuyas referencias se consignan en el documento.

Esperamos poder brindar información que contribuya a la labor parlamentaria.

1. CONSIDERACIONES GENERALES

La gobernanza digital "es la articulación y concreción de políticas de interés público con los diversos actores involucrados (Estado, Sociedad Civil y Sector Privado), con la finalidad de alcanzar competencias y cooperación para crear valor público y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales[1]". Busca:

- Establecer las estructuras y procesos que aseguren que la estrategia de gobierno digital se alinea con los objetivos estratégicos de gobierno
- Articular y concretar políticas de interés público entre actores involucrados para crear valor público
- Que los riesgos y oportunidades sean adecuadamente administrados
- Optimizar los recursos disponibles a través del uso racional de las tecnologías digitales[2]

En dicho contexto, el gobierno digital debe entenderse como "el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos con el fin de crear valor público (…) un ecosistema de gobierno digital constituido por los actores estatales, organizaciones no gubernamentales, empresas, asociaciones de ciudadanos y personas encargadas de la producción y acceso a los datos, servicios y contenidos a través de interacciones con el gobierno[3]". Sus componentes estructurales son; (i) la identidad digital; (ii) el portal digital del Estado; (iii) la interoperabilidad gubernamental; (iv) la carpeta digital ciudadana; (v) la casilla digital del ciudadano; y (vi) la ciberseguridad.

1.1 Firma digital

La identidad digital es el uso de tecnología para asegurar y probar identidad[4] (la representación de la persona en el entorno digital); así como para acceder a determinados recursos de información o físicos, y realizar transacciones a través de Internet o redes privadas[5]. Y la herramienta por medio de la cual se valida dicha identidad y garantiza la autenticidad de los documentos digitales es la firma digital.

La *Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública*[6], de la Secretaría de Gobierno y Transformación Digita, de la Presidencia del Consejo de Ministros, indica que la Plataforma FIRMA PERÚ permite la creación y validación de firmas digitales dentro del marco de la *Infraestructura Oficial de Firma Electrónica*, para la provisión de los servicios digitales prestados por las entidades de la Administración Pública. Y presenta las siguientes definiciones:

> **a) Firma digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al

[1] NASER, Alejandra. Gobernanza digital e interoperabilidad gubernamental. Una guía para su implementación. CEPAL, 2021.p. 14. https://www.cepal.org/es/publicaciones/47018-gobernanza-digital-interoperabilidad-gubernamental-guia-su-implementacion
[2] https://biblioguias.cepal.org/gobierno-digital/concepto-gobernanza
[3] NASER, Alejandra, Op. cit, p. 15.
[4] FATF GUIDANCE ON DIGITAL IDENTITY IN BRIEF, 2020, https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/Digital-ID-in-brief.pdf
[5] https://biblioguias.cepal.org/gobierno-digital/identidad-digital
[6] https://cdn.www.gob.pe/uploads/document/file/3690615/Gu%C3%ADa%20para%20el%20uso%20e%20integraci%C3%B3n%20de%20la%20Plataforma%20Nacional%20de%20Firma%20Digital%20en%20la%20Administraci%C3%B3n%20P%C3%BAblica.pdf?v=1664204905

signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil.

b) Firma digital de agente automatizado: Es aquella firma digital generada sin intervención humana utilizando una llave privada asociada a un certificado digital de agente automatizado emitido en el marco de la IOFE.

c) Certificado digital: Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de llaves con una persona natural o jurídica. El ciclo de vida de un certificado digital comprende: la emisión, la cancelación, y la renovación.

d) Sello de tiempo: Es el dato que consigna la fecha y hora cierta para evidenciar que un dato u objeto digital ha existido en un momento determinado en el tiempo, y que no ha sido alterado desde entonces.

e) Documento electrónico: Es la unidad básica estructurada de información, es susceptible de ser clasificada, transmitida, procesada o conservada utilizando medios electrónicos, sistemas de información o similares. Contiene información de cualquier naturaleza, es registrado en un soporte electrónico o digital, en formato abierto y de aceptación general, a fin de facilitar su recuperación y conservación en el largo plazo.

f) Flujo de firma: Es la secuencia ordenada de operaciones de creación de firma digital, aplicadas a un documento electrónico, y efectuadas por múltiples firmantes.

g) Flujo documental: Es la secuencia de pasos o recorrido de un documento electrónico a lo largo de su tramitación en una entidad.

Firma Perú cuenta con servicios de:

Para la ciudadanía en general:

- Firmador de documentos: aplicación para PC que te permite generar tu firma digital.
- Validador de firmas digitales: servicio digital que te permite validar firmas digitales.

Para las entidades públicas:

- Firmador: componente que se integra a las aplicaciones web y de PC institucionales para generar firmas digitales a nombre de personas jurídicas o naturales (con DNIe).
- Validador: aplicación tipo servicio web para los servicios de las entidades públicas para la validación desatendida de firma digital.
- Agente: aplicación tipo servicio web para los servicios de las entidades públicas para la generación desatendida de firma digital.

CUADRO 1
LEGISLACIÓN COMPARADA

País	Requisitos para la validez de una firma digital	Firma digital o electrónica como firma manuscrita para efectos legales	
		Digital	Electrónica
Argentina	➢ Haber sido creada durante el período de vigencia del certificado digital válido del firmante. ➢ Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en el certificado. ➢ Que dicho certificado haya sido emitido o reconocido por un certificador licenciado.	✓	
Chile	(Firma electrónica) ➢ Un código de identificación único del certificado. ➢ Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada. ➢ Los datos de la identidad del titular, entre los cuales deben incluir su nombre, dirección de correo electrónico y su rol único tributario. ➢ Su plazo de vigencia.		✓
Colombia	➢ Es única a la persona que la usa. ➢ Es susceptible de ser verificada. ➢ Está bajo el control exclusivo de la persona que la usa. ➢ Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada. ➢ Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.	✓	✓
Costa Rica	➢ Utilizar al menos un proceso de verificación y registro presencial (cara a cara) de sus suscriptores. ➢ Guardar copia de la documentación utilizada para verificar la identidad de la persona. ➢ Registrar de forma biométrica (fotografía, huellas digitales, etc.) al suscriptor a quién le será emitido un certificado. ➢ Requerir el uso de módulos seguros de creación de firma, con certificación de seguridad que se indique conforme a las normas internacionales y a las Políticas establecidas por la DCFD. ➢ Establecer un contrato de suscripción detallando el nivel de servicio que ofrece y los deberes y responsabilidades de las partes.	✓	
Ecuador	➢ Ser individual y estar vinculada exclusivamente a su titular. ➢ Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos. ➢ Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.	✓	

	➢ Que, al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, ➢ Que la firma sea controlada por la persona a quien pertenece.		
El Salvador	➢ Vincular al firmante, de manera única. ➢ Estar basado en un certificado electrónico emitido por un proveedor de servicios de certificación. ➢ Permitir la verificación inequívoca de la autoría e identidad del signatario. ➢ Haber sido creada utilizando medios de creación y verificación confiable y seguro, bajo el control exclusivo del signatario. ➢ Estar vinculada con la información de modo tal que cualquier modificación ulterior de los mismos sea detectable. ➢ Los certificados electrónicos emitidos para firma electrónica certificada cumplirán los requisitos del artículo 58, de la presente ley.	✓	
Perú	➢ Datos que identifiquen indubitablemente al suscriptor. ➢ Datos que identifiquen a la Entidad de Certificación. ➢ La clave pública. ➢ La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos. ➢ Número de serie del certificado. ➢ Vigencia del certificado. ➢ Firma digital de la Entidad de Certificación.	✓	

Fuente: Normas de los países señalados
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP).

CUADRO 2
FIRMA DIGITAL

País	Norma	Artículo
Argentina	Ley 25.506 Ley de Firma Digital	CAPITULO I Consideraciones generales **ARTICULO 1º** — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley. **ARTICULO 2º** — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes. **ARTICULO 3º** — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia. **ARTICULO 4º** — Exclusiones. Las disposiciones de esta ley no son aplicables: a) A las disposiciones por causa de muerte; b) A los actos jurídicos del derecho de familia; c) A los actos personalísimos en general; d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes. **ARTICULO 5º** — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

		ARTICULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura. **ARTICULO 7º** — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. **ARTICULO 8º** — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma. **ARTICULO 9º** — Validez. Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado. **ARTICULO 10.** — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente. **ARTICULO 11.** — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación. **ARTICULO 12.** — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción. CAPITULO II De los certificados digitales **ARTICULO 13.** — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular. **ARTICULO 14.** — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben: a) Ser emitidos por un certificador licenciado por el ente licenciante;

		b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan: 1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única; 2. Ser susceptible de verificación respecto de su estado de revocación; 3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado; 4. Contemplar la información necesaria para la verificación de la firma; 5. Identificar la política de certificación bajo la cual fue emitido. **ARTICULO 15.** — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado. La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió. La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales. **ARTICULO 16.** — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando: a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.
	Decreto 2628/2002 Reglamentación de la Ley 25.506.	CAPITULO I CONSIDERACIONES GENERALES **Artículo 1°** — Objeto. La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica. En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad: a) Firma electrónica, b) Firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación, c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,

		d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos: 1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero. 2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación. **Art. 2°** — Validez de los certificados, digitales emitidos por certificadores no licenciados. Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica. **Art. 3°** — Certificados digitales emitidos por certificadores licenciados. Los certificados digitales contemplados, en el artículo 13 de la Ley N° 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada. CAPITULO II DE LA AUTORIDAD DE APLICACIÓN **Art. 4°** — Normas técnicas. Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506. **Art. 5°** — Conservación. El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas. Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia. **Art. 6°** — Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer: a) Los estándares tecnológicos y de seguridadaplicables en consonancia con estándares internacionales. b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente. c) Las condiciones mínimas de emisión de certificadosdigitales. d) Los casos en los cuales deben revocarse los certificados digitales. e) Los datos considerados públicos contenidos en los certificados digitales.

		f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados. g) La información que los certificadores licenciados deberán publicar por internet. h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial. i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad . j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías. k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias. l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales. m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital. n) El procedimiento de instrucción sumarial y lagradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad. o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros. p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación digital para las entidades y jurisdicciones de la Administración Pública Nacional. q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado. r) Los niveles de licenciamiento. s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos. t) Exigir las garantías y seguros necesarios para prestar el servicio previsto. u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley. CAPITULO III

		DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL **Art. 7°** — Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506. **Art. 8°** — Integración. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos: a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia. b) Antecedentes académicos y/o profesionales o laborales en la materia. **Art. 9°** — Ejercicio de funciones. El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem. **Art. 10.** — Consulta Pública. La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se está tratandoa los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario. CAPITULO IV DEL ENTE ADMINISTRADOR DE FIRMA DIGITAL **Art. 11.** — Ente Administrador de Firma Digital. Créase el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios. **Art. 12.** — Autoridades del Ente Administrador de Firma Digital. El Ente Administrador de Firma Digital será conducido por un Directorio integrado por TRES (3) miembros, designados por el JEFE DE GABINETE DE MINISTROS, previo concurso. Hasta tanto, sea realizado el concurso el JEFE DE GABINETE DE MINISTROS designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS.

		Art. 13. — Funciones del Ente Administrador. Son funciones del Ente Administrador: a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro. b) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados. c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento . d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento. e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados. f) Solicitar los informes de auditoría en los casos que correspondiere. g) Realizar inspecciones a los certificadores licenciados por sí o por terceros. h) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación. i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley N° 25.506, el presente decreto y las normas complementarias. j) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de internet y certificados digitales de los certificadores licenciados. k) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, los números telefónicos, direcciones de internet y certificados digitales de los certificadores cuyas licencias han sido revocadas. l) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, el domicilio, números telefónicos, direcciones de internet y certificados digitales del Ente Administrador.

		m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento. n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley N° 25.506 y en el artículo 16 de la presente reglamentación. o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador. p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios. **Art. 14.** — Obligaciones del Ente Administrador. El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe: a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes. b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones; c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas. d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados. e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes. f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados. **Art. 15.** — Organización del Ente Administrador. Dentro del plazo de SESENTA (60) días corridos de la fecha de constitución del Directorio, el ENTE ADMINISTRADOR DE FIRMA DIGITAL elevará para su consideración al JEFE DE GABINETE DE MINISTROS la propuesta de su estructura organizativa y de su reglamento de funcionamiento. **Art. 16.** — Recursos del Ente Administrador. El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con: a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios: 1.- Servicios de certificación digital,

		2.- Servicios de certificación digital de fecha y hora , 3.- Servicios de almacenamiento seguro de documentos electrónicos, 4.- Servicios prestados por autoridades de registro, 5. - Servicios prestados por terceras partes confiables, 6. - Servicios de certificación de documentos electrónicos firmados digitalmente, 7.- Otros servicios o actividades relacionados a la firma digital. b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales. c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital. d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros. e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba. f) El producido de multas. g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional. h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables. **Art. 17.** — Financiamiento del Ente Administrador. Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones . Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS. (…).
Chile	Ley 19799 Sobre documentos	TITULO I Disposiciones Generales

	electrónicos, firma electrónica y servicios de certificación de dicha firma	**Artículo 1º.-** La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso. Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel. Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados. **Artículo 2º.-** Para los efectos de esta ley se entenderá por: a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares; b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica; c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas; d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior; e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción; f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor; g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica. i). Fecha electrónica: 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. **Artículo 3º.-** Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito. Lo dispuesto en el inciso anterior no será aplicable a los actos o contratos otorgados o celebrados en los casos siguientes: a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y c) Aquellos relativos al derecho de familia.

		La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en los artículos siguientes. **Artículo 4º.-** Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada. **Artículo 5º.-** Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes: 1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y 2. Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos con firma electrónica avanzada, tendrán el mismo valor probatorio señalado en el número anterior. Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado. En el caso de documentos electrónicos que posean la calidad de instrumento privado y estén suscritos mediante firma electrónica, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales. TITULO II Uso de Firmas Electrónicas por los Órganos del Estado **Artículo 6º.-** Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas. Lo dispuesto en este Título no se aplicará a las empresas públicas creadas por ley, las que se regirán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares. **Artículo 7º.-** Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel. Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.

		Artículo 8º.- Las personas podrán relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos. Los órganos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias. **Artículo 9º.-** La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos del Estado se realizará por los respectivos ministros de fe. Si éste no se encontrare establecido en la ley, el reglamento a que se refiere el artículo 10 indicará la forma en que se designará un funcionario para estos efectos. Dicha certificación deberá contener, además de las menciones que corresponda, la fecha y hora de la emisión del documento. Los efectos probatorios de la certificación practicada por el ministro de fe competente serán equivalentes a los de la certificación realizada por un prestador acreditado de servicios de certificación. Sin perjuicio de lo dispuesto en el inciso primero, los órganos del Estado podrán contratar los servicios de certificación de firmas electrónicas con entidades certificadoras acreditadas, si ello resultare más conveniente, técnica o económicamente, en las condiciones que señale el respectivo reglamento. **Artículo 10.-** Los reglamentos aplicables a los correspondientes órganos del Estado regularán la forma cómo se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este Título. (…). TITULO IV De los Certificados de Firma Electrónica **Artículo 15.-** Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones: a) Un código de identificación único del certificado; b) Identificación del prestador de servicio de Ley 19799 Biblioteca del Congreso Nacional de Chile - www.leychile.cl - documento generado el 14-Dic-2020 página 7 de 12 certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada; c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y d) Su plazo de vigencia.

		Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente. **Artículo 16.-** Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos: 1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión; 2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias: a) A solicitud del titular del certificado; b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso; c) Por resolución judicial ejecutoriada, o d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24; 3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12, y 4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12. La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador. El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.
	Decreto 181 Aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma	**Artículo 1º.** Los documentos electrónicos, la certificación y uso de la firma electrónica por las personas naturales y jurídicas de derecho privado y la administración del Estado, la prestación de los servicios de certificación, la acreditación de los certificadores, y los derechos y obligaciones de los usuarios se regirá por lo dispuesto en la ley Nº 19.799, el presente Reglamento y las normas técnicas que se dicten al efecto. (…). **Artículo 7º.** El prestador de servicios de certificación deberá mantener un registro de certificados de acceso público, en el que se garantice la disponibilidad de la información contenida en él de manera regular y continua.

		A dicho registro se podrá acceder por medios electrónicos y en él deberán constar los certificados emitidos por el certificador, indicando si los mismos se encuentran vigentes, revocados, suspendidos, traspasados de otro prestador de servicios de certificación u homologados. (…). **De los Certificados de Firma Electrónica** **Artículo 28.** El certificado de firma electrónica es la certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de firma electrónica. Los certificados de firma electrónica deben contener, al menos, las siguientes menciones: a. Un código de identificación único del certificado. b. Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada. c. Los datos de la identidad del titular, entre los cuales deben incluir su nombre, dirección de correo electrónico y su rol único tributario. d. Su plazo de vigencia. **Artículo 29.** Los prestadores de servicios de certificación deberán introducir en los certificados de firma electrónica que emitan, las menciones señaladas en el artículo 15 de la Ley, de acuerdo con las normas fijadas por este Reglamento para el desarrollo de la actividad. Los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado, no deberán dificultar o impedir la lectura de las menciones señaladas en el inciso anterior ni su reconocimiento por terceros. **Artículo 30.** Tratándose de un certificado de firma electrónica avanzada, deberá el prestador de servicios de certificación comprobar fehacientemente la identidad del solicitante antes de la emisión del mismo, de conformidad con las normas técnicas. Dicha comprobación la hará el prestador de servicios de certificación, ante sí o ante notario u oficial del Registro Civil, requiriendo la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica. **Artículo 31**. Los datos de creación de firma, cuando sean generados por el prestador de servicios de certificación, deben ser entregados al usuario o titular del certificado de manera de garantizar la recepción de los mismos en forma personal. Queda prohibido al prestador de servicios de certificación mantener copia de los datos de creación de firma electrónica una vez que éstos hayan sido entregados a su titular, momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

		Artículo 32. El certificado de firma electrónica podrá ser usado por su titular de conformidad con las operaciones que han sido autorizadas a realizar en las prácticas de certificación del prestador de servicios de certificación con quien se ha contratado. El certificado de firma electrónica avanzada deberá permitir a quien lo reciba verificar, en forma directa o mediante consulta electrónica, que ha sido emitido por un prestador acreditado de servicios de certificación, con la finalidad de comprobar la validez del mismo. **Artículo 33.** Procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias: a. Solicitud del titular del certificado. b. Decisión del prestador de servicios de certificación en virtud de razones técnicas. El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular. La suspensión del certificado terminará por cualquiera de las siguientes causas: a. Por la decisión del prestador de servicios de certificación de revocar el certificado, en los casos previstos en la Ley. b. Por la decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron. c. Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste. **Artículo 34.** Los certificados de firma electrónica quedarán sin efecto por la revocación practicada por el prestador de servicios de certificación. La revocación tendrá lugar cuando el prestador de servicios de certificación constate alguna de las siguientes circunstancias: a) Solicitud del titular del certificado. b) Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso. c) Resolución judicial ejecutoriada. d) Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.

		e) Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador. f) Que el titular del certificado no ha actualizado sus datos al cambiar éstos. g) Las demás causas que convengan el prestador de servicios de certificación con el titular del certificado. El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de éste conforme a los usos que le son propios e impide el uso legítimo del mismo. **Artículo 35.** Los prestadores acreditados de servicios de certificación podrán homologar los certificados de firma electrónica avanzada emitidos por certificadores no establecidos en Chile, bajo su responsabilidad. Para ello el prestador acreditado de servicios de certificación deberá demostrar a la Entidad Acreditadora que los certificados por ella homologados han sido emitidos por un prestador de servicios de certificación no establecido en Chile que cumple con normas técnicas equivalentes a las aprobadas de acuerdo al artículo 5º para el desarrollo de la actividad. Una vez practicada la homologación de un certificado o de un grupo de certificados de firma electrónica avanzada el prestador acreditado de servicios de certificación deberá, dentro del plazo de tercero día, comunicar tal situación a la Entidad Acreditadora y se deberá publicar, inmediatamente, en el registro de acceso público señalado en el artículo 7 de este Reglamento. Las prácticas de homologación deberán estar declaradas en las Prácticas de Certificación. **Artículo 36.** La revocación de un certificado de firma electrónica podrá producirse de oficio o a petición de su titular por la concurrencia de algunas de las causales previstas en la Ley o en este Reglamento. La solicitud de suspensión o revocación, según corresponda, se podrá dirigir al prestador de servicios de certificación en cualquiera de las formas que prevean sus prácticas de certificación. La suspensión o revocación del certificado deberá ser comunicada inmediatamente a su titular, sin perjuicio que deba publicarse en el registro de acceso público que señala el artículo 7 de este Reglamento. Tratándose de la suspensión por razones técnicas o revocación del certificado de firma electrónica por las causales de las letras d), e) o f) del artículo 34, dicha decisión deberá ser comunicada al titular con anterioridad a su puesta en práctica, indicando la causa que la provoca y el momento en que se hará efectiva. El término de la vigencia del certificado será oponible a terceros desde el momento de la publicación de ésta en el registro de acceso público que señala el artículo 7 de este Reglamento.
Colombia	Ley 527 de 1999 (agosto 18) "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de	PARTE I PARTE GENERAL CAPÍTULO II APLICACIÓN DE LOS REQUISITOS JURÍDICOS DE LOS MENSAJES DE DATOS (…). **ARTÍCULO 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:

	datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”	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. PARTE III FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACION CAPÍTULO I FIRMAS DIGITALES **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. **PARÁGRAFO.** 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. CAPÍTULO II ENTIDADES DE CERTIFICACIÓN **ARTÍCULO 29.** *Características y requerimientos de las entidades de certificación*. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos 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. **ARTÍCULO 30.** *Actividades de las entidades de certificación*. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades: 1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas. 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos. 3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley. 4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas. 5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos. 6. Ofrecer los servicios de archivo y conservación de mensajes de datos. (…) CAPÍTULO III CERTIFICADOS **ARTÍCULO 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. **ARTÍCULO 36**. *Aceptación de un certificado*. Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio. **ARTÍCULO 37.** *Revocación de certificados*. El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos: 1. Por pérdida de la clave privada. 2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido. Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

		Una entidad de certificación revocará un certificado emitido por las siguientes razones: 1. A petición del suscriptor o un tercero en su nombre y representación. 2. Por muerte del suscriptor. 3. Por liquidación del suscriptor en el caso de las personas jurídicas. 4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso. 5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado. 6. Por el cese de actividades de la entidad de certificación, y 7. Por orden judicial o de entidad administrativa competente. **ARTÍCULO 38.** *Término de conservación de los registros*. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular. **CAPÍTULO IV** **SUSCRIPTORES DE FIRMAS DIGITALES** **ARTÍCULO 39.** *Deberes de los suscriptores*. Son deberes de los suscriptores: 1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta. 2. Suministrar la información que requiera la entidad de certificación. 3. Mantener el control de la firma digital. 4. Solicitar oportunamente la revocación de los certificados. **ARTÍCULO 40.** *Responsabilidad de los suscriptores*. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.
	Decreto 2364 de 2012 (noviembre 22) Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se	**Artículo 2°. *Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica.*** Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el artículo 7° de la Ley 527 de 1999. **Artículo 3°. *Cumplimiento del requisito de firma.*** Cuando se 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 tan confiable como apropiada para los fines con los cuales se generó o comunicó ese mensaje. **Artículo 4°. *Confiabilidad de la firma electrónica.*** La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:

	dictan otras disposiciones.	1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante. 2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma. Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona: 1. Demuestre de otra manera que la firma electrónica es confiable; o 2. Aduzca pruebas de que una firma electrónica no es confiable. **Artículo 5°. *Efectos jurídicos de la firma electrónica.*** La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3° de este decreto. **Artículo 6°. *Obligaciones del firmante.*** El firmante debe: 1. Mantener control y custodia sobre los datos de creación de la firma. 2. Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma. 3. Dar aviso oportuno a cualquier persona que posea, haya recibido o vaya a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si: a) El firmante sabe que los datos de creación de la firma han quedado en entredicho; o b) Las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho. **Parágrafo.** Se entiende que los datos de creación del firmante han quedado en entredicho cuando estos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma. **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.

		Parágrafo. La parte que mediante acuerdo provee los métodos de firma electrónica deberá asegurarse de que sus mecanismos son técnicamente seguros y confiables para el propósito de los mismos. A dicha parte le corresponderá probar estos requisitos en caso de que sea necesario. **Artículo 8°. *Criterios para establecer el grado de seguridad de las firmas electrónicas.*** Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta, entre otros, los siguientes factores: 1. El concepto técnico emitido por un perito o un órgano independiente y especializado. 2. La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal.
Costa Rica	Ley 8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos	CAPÍTULO III Firmas digitales **Artículo 8º-Alcance del concepto.** Entiéndese 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. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado. **Artículo 9º-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. **Artículo 10.-Presunción de autoría y responsabilidad.** Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión. No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado. CAPÍTULO IV Certificación digital

		SECCIÓN I Los certificados **Artículo 11.-Alcance.** Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente: a) La vinculación jurídica entre un documento, una firma digital y una persona. b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada. c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras. d) Las demás que establezca esta Ley y su Reglamento. **Artículo 12.-Mecanismos.** Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus intereses. Para tales efectos podrán: a) Utilizar mecanismos de certificación o validación máquina a máquina, persona a persona, programa a programa y sus interrelaciones, incluso sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales que ofrezcan una óptima seguridad. b) Establecer mecanismos de adscripción voluntaria para la emisión, la percepción y el intercambio de documentos electrónicos y firmas asociadas, en función de las competencias, los intereses y el giro comercial. c) De consuno, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas. d) Instaurar, en el caso de dependencias públicas, sistemas de certificación por intermedio de particulares, quienes deberán cumplir los trámites de la Ley de contratación administrativa. e) Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas. f) Ofrecer, en el caso de las empresas públicas cuyo giro lo admita, servicios comerciales de certificación en condiciones de igualdad con las empresas de carácter privado.

		g) Implantar mecanismos de certificación para la tramitación, gestión y conservación de expedientes judiciales y administrativos. **Artículo 13.-Homologación de certificados extranjeros.** Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de los siguientes casos: a) Cuando esté respaldado por un certificador registrado en el país, en virtud de existir una relación de corresponsalía en los términos del artículo 20 de esta Ley. b) Cuando cumpla todos los requisitos enunciados en el artículo 19 de esta Ley y exista un acuerdo recíproco en este sentido entre Costa Rica y el país de origen del certificador extranjero. **Artículo 14.-Suspensión de certificados digitales.** Se podrá suspender un certificado digital en los siguientes casos: a) Por petición del propio usuario a favor de quien se expidió. b) Como medida cautelar, cuando el certificador que lo emitió tenga sospechas fundadas de que el propio usuario haya comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido cualquier otra información relevante, para obtener o renovar el certificado. En este caso, la suspensión podrá ser recurrida ante la Dirección de Certificadores de Firma Digital regulada en la siguiente sección, con aplicación de lo dispuesto en el artículo 148 de la Ley General de la Administración Pública. c) Si contra el usuario se ha dictado auto de apertura a juicio, por delitos en cuya comisión se haya utilizado la firma digital. d) Por orden judicial o de la Dirección de Certificadores de Firma Digital. En este último caso, cuando esta lo determine o cuando el Ente Costarricense de Acreditación (ECA) acredite que el usuario incumple las obligaciones que le imponen esta Ley y su Reglamento. e) Por no cancelar oportunamente el costo del servicio **Artículo 15.-Revocación de certificados digitales.** El certificado digital será revocado en los siguientes supuestos: a) A petición del usuario, en favor de quien se expidió. b) Cuando se confirme que el usuario ha comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o renovar el certificado. c) Por fallecimiento, ausencia legalmente declarada, interdicción o insolvencia del usuario persona física, o por cese de actividades, quiebra o liquidación, en el caso de las personas jurídicas. d) Por orden de la autoridad judicial o cuando recaiga condena firme contra el usuario, por delitos en cuya comisión se haya utilizado la firma digital.

		Artículo 16.-Revocación por el cese de actividades del certificador. El cese de actividades del certificador implicará la revocatoria de todos los certificados que haya expedido, salvo que anteriormente hayan sido traspasados a otro certificador, previo consentimiento del usuario. **Artículo 17.-Conservación de efectos.** La suspensión o revocación de un certificado digital no producirá, por sí sola, la invalidez de los actos o negocios realizados con anterioridad al amparo de dicho certificado. Artículo 23.-**Dirección.** La Dirección de Certificadores de Firma Digital, perteneciente al Ministerio de Ciencia, Tecnología y Telecomunicaciones (*), será el órgano administrador y supervisor del Sistema de Certificación.
	Decreto Nº.33018 Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos	CAPÍTULO SEGUNDO **Certificados Digitales** **Artículo 5°-Contenido y características.** El contenido, condiciones de emisión, suspensión, revocación y expiración de los certificados digitales, serán los que se señalan en la Norma INTE /ISO 21188 versión vigente y las políticas que al efecto emita la DCFD. **Artículo 6°-Tipos de certificados.** La DCFD establecerá los tipos de certificados que podrán emitir los certificadores, con estricto apego a las normas técnicas y estándares internacionales aplicables que promuevan la interoperabilidad con otros sistemas. En el caso de los certificados digitales que vayan a ser utilizados en procesos de firma digital y de autenticación de la identidad, los certificadores necesariamente deberán: 1) Utilizar al menos un proceso de verificación y registro presencial (cara a cara) de sus suscriptores. 2) Guardar copia de la documentación utilizada para verificar la identidad de la persona. 3) Registrar de forma biométrica (fotografía, huellas digitales, etc.) al suscriptor a quién le será emitido un certificado. 4) Requerir el uso de módulos seguros de creación de firma, con certificación de seguridad que se indique conforme a las normas internacionales y a las Políticas establecidas por la DCFD. 5) Establecer un contrato de suscripción detallando el nivel de servicio que ofrece y los deberes y responsabilidades de las partes. 6) La DCFD podrá establecer cualquier otro requisito que considere pertinente, en tanto emisor y gestor de políticas del sistema de firma digital.

		Artículo 7º-Obligaciones de los usuarios. Para los efectos de los artículos 14, inciso d) y 15 de la Ley, todos los suscriptores del sistema de certificados y firmas digitales estarán obligados a: 1) Suministrar a los certificadores la información veraz, completa y actualizada que éstos requieran para la prestación de sus servicios. 2) Resguardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación que se les haya asignado con ese carácter, informando inmediatamente al certificador en caso de que dicha confidencialidad se vea o se sospeche que haya sido comprometida. 3) Acatar las recomendaciones técnicas y de seguridad que le señale el correspondiente certificador. **Artículo 8°-Plazo de suspensión de certificados.** Cuando un certificado digital deba ser suspendido por incurrir en alguna de las causales establecidas en el artículo 14 de la Ley , éste será revocado y, una vez desaparecido el motivo de suspensión, se procederá a la emisión de un nuevo certificado. **Artículo 9º-Revocación por cese de actividades.** Para los efectos del artículo 16 de la Ley, en el caso del cese de actividades de un certificador, éste mismo -o la DCFD en su defecto- gestionarán el traslado de la cartera de suscriptores que así lo hayan consentido a otro certificador, que expedirá los nuevos certificados. (…).
Ecuador	Ley 2002-67 Ley de comercio electrónico, firmas electrónicas y mensajes de datos	Título II DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRÓNICA, ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Capítulo I DE LAS FIRMAS ELECTRÓNICAS **Art. 13.- Firma electrónica.** - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos. **Art. 14.- Efectos de la firma electrónica. -** La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio. **Art. 15.- Requisitos de la firma electrónica. -** Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

		a) Ser individual y estar vinculada exclusivamente a su titular; b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos; c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado. d) Que, al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y, e) Que la firma sea controlada por la persona a quien pertenece. **Art. 16.- La firma electrónica en un mensaje de datos. -** Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley. **Art. 17.- Obligaciones del titular de la firma electrónica. -** El titular de la firma electrónica deberá: a) Cumplir con las obligaciones derivadas del uso de la firma electrónica; b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada; c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente; d) Verificar la exactitud de sus declaraciones; e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia; f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y, g) Las demás señaladas en la Ley y sus reglamentos.

		Art. 18.- Duración de la firma electrónica. - Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale. **Art. 19.- Extinción de la firma electrónica. -** La firma electrónica se extinguirá por: a) Voluntad de su titular; b) Fallecimiento o incapacidad de su titular; c) Disolución o liquidación de la persona jurídica, titular de la firma; y, d) Por causa judicialmente declarada. La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso. Capítulo II DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA **Art. 20.- Certificado de firma electrónica. -** Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad. **Art. 21.- Uso del certificado de firma electrónica. -** El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento. **Art. 22.- Requisitos del certificado de firma electrónica. -** El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos: a) Identificación de la entidad de certificación de información; b) Domicilio legal de la entidad de certificación de información; c) Los datos del titular del certificado que permitan su ubicación e identificación; d) El método de verificación de la firma del titular del certificado; e) Las fechas de emisión y expiración del certificado; f) El número único de serie que identifica el certificado;

		g) La firma electrónica de la entidad de certificación de información; h) Las limitaciones o restricciones para los usos del certificado; e, i) Los demás señalados en esta ley y los reglamentos. **Art. 23.- Duración del certificado de firma electrónica.-** Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta Ley. **Art. 24.- Extinción del certificado de firma electrónica.-** Los certificados de firma electrónica, se extinguen, por las siguientes causas: a) Solicitud de su titular; b) Extinción de la firma electrónica, de conformidad con lo establecido en el Art. 19 de esta Ley; y, c) Expiración del plazo de validez del certificado de firma electrónica. La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso. **Art. 25.- Suspensión del certificado de firma electrónica. -** La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando: a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley; b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y, c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica. La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

		La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica. **Art. 26.- Revocatoria del certificado de firma electrónica.-** El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando: a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y, b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada. La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado. **Art. 27.-** Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso. La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso. **Art. 28.- Reconocimiento internacional de certificados de firma electrónica. -** Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo. Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento. Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho. Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

	Decreto Ejecutivo 3496 Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos	**Art. 10.-** Elementos de la infraestructura de firma electrónica. - La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento. Los principios y elementos que respaldan a la firma electrónica son: a) No discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada; b) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente; c) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b); d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y, e) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación. **Art. 11.-** Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en la ley. **Art. 12.-** Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos. Los períodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente. **Art. 13.-** Revocación del certificado de firma electrónica. - Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

		En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades. La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado. La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento. **Art. 14.-** De la notificación por extinción, suspensión o revocación del certificado de firma electrónica. - La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al artículo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado. **Art. 15.-** Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículo 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios: a) Siempre en la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y, b) Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica. Opcionalmente, en caso de que la entidad certificadora o el tercero vinculado relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública. **Art. 16.-** Sin perjuicio de la reglamentación que emita el CONATEL, para la aplicación del artículo 28 de la Ley No. 67, los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en el Ecuador una vez obtenida la revalidación respectiva por una Entidad de Certificación de Información y Servicios Relacionados Acreditada ante el CONATEL, la cual deberá comprobar el grado de fiabilidad de dichos certificados y de quien los emite Nota: Artículo reformado por Decreto Ejecutivo No. 908, publicado en Registro Oficial 168 de 19 de Diciembre del 2005. Nota: Artículo sustituido por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008. **Art. 17.-** Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL. Los certificados de firma electrónica emitidos y revalidados por las Entidades de Certificación de Información y Servicios Relacionados Acreditadas por el CONATEL, tienen carácter probatorio.

		Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten. (…).
El Salvador	Decreto 133 Ley de firma electrónica	TITULO I DISPOSICIONES GENERALES CAPITULO I OBJETO Y ALCANCE **Objeto** **Art. 1.-** SON OBJETO DE LA PRESENTE LEY LOS SIGUIENTES: a) EQUIPARAR LA FIRMA ELECTRÓNICA SIMPLE Y FIRMA ELECTRÓNICA CERTIFICADA CON LA FIRMA AUTÓGRAFA; b) OTORGAR Y RECONOCER EFICACIA Y VALOR JURÍDICO A LA FIRMA ELECTRÓNICA CERTIFICADA, A LOS MENSAJES DE DATOS Y A TODA INFORMACIÓN EN FORMATO ELECTRÓNICO QUE SE ENCUENTREN SUSCRITOS CON UNA FIRMA ELECTRÓNICA CERTIFICADA, INDEPENDIENTEMENTE DE SU SOPORTE MATERIAL; Y, c) REGULAR Y FISCALIZAR LO RELATIVO A LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA, CERTIFICADOS ELECTRÓNICOS Y PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS. **Neutralidad Tecnológica y Equivalencia Funcional** **Art. 2.-** Las regulaciones de la presente Ley serán aplicables a la comunicación electrónica, firma electrónica certificada y firma electrónica simple, o cualquier formato electrónico, independientemente de sus características técnicas o de los desarrollos tecnológicos que se produzcan en el futuro; sus normas serán desarrolladas e interpretadas progresivamente, siempre que se encuentren fundamentadas en la neutralidad tecnológica y equivalencia funcional. CAPITULO II DEFINICIONES Y PRINCIPIOS GENERALES **Definiciones** **Art. 3.-** PARA LOS EFECTOS DE LA APLICACIÓN DE LA PRESENTE LEY, SE UTILIZARÁN LAS SIGUIENTES DEFINICIONES:

		a) ACREDITACIÓN: AUTORIZACIÓN QUE EMITE LA UNIDAD DE FIRMA ELECTRÓNICA, A UNA PERSONA JURÍDICA, TRAS DEMOSTRAR QUE CUMPLE SATISFACTORIAMENTE LOS REQUISITOS DE ACREDITACIÓN A QUE DEBE SOMETERSE PARA LA PRESTACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN Y ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS. b) ARCHIVO ELECTRÓNICO: SOLUCIÓN INFORMÁTICA QUE PERMITE ALMACENAR DE FORMA ELECTRÓNICA LOS DOCUMENTOS DE UNA ENTIDAD PARA GARANTIZAR SU DISPONIBILIDAD, LEGIBILIDAD Y ACCESIBILIDAD A LARGO PLAZO. c) AUTENTICACIÓN DE SITIO WEB: PROPORCIONA UN MEDIO POR EL QUE PUEDE GARANTIZARSE A LA PERSONA QUE VISITA UN SITIO WEB, QUE EXISTE UNA ENTIDAD AUTÉNTICA Y LEGÍTIMA QUE RESPALDA LA EXISTENCIA DE DICHO SITIO. d) CERTIFICADO ELECTRÓNICO: DECLARACIÓN ELECTRÓNICA, EXPEDIDA POR UN PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN, QUE VINCULA LOS DATOS DE VALIDACIÓN DE UNA FIRMA ELECTRÓNICA CERTIFICADA CON UNA PERSONA NATURAL O JURÍDICA, LOS DATOS DE VALIDACIÓN DE UN SELLO ELECTRÓNICO CON UNA PERSONA JURÍDICA, O UN SITIO WEB CON LA PERSONA NATURAL O JURÍDICA. e) CREADOR DE SELLO: PERSONA JURÍDICA QUE CREA UN SELLO ELECTRÓNICO. f) DATOS PERSONALES: CUALQUIER INFORMACIÓN NUMÉRICA, ALFABÉTICA, GRÁFICA O FOTOGRÁFICA O DE CUALQUIER OTRO TIPO, CONCERNIENTE APERSONAS NATURALES IDENTIFICADAS O IDENTIFICABLES. g) DESMATERIALIZACIÓN: PROCESO POR EL CUAL, UN PROVEEDOR DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, AUTORIZADO POR LA UNIDAD DE FIRMA ELECTRÓNICA, TRANSFORMA DOCUMENTOS FÍSICOS EN DOCUMENTOS ELECTRÓNICOS. h) DESTINATARIO: LA PERSONA DESIGNADA POR EL EMISOR, PARA RECIBIR EL MENSAJE DE DATOS O DOCUMENTO ELECTRÓNICO, PERO QUE NO ESTÉ ACTUANDO A TÍTULO DE INTERMEDIARIO CON RESPECTO HA DICHO MENSAJE O DOCUMENTO. i) DISPOSITIVO SEGURO DE CREACIÓN: UN EQUIPO O PROGRAMA INFORMÁTICO CONFIGURADO, QUE SE UTILIZA PARA CREAR UNA FIRMA ELECTRÓNICA CERTIFICADA O SELLO ELECTRÓNICO. j) DOCUMENTO ELECTRÓNICO: INFORMACIÓN DE CUALQUIER NATURALEZA, CONTENIDA EN SOPORTE ELECTRÓNICO, SEGÚN UN FORMATO DETERMINADO. k) FIRMA AUTÓGRAFA: MARCA O SIGNO QUE UNA PERSONA ESCRIBE DE SU PROPIA MANO EN UN DOCUMENTO, PARA ASEGURAR O AUTENTICAR SU PROPIA IDENTIDAD, COMO PRUEBA DEL CONSENTIMIENTO SOBRE LA INFORMACIÓN CONTENIDA EN DICHO DOCUMENTO.

		l) FIRMA ELECTRÓNICA SIMPLE: SON DATOS EN FORMA ELECTRÓNICA, CONSIGNADOS EN UN MENSAJE DE DATOS O DOCUMENTO ELECTRÓNICO, LÓGICAMENTE ASOCIADOS AL MISMO, QUE PUEDAN SER UTILIZADOS PARA IDENTIFICAR AL FIRMANTE POR CUALQUIER MEDIO TECNOLÓGICO DISPONIBLE, E INDICAR QUE EL FIRMANTE APRUEBA LA INFORMACIÓN RECOGIDA EN EL MENSAJE DE DATOS O DOCUMENTO ELECTRÓNICO. m) FIRMA ELECTRÓNICA CERTIFICADA: SON LOS DATOS EN FORMA ELECTRÓNICA, CONSIGNADOS EN UN MENSAJE DE DATOS O DOCUMENTO ELECTRÓNICO, LÓGICAMENTE ASOCIADOS AL MISMO, QUE SON GENERADOS MEDIANTE UN DISPOSITIVO SEGURO DE CREACIÓN Y PERMITEN VINCULAR DE MANERA EXCLUSIVA, LA FIRMA CON SU TITULAR. n) FIRMANTE O SIGNATARIO: PERSONA NATURAL QUE CREA UNA FIRMA ELECTRÓNICA. o) INICIADOR DE UN MENSAJE DE DATOS: SE ENTENDERÁ TODA PERSONA QUE, A TENOR DEL MENSAJE, HAYA ACTUADO POR SU CUENTA PARA ENVIAR O GENERAR ESE MENSAJE ANTES DE SER ARCHIVADO, SI ÉSTE ES EL CASO, PERO QUE NO HAYA ACTUADO A TÍTULO DE INTERMEDIARIO CON RESPECTO A ÉL. p) MENSAJE DE DATOS: LA INFORMACIÓN GENERADA, ENVIADA, RECIBIDA O ARCHIVADA A TRAVÉS DE MEDIOS ELECTRÓNICOS O SIMILARES, QUE PUEDE CONTENER DOCUMENTOS ELECTRÓNICOS. q) PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN: PERSONA JURÍDICA ACREDITADA POR LA UNIDAD DE FIRMA ELECTRÓNICA, PARA PRESTAR LOS SERVICIOS DE CERTIFICACIÓN, EN LA MODALIDAD DE FIRMA ELECTRÓNICA CERTIFICADA, SELLO ELECTRÓNICO, SELLO DE TIEMPO O AUTENTICACIÓN DE SITIO WEB. r) PROVEEDOR DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS: PERSONA JURÍDICA ACREDITADA POR LA UNIDAD DE FIRMA ELECTRÓNICA, PARA PRESTAR LOS SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS. s) SELLO ELECTRÓNICO: SON LOS DATOS EN FORMA ELECTRÓNICA, CONSIGNADOS EN UN MENSAJE DE DATOS O DOCUMENTO ELECTRÓNICO, GENERADOS MEDIANTE UN DISPOSITIVO SEGURO DE CREACIÓN, QUE GARANTIZAN EL ORIGEN Y LA INTEGRIDAD DE ESTOS, ASOCIADOS INEQUÍVOCAMENTE AL TITULAR DEL CERTIFICADO ELECTRÓNICO. t) SELLO DE TIEMPO: MECANISMO QUE APORTA CERTEZA SOBRE LA INTEGRIDAD DEL DOCUMENTO ELECTRÓNICO O MENSAJE DE DATOS, ASIGNANDO UNA FECHA Y HORA QUE PERMITEN DEMOSTRAR QUE, UNA SERIE DE DATOS DE CARÁCTER ELECTRÓNICO HAN EXISTIDO, NO HAN SIDO ALTERADOS A PARTIR DE UN INSTANTE ESPECÍFICO EN EL TIEMPO. u) TITULAR: ES LA PERSONA A CUYO FAVOR LE FUE EXPEDIDO UN CERTIFICADO ELECTRÓNICO DE FIRMA ELECTRÓNICA CERTIFICADA, SELLO ELECTRÓNICO, SELLO DE TIEMPO O AUTENTICACIÓN DE SITIO WEB. (...). CAPÍTULO III

		EQUIVALENCIA Y VALOR JURÍDICO DE LA FIRMA ELECTRÓNICA **Equivalencia y Valor Jurídico de la Firma Electrónica Simple** Art. 6.- LA FIRMA ELECTRÓNICA SIMPLE TENDRÁ LA MISMA VALIDEZ JURÍDICA QUE LA FIRMA AUTÓGRAFA. EN CUANTO A SUS EFECTOS JURÍDICOS, LA FIRMA ELECTRÓNICA SIMPLE NO TENDRÁ VALIDEZ PROBATORIA EN LOS MISMOS TÉRMINOS A LOS CONCEDIDOS POR ESTA LEY A LA FIRMA ELECTRÓNICA CERTIFICADA; SIN EMBARGO, PODRÁ CONSTITUIR UN ELEMENTO DE PRUEBA CONFORME A LAS REGLAS DE LA SANA CRÍTICA. (…). TÍTULO III FIRMA ELECTRÓNICA CERTIFICADA, SELLO ELECTRÓNICO, SELLO DE TIEMPO, AUTENTICACIÓN DE SITIO WEB, CERTIFICADOS ELECTRÓNICOS Y DOCUMENTOS ELECTRÓNICOS CAPÍTULO I DISPOSICIONES GENERALES **REQUISITOS PARA LA FIRMA ELECTRÓNICA CERTIFICADA** **Art. 23.-** LA FIRMA ELECTRÓNICA CERTIFICADA DEBERÁ DE CUMPLIR LOS SIGUIENTES REQUISITOS: a) VINCULAR AL FIRMANTE, DE MANERA ÚNICA; b) ESTAR BASADO EN UN CERTIFICADO ELECTRÓNICO EMITIDO POR UN PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN; c) PERMITIR LA VERIFICACIÓN INEQUÍVOCA DE LA AUTORÍA E IDENTIDAD DEL SIGNATARIO; d) HABER SIDO CREADA UTILIZANDO MEDIOS DE CREACIÓN Y VERIFICACIÓN CONFIABLE Y SEGURO, BAJO EL CONTROL EXCLUSIVO DEL SIGNATARIO; e) ESTAR VINCULADA CON LA INFORMACIÓN DE MODO TAL QUE CUALQUIER MODIFICACIÓN ULTERIOR DE LOS MISMOS SEA DETECTABLE; f) LOS CERTIFICADOS ELECTRÓNICOS EMITIDOS PARA FIRMA ELECTRÓNICA CERTIFICADA CUMPLIRÁN LOS REQUISITOS DEL ARTÍCULO 58, DE LA PRESENTE LEY. (…).

		EFECTOS JURÍDICOS PROBATORIOS DE LA FIRMA ELECTRÓNICA CERTIFICADA **Art. 24.-** La firma electrónica certificada tendrá igual validez y los mismos efectos jurídicos y probatorios que una firma manuscrita en relación con los datos consignados en un documento o mensaje de datos electrónicos en que fuere empleada. En todo caso, al valorar la fuerza probatoria de un documento electrónico, se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado, comunicado, y en la que se haya conservado la integridad de la información. **Presunciones del Empleo de la Firma Electrónica Certificada** **Art. 25.-** EL EMPLEO DE LA FIRMA ELECTRÓNICA CERTIFICADA QUE CUMPLA LOS REQUISITOS EXIGIDOS EN LA PRESENTE LEY, SALVO PRUEBA EN CONTRARIO, PRESUME LO SIGUIENTE: a) QUE LA FIRMA ELECTRÓNICA CERTIFICADA PERTENECE AL TITULAR DEL CERTIFICADO ELECTRÓNICO; Y, b) QUE LA FIRMA ELECTRÓNICA CERTIFICADA VINCULADA AL DOCUMENTO ELECTRÓNICO O MENSAJE DE DATOS NO HA SIDO MODIFICADA DESDE EL MOMENTO DE SU FIRMA, SI EL RESULTADO DEL PROCEDIMIENTO DE VERIFICACIÓN ASÍ LO INDICA. (...). **Inhabilitación en el Uso de Firma Electrónica Certificada** **Art. 26.-** NO PODRÁN SOLICITAR CERTIFICADOS ELECTRÓNICOS Y HACER USO DE LA FIRMA ELECTRÓNICA CERTIFICADA, LOS MENORES DE EDAD Y LOS INCAPACES DECLARADOS CONFORME A LAS REGLAS DEL DERECHO COMÚN, Y LOS PRIVADOS DE LIBERTAD CONDENADOS EN SENTENCIA FIRME. LO ANTERIOR, SIN PERJUICIO DE LO DISPUESTO EN LAS LEYES ESPECIALES PERTINENTES. (…). **SOLICITUD PARA EL USO DE LA FIRMA ELECTRÓNICA CERTIFICADA POR REPRESENTANTES DE PERSONAS NATURALES** **Art. 27.-** PARA LOS MANDATARIOS DE LAS PERSONAS NATURALES, SÓLO SE UTILIZARÁ LA FIRMA ELECTRÓNICA CERTIFICADA DE AQUELLOS, PREVIA VERIFICACIÓN DE TAL CALIDAD POR PARTE DEL PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN, A TRAVÉS DE LA PRESENTACIÓN DE LOS DOCUMENTOS LEGALES PERTINENTES DE CONFORMIDAD AL ORDENAMIENTO JURÍDICO Y PODER SUFICIENTE QUE ACREDITEN TAL CALIDAD, CIRCUNSTANCIA QUE DEBERÁ CONSTAR EN EL CERTIFICADO ELECTRÓNICO QUE SE LE EXTIENDA, ASÍ COMO LOS LÍMITES DE SUS FACULTADES. LA CUSTODIA DE LOS DATOS DE CREACIÓN DE FIRMA, Y EL USO DE ESTOS A TRAVÉS DE LOS MÉTODOS DE AUTENTICACIÓN HABILITADOS PARA TALES EFECTOS, SERÁ RESPONSABILIDAD DEL REPRESENTANTE DE LA PERSONA NATURAL TITULAR DEL CERTIFICADO ELECTRÓNICO, CUYA IDENTIFICACIÓN SE INCLUIRÁ EN EL MISMO. (…). USO DE LA FIRMA ELECTRÓNICA, SELLO ELECTRÓNICO Y SELLO DE TIEMPO POR LOS

		ÓRGANOS DE GOBIERNO **Uso de Firma Electrónica Simple** **Art. 29**.- Las autoridades, funcionarios y empleados del Estado que presten servicios públicos, ejecuten o realicen actos dentro de su ámbito de competencia, podrán suscribirlos por medio de firma electrónica simple. **Uso de Firma Electrónica Certificada** **Art. 30.-** EN AQUELLOS CASOS EN QUE LOS FUNCIONARIOS O EMPLEADOS DEL ESTADO EXPIDAN CUALQUIER DOCUMENTO O REALICEN ACTOS ADMINISTRATIVOS EN QUE SE OTORGUEN DERECHOS, SANCIONEN, O CONSTITUYAN INFORMACIÓN CONFIDENCIAL, SEGÚN LO DISPUESTO EN EL ARTÍCULO 24 DE LA LEY DE ACCESO A LA INFORMACIÓN PÚBLICA A LOS ADMINISTRADOS, SERÁ NECESARIO UTILIZAR FIRMA ELECTRÓNICA CERTIFICADA. EL PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DEBERÁ CONSIGNAR EN EL CERTIFICADO LA CALIDAD CON LA QUE FIRMARÁ ELECTRÓNICAMENTE, ASÍ COMO LOS LÍMITES DE SU COMPETENCIA. SE EXCEPTÚAN DEL USO DE LA FIRMA ELECTRÓNICA CERTIFICADA, EN AQUELLAS ACTUACIONES PARA LAS CUALES LA CONSTITUCIÓN DE LA REPÚBLICA O LAS LEYES EXIJAN ALGUNA SOLEMNIDAD QUE NO SEA SUSCEPTIBLE DE CUMPLIRSE MEDIANTE DOCUMENTOS ELECTRÓNICOS. EN CUANTO AL SELLO ELECTRÓNICO Y SELLO DE TIEMPO, LOS FUNCIONARIOS O EMPLEADOS DEL ESTADO, Y EN GENERAL LAS DISTINTAS INSTITUCIONES PÚBLICAS, PODRÁN UTILIZARLOS, EN ATENCIÓN A LA NATURALEZA DE LA ACTUACIÓN A REALIZAR. **Validez de Actos y Contratos** **Art. 31.-** LOS ACTOS Y DOCUMENTOS DE LAS INSTITUCIONES DEL ESTADO QUE TENGAN LA CALIDAD DE INSTRUMENTO PÚBLICO, PODRÁN SUSCRIBIRSE MEDIANTE FIRMA ELECTRÓNICA CERTIFICADA. LO ANTERIOR SIN PERJUICIO DE LO DISPUESTO EN EL ARTÍCULO 19 DE LA LEY DE PROCEDIMIENTOS ADMINISTRATIVOS. **Interacción Electrónica entre Administrados y Funcionarios Públicos** **Art. 32.-** EN LAS ACTUACIONES DE LOS ADMINISTRADOS, ÉSTOS PODRÁN PRESENTAR LA INFORMACIÓN SOLICITADA POR LA ADMINISTRACIÓN PÚBLICA EN FORMULARIOS ELECTRÓNICOS OFICIALES, SISTEMAS ELECTRÓNICOS EN LÍNEA O MEDIANTE DOCUMENTOS ELECTRÓNICOS SUSCRITOS CON FIRMA ELECTRÓNICA SIMPLE O CERTIFICADA, SELLO ELECTRÓNICO O SELLO DE TIEMPO. **DEL REQUERIMIENTO DE FIRMA** **Art. 32-A.-** CUANDO LA LEY REQUIERA UNA FIRMA AUTÓGRAFA, ESA EXIGENCIA TAMBIÉN QUEDA SATISFECHA POR UNA FIRMA ELECTRÓNICA. ESTE PRINCIPIO ES APLICABLE A LOS CASOS EN QUE LA LEY ESTABLECE LA OBLIGACIÓN DE FIRMAR O PRESCRIBE CONSECUENCIAS PARA SU AUSENCIA. **PRESUNCIÓN DE REMITENTE**

		Art. 32-B.- CUANDO UN DOCUMENTO ELECTRÓNICO SEA FIRMADO POR UN CERTIFICADO DE APLICACIÓN, SE PRESUMIRÁ, SALVO PRUEBA EN CONTRARIO, QUE EL DOCUMENTO FIRMADO PROVIENE DE LA PERSONA TITULAR DEL CERTIFICADO. **Actos de Comunicaciones** **Art. 33.-** Cualquier institución del Estado, siempre y cuando cuente con la infraestructura tecnológica adecuada, deberá realizar comunicaciones por vía electrónica utilizando firma electrónica simple, de actos tales como citaciones y notificaciones, siempre y cuando el destinatario de los servicios públicos hubiera autorizado ese medio de comunicación. Dicha autorización surtirá efecto mientras el destinatario no comunique una modificación al respecto. **Conservación, Registro y Archivo** **Art. 34.-** LAS INSTITUCIONES DEL ESTADO PODRÁN DISPONER LA CONSERVACIÓN, REGISTRO Y ARCHIVO DE CUALQUIER ACTUACIÓN QUE ESTÉ BAJO SU COMPETENCIA, POR MEDIO DE SISTEMAS ELECTRÓNICOS, BAJO LA FIGURA DEL ALMACENADOR POR CUENTA PROPIA. TALES ARCHIVOS Y REGISTROS SUSTITUIRÁN A LOS REGISTROS FÍSICOS PARA TODO EFECTO, DEBIÉNDOSE CUMPLIR PARA ELLO CON LOS REQUISITOS ESTABLECIDOS EN EL ARTÍCULO 13-A DE ESTA LEY Y DEMÁS LEYES PERTINENTES. LAS INSTITUCIONES DEL ESTADO PODRÁN CONTRATAR A CUALQUIER PRESTADOR DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS QUE CUMPLA CON LAS CONDICIONES TÉCNICAS Y LEGALES ESTABLECIDAS EN ESTA LEY, SU REGLAMENTO Y LAS NORMAS Y REGLAMENTOS TÉCNICOS. NO OBSTANTE, LO ANTERIOR, LAS INSTITUCIONES OFICIALES AUTÓNOMAS Y DEMÁS INSTITUCIONES DEL ESTADO CON PERSONERÍA JURÍDICA PROPIA, ESTABLECIDAS CONFORME A LAS LEYES DE LA REPÚBLICA, PODRÁN PRESTAR LOS SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, PREVIA ACREDITACIÓN POR PARTE DE LA UNIDAD DE FIRMA ELECTRÓNICA, DE ACUERDO CON EL TRÁMITE SEÑALADO EN LA PRESENTE LEY. CAPÍTULO III DE LA AUTORIDAD COMPETENTE **La Autoridad de Control y Vigilancia** **Art. 35.-** Créase la Unidad de Firma Electrónica, como parte del Ministerio de Economía, el que en el texto de esta Ley podrá abreviarse MINEC. El Ministro nombrará al funcionario que estará a cargo de esta Unidad, quien deberá reunir los requisitos que para tal efecto se establezcan en el reglamento de esta Ley. **De la Unidad de Firma Electrónica** **Art. 36.-** La Unidad de Firma Electrónica será la autoridad registradora y acreditadora raíz, y la competente para la acreditación, control y vigilancia de los proveedores de los servicios de certificación electrónica y de almacenamiento de documentos electrónicos, de conformidad con esta Ley, su reglamento y las normas y reglamentos técnicos. **Competencias de la Unidad de Firma Electrónica**

		Art. 37.- LA UNIDAD DE FIRMA ELECTRÓNICA TENDRÁ LAS SIGUIENTES COMPETENCIAS: a) ELABORAR LAS NORMAS Y LOS REGLAMENTOS TÉCNICOS QUE SEAN NECESARIOS PARA LA IMPLEMENTACIÓN DE LA PRESENTE LEY, EN COORDINACIÓN CON EL ORGANISMO SALVADOREÑO DE REGLAMENTACIÓN TÉCNICA (OSARTEC) Y EL ORGANISMO SALVADOREÑO DE NORMALIZACIÓN (OSN); b) OTORGAR Y REGISTRAR LA ACREDITACIÓN A LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN Y A LOS PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, UNA VEZ CUMPLIDAS LAS FORMALIDADES Y REQUISITOS DE ESTA LEY, SU REGLAMENTO Y DEMÁS NORMAS Y REGLAMENTOS TÉCNICOS APLICABLES. ASÍ COMO DENEGAR, SUSPENDER, RENOVAR O REVOCAR, LA ACREDITACIÓN DE AQUELLOS QUE INCUMPLAN DICHAS NORMATIVAS; c) VALIDAR LOS CERTIFICADOS ELECTRÓNICOS EMITIDOS A FAVOR DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN Y DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS; d) SUPERVISAR, VERIFICAR E INSPECCIONAR QUE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN Y LOS PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, CUMPLAN CON LOS REQUISITOS CONTENIDOS EN LA PRESENTE LEY, SU REGLAMENTO, ASÍ COMO EN NORMAS Y REGLAMENTOS TÉCNICOS APLICABLES; e) RECAUDAR LOS ARANCELES REGISTRALES ESTABLECIDOS EN LA PRESENTE LEY; f) IMPONER LAS SANCIONES ESTABLECIDAS EN ESTA LEY; g) IMPONER LAS MULTAS ESTABLECIDAS EN LA PRESENTE LEY, LAS CUALES INGRESARÁN AL FONDO GENERAL DE LA NACIÓN; h) COORDINAR Y REPRESENTAR AL PAÍS FRENTE A LOS ORGANISMOS NACIONALES E INTERNACIONALES DE CONFORMIDAD A LA LEGISLACIÓN APLICABLE SOBRE CUALQUIER ASPECTO RELACIONADO CON EL OBJETO DE ESTA LEY; i) INSTRUIR DE OFICIO O A INSTANCIA DE PARTE, SUSTANCIAR Y DECIDIR LOS PROCEDIMIENTOS ADMINISTRATIVOS RELATIVOS A PRESUNTAS INFRACCIONES A ESTA LEY; j) INFORMAR DE OFICIO A LA FISCALÍA GENERAL DE LA REPÚBLICA, CUANDO TENGA INDICIOS DE UN DELITO; k) REQUERIR DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN Y A LOS PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, O SUS USUARIOS, CUALQUIER INFORMACIÓN QUE CONSIDERE NECESARIA Y QUE ESTÉ RELACIONADA CON MATERIAS RELATIVAS AL ÁMBITO DE SUS FUNCIONES;

		l) PUBLICAR Y MANTENER ACTUALIZADO EN LA PÁGINA WEB INSTITUCIONAL, EL LISTADO DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN Y DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS; m) DEFINIR Y REALIZAR LOS PROCEDIMIENTOS PARA LA RECEPCIÓN Y RESOLUCIÓN DE DENUNCIAS; n) ELABORAR UN MARCO DE REFERENCIA DE LOS PRECIOS DE LOS SERVICIOS DE CERTIFICACIÓN Y DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, EN BASE A ESTUDIOS TÉCNICOS REFERENTES A LA MATERIA; o) ESTABLECER, MANTENER Y PUBLICAR LISTAS DE CONFIANZA CON INFORMACIÓN RELATIVA A LOS PROVEEDORES ACREDITADOS, ASÍ COMO DE LOS SERVICIOS PRESTADOS POR ESTOS; Y, p) LAS DEMÁS QUE ESTABLEZCA LA PRESENTE LEY Y SU REGLAMENTO, ASÍ COMO LAS PREVISTAS EN OTRAS NORMAS Y REGLAMENTOS TÉCNICOS APLICABLES. LA UNIDAD DE FIRMA ELECTRÓNICA ESTABLECERÁ, MANTENDRÁ Y PUBLICARÁ, DE MANERA SEGURA, LAS LISTAS DE CONFIANZA FIRMADAS O SELLADAS ELECTRÓNICAMENTE A QUE SE REFIERE EL LITERAL o) DE ESTE ARTÍCULO, EN UNA FORMA APROPIADA PARA EL TRATAMIENTO AUTOMÁTICO. **Conformación del Comité Técnico Consultivo** **Art. 38.-** Créase el Comité Técnico Consultivo, con el objeto de asesorar al Ministerio de Economía en lo relativo a la Ley de Firma Electrónica. Este Comité podrá ser consultado sobre cualquier aspecto de la aplicación e implementación de la presente Ley, y sesionará al menos una vez trimestralmente; su funcionamiento será regulado por el reglamento de esta Ley. El Comité estará integrado por un propietario y su respectivo suplente, de las siguientes instituciones e instancias: a) El Jefe de la Unidad de Firma Electrónica del Ministerio de Economía, quien lo presidirá; b) La Superintendencia de Competencia; c) LA INSTITUCIÓN, OFICINA O ENTIDAD CON COMPETENCIA EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, QUE DESIGNE LA PRESIDENCIA DE LA REPÚBLICA; d) La Superintendencia General de Electricidad y Telecomunicaciones; e) La Defensoría del Consumidor; f) De las gremiales de la empresa privada con personería jurídica relacionada con el objeto de esta Ley;

		g) Las universidades acreditadas por el Ministerio de Educación; y, h) Las organizaciones no gubernamentales con personalidad jurídica relacionadas al objeto de esta Ley. En el caso de los literales f), g) y h) del inciso anterior, los nominados serán seleccionados y propuestos por cada una de las instituciones de acuerdo a su ordenamiento interno, estableciéndose en el reglamento de esta Ley el procedimiento para su nombramiento. El ejercicio del cargo de los miembros del Comité será ad-honorem, los cuales serán nombrados para un período de tres años. (…). **MEDIDAS PARA GARANTIZAR LOS SERVICIOS** **Art. 42.-** LA UNIDAD DE FIRMA ELECTRÓNICA DEL MINISTERIO DE ECONOMÍA, ADOPTARÁ LAS MEDIDAS PREVENTIVAS NECESARIAS PARA GARANTIZAR LA CONFIABILIDAD DE LOS SERVICIOS PRESTADOS POR LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN, Y DE LOS PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, LOS CUALES DEBERÁN SER DE ALTA DISPONIBILIDAD. A TAL EFECTO, DICTARÁ LAS NORMAS Y REGLAMENTOS TÉCNICOS NECESARIOS Y, ENTRE OTRAS MEDIDAS, EMITIRÁ LAS RELACIONADAS CON EL USO DE ESTÁNDARES O PRÁCTICAS INTERNACIONALMENTE ACEPTADAS PARA LA PRESTACIÓN DE LOS SERVICIOS DE FIRMA ELECTRÓNICA CERTIFICADA, Y DE LOS SERVICIOS DE ALMACENAMIENTO DE DOCUMENTOS ELECTRÓNICOS, O QUE EL PROVEEDOR SE ABSTENGA DE REALIZAR CUALQUIER ACTIVIDAD QUE PONGA EN PELIGRO LA INTEGRIDAD O EL BUEN USO DEL SERVICIO. CAPÍTULO IV DE LA ACREDITACIÓN Y PRESTACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN **Requisitos Generales** **Art. 43.-** EL SERVICIO DE CERTIFICACIÓN SÓLO PODRÁ SER PRESTADO POR AQUELLAS PERSONAS JURÍDICAS, NACIONALES O EXTRANJERAS, QUE CUMPLAN CON LOS REQUISITOS ESTABLECIDOS EN LAS LEYES COMPETENTES PARA OPERAR EN EL PAÍS, Y QUE DEMUESTREN PARA SU AUTORIZACIÓN Y DURANTE TODO EL PERÍODO EN QUE SE PRESTEN LOS SERVICIOS DE CERTIFICACIÓN, CUMPLIR CON LOS SIGUIENTES REQUISITOS: a) CONTAR CON SUFICIENTE CAPACIDAD TÉCNICA PARA GARANTIZAR LA SEGURIDAD, LA CALIDAD Y LA FIABILIDAD DE LOS SERVICIOS DE CERTIFICACIÓN, DE CONFORMIDAD A LOS REQUERIMIENTOS CONTENIDOS EN LAS NORMAS TÉCNICAS; b) CONTAR CON EL PERSONAL TÉCNICO ADECUADO CON CONOCIMIENTO ESPECIALIZADO COMPROBABLE EN LA MATERIA Y EXPERIENCIA EN EL SERVICIO A PRESTAR;

		c) POSEER LA CAPACIDAD ECONÓMICA Y FINANCIERA SUFICIENTE PARA PRESTAR LOS SERVICIOS DE CERTIFICACIÓN, EN LAS MODALIDADES AUTORIZADAS. LA CAPACIDAD ANTES MENCIONADA SERÁ MEDIDA, NO SÓLO POR LOS EQUIPOS, INSUMOS, LICENCIAS Y OTROS BIENES CON LOS QUE CUENTE PARA PRESTAR SUS SERVICIOS, SINO TAMBIÉN POR EL CAPITAL DE TRABAJO CON EL QUE FUNCIONARÁ. ESTA CONSTATACIÓN LA REALIZARÁ LA UNIDAD DE FIRMA ELECTRÓNICA, MEDIANTE LAS AUDITORÍAS Y ESTUDIOS QUE CONSIDERE CONVENIENTE, Y SE REVISARÁ DURANTE EL TIEMPO DE FUNCIONAMIENTO DEL PROVEEDOR; d) RENDIR UNA GARANTÍA POR UN MONTO ADECUADO AL RIESGO ASUMIDO POR LA PRESTACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN, OTORGADA POR UNA SOCIEDAD AUTORIZADA POR LA SUPERINTENDENCIA DEL SISTEMA FINANCIERO, LA QUE SE CALCULARÁ CONFORME A LOS REQUERIMIENTOS DEFINIDOS EN EL REGLAMENTO DE LA PRESENTE LEY. PARA LOS EFECTOS DE ESTA LEY, SE EXCLUYEN LAS GARANTÍAS Y LOS DERECHOS REALES QUE PUEDAN CONSTITUIRSE SOBRE UN BIEN MUEBLE O INMUEBLE DETERMINADO. ESTA GARANTÍA SERÁ UTILIZADA PARA INDEMNIZAR LOS DAÑOS Y PERJUICIOS QUE SE OCASIONASEN A LOS USUARIOS DE LOS SERVICIOS. LA GARANTÍA SERÁ REVISADA ANUALMENTE TOMANDO EN CUENTA LOS CAMBIOS EN EL NIVEL DE RIESGO ASUMIDO POR EL PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN. (1) (2) LAS INSTITUCIONES PÚBLICAS QUE DESEEN ACREDITARSE COMO PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN, POR SU NATURALEZA ESTATAL ESTARÁN EXCLUIDAS DE ESTE REQUISITO, DEBIENDO PRESENTAR EN SU LUGAR UN PLAN DE ACCIÓN QUE DETALLE LA FORMA DE INDEMNIZAR DAÑOS Y PERJUICIOS EN CASO DE INCUMPLIMIENTOS. UN REGLAMENTO TÉCNICO DESARROLLARÁ EL PROCEDIMIENTO PARA HACER EFECTIVAS LAS GARANTÍAS O EL PLAN DE ACCIÓN CORRESPONDIENTE; e) CONTAR CON UN SISTEMA DE INFORMACIÓN DE ALTA DISPONIBILIDAD, ACTUALIZADO Y EFICIENTE PARA LA PRESTACIÓN DEL SERVICIO, DE ACUERDO A LOS PARÁMETROS ESTABLECIDOS EN EL REGLAMENTO TÉCNICO CORRESPONDIENTE, EMITIDO POR LA UNIDAD DE FIRMA ELECTRÓNICA; f) PUBLICAR LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y LA POLÍTICA DE CERTIFICACIÓN EN UN MEDIO ELECTRÓNICO PERMANENTE; Y, g) SATISFACER LOS DEMÁS REQUISITOS PREVISTOS EN ESTA LEY. LAS INSTITUCIONES OFICIALES AUTÓNOMAS Y DEMÁS INSTITUCIONES PÚBLICAS CON PERSONERÍA JURÍDICA PROPIA ESTABLECIDAS CONFORME A LAS LEYES DE LA REPÚBLICA, QUEDAN FACULTADAS PARA PRESTAR LOS SERVICIOS REGULADOS EN ESTA LEY. DICHAS INSTITUCIONES DEBERÁN CUMPLIR LOS REQUISITOS ESTABLECIDOS EN EL PRESENTE ARTÍCULO PARA SER ACREDITADAS. **MODALIDAD DE SERVICIOS** **Art. 43-A.-** LOS SERVICIOS DE CERTIFICACIÓN COMPRENDEN LAS MODALIDADES DE FIRMA ELECTRÓNICA CERTIFICADA, SELLO ELECTRÓNICO, SELLO DE TIEMPO Y AUTENTICACIÓN DE SITIOS WEB. TRATÁNDOSE DE PROVEEDORES DE

		SERVICIOS DE CERTIFICACIÓN QUE HAYAN SIDO ACREDITADOS EN ALGUNA DE LAS MODALIDADES ANTES MENCIONADAS, Y DESEEN OFRECER SERVICIOS EN UNA MODALIDAD DISTINTA A LA CUAL FUERON ACREDITADOS, DEBERÁN DE SEGUIR EL TRÁMITE PREVISTO EN EL ARTÍCULO 44 DE ESTA LEY, Y DEMOSTRAR EL CUMPLIMIENTO DE LOS REQUISITOS PREVISTOS EN EL ARTÍCULO ANTERIOR, EN RELACIÓN A LA NUEVA MODALIDAD QUE PRETENDEN PRESTAR. (…). **DECLARACIÓN DE PRÁCTICAS Y POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA CERTIFICADA Y SELLO ELECTRÓNICO** **Art. 44-A.-** TODA PERSONA QUE PROVEA SERVICIOS DE CERTIFICACIÓN EN LA MODALIDAD DE FIRMA ELECTRÓNICA CERTIFICADA Y SELLO ELECTRÓNICO, REDACTARÁ UNA DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN, EN LA QUE DETALLARÁ, LA SIGUIENTE INFORMACIÓN: a) LAS OBLIGACIONES QUE SE COMPROMETEN A CUMPLIR, EN RELACIÓN CON LA GESTIÓN DE CERTIFICADOS ELECTRÓNICOS Y DATOS DE CREACIÓN Y VERIFICACIÓN DE FIRMA Y SELLO; b) EL DETALLE DE LOS SERVICIOS QUE FUERON AUTORIZADOS A PRESTAR POR LA UNIDAD COMPETENTE Y LAS FUNCIONES DE VERIFICACIÓN Y REGISTRO; c) LAS CONDICIONES APLICABLES A LA SOLICITUD, EMISIÓN, SUSPENSIÓN, RENOVACIÓN, REVOCACIÓN, MODIFICACIÓN, TRASPASO A OTROS PROVEEDORES, USO Y EXTINCIÓN DE LA VIGENCIA DE LOS CERTIFICADOS ELECTRÓNICOS; d) LAS MEDIDAS DE SEGURIDAD TÉCNICA, LÓGICA, FÍSICA Y ORGANIZATIVA; e) LOS MECANISMOS DE NOTIFICACIÓN SOBRE LA EMISIÓN, SUSPENSIÓN, RENOVACIÓN, REVOCACIÓN, MODIFICACIÓN Y VIGENCIA DE LOS CERTIFICADOS, CANCELACIÓN DEL SERVICIO, TRASPASO A OTROS PROVEEDORES, TÉRMINOS Y CONDICIONES, Y CESE DE ACTIVIDAD; f) LOS LÍMITES DE RESPONSABILIDAD PARA PRESTAR LOS SERVICIOS DE CERTIFICACIÓN Y CUALQUIER EVENTO QUE LIMITE LA OPERACIÓN DEL PROVEEDOR; g) LA LISTA DE NORMAS Y PROCEDIMIENTOS DE CERTIFICACIÓN; h) REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS; i) PROCEDIMIENTOS SOBRE LA VALIDACIÓN INICIAL DE LA IDENTIDAD; Y, j) CUALQUIER OTRA INFORMACIÓN QUE LA UNIDAD DE FIRMA ELECTRÓNICA SOLICITE MEDIANTE NORMAS Y REGLAMENTOS TÉCNICOS.

		LA DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN SERÁN PROPORCIONADAS A LA UNIDAD DE FIRMA ELECTRÓNICA PARA SU APROBACIÓN, Y DEBERÁ SER ACCESIBLE AL PÚBLICO POR VÍA ELECTRÓNICA O POR CUALQUIER OTRO MEDIO, Y DE FORMA GRATUITA. (…).
	Decreto No. 60. Reglamento de la Ley de Firma Electrónica	CAPÍTULO I Disposiciones Generales **Art. 1.- Objeto** El presente Reglamento tiene por objeto la aplicación y desarrollo de las disposiciones establecidas en la Ley de Firma Electrónica, a efecto que se cumpla con sus finalidades. **Art. 2.- Definiciones** Para la aplicación del presente Reglamento, se entenderá por: Certificado Electrónico Extranjero**:** Certificado electrónico emitido por un proveedor de servicios de certificación extranjero, que no ha sido acreditado por la Unidad de Firma Electrónica para brindar dichos servicios dentro del territorio nacional, pero que cuenta con un grado de fiabilidad equivalente. Se entenderá que un certificado electrónico extranjero, cuenta con un grado de fiabilidad equivalente, si cumple los requisitos establecidos en la Ley de Firma Electrónica. Documento Físico: Información de cualquier naturaleza, contenida en soporte material. Documento Electrónico: Información de cualquier naturaleza, contenida en soporte electrónico, según un formato determinado. Proveedor de Servicios: Persona jurídica acreditada por la Unidad de Firma Electrónica para prestar servicios de certificación, en las modalidades que establece la Ley, o de almacenamiento de documentos electrónicos. **Art. 3.- Ámbito de aplicación** El presente Reglamento será de aplicación y de obligatorio cumplimiento para los particulares, servidores públicos, los proveedores de servicios de certificación y almacenamiento de documentos electrónicos, públicos y privados, así como la Unidad de Firma Electrónica, en adelante denominada la Unidad. (…). CAPÍTULO VII CERTIFICADOS ELECTRÓNICOS **Art. 32.- De los Certificados Electrónicos** Los proveedores de servicios de certificación deberán introducir en los certificados electrónicos que emitan, las menciones señaladas en el artículo 58 de la Ley y los requisitos establecidos en las normas técnicas, de conformidad al rubro correspondiente.

		Los atributos adicionales que los proveedores de servicios de certificación introduzcan, con la finalidad de incorporar límites al uso del certificado, no deberán dificultar o impedir la lectura de las menciones señaladas en el inciso anterior, ni su reconocimiento por terceros. **Art. 33.- Identificación del usuario** Los Proveedores de Servicios de Certificación deberán comprobar fehacientemente la identidad del solicitante, antes de la emisión de cualquier certificado electrónico. La comprobación la hará el proveedor de servicios de certificación, ante sí, por cualquiera de los métodos de identificación previstos en la Ley, en todo caso, el solicitante deberá presentar o exhibir como mínimo el documento de identidad personal y en el caso de personas jurídicas, los documentos que acrediten la existencia legal y quien ejerce su representación legal. **Art. 33-A.- De los Certificados Electrónicos de Personas Jurídicas.** Las personas jurídicas legalmente constituidas podrán hacer uso de cualquiera de los servicios de certificación que se detallan en la Ley. Los certificados electrónicos correspondientes a cualquiera de los servicios antes mencionados podrán ser solicitados a través de quien ejerza la representación legal de la persona jurídica, por ejecutores especiales o por medio de apoderado. Las personas jurídicas podrán imponer los límites que consideren necesarios para el uso de los certificados electrónicos a que se refiere el inciso anterior, dichos límites deberán figurar en el certificado en cuestión. La revocación o suspensión de los certificados electrónicos a que se refiere el presente artículo podrá llevarse a cabo por medio del representante legal, ejecutores especiales o por medio de apoderado. No podrán solicitar certificados electrónicos de ninguna de las modalidades previstas en la Ley, ni hacer uso de estos, las uniones y entidades que no cumplan los requisitos legalmente establecidos para constituirse como personas jurídicas. **Art. 34.- Información del Usuario** Los datos de creación de firma, al ser generados por el proveedor de servicios de certificación, deben ser entregados al usuario o titular del certificado, por medio de cualquier método que garantice la seguridad, confidencialidad e integridad de estos. Queda prohibido al proveedor de servicios de certificación, mantener copia de los datos de creación de firma electrónica o de cualquier otra modalidad de servicios de certificación, una vez que estos hayan sido entregados a su titular, momento desde el cual este comenzará a ser responsable de mantenerlos bajo su exclusivo control. **Art. 35.- Límites del uso del certificado** El certificado electrónico para la firma electrónica podrá ser usado por su titular, de conformidad con las operaciones que han sido autorizadas a realizar en las prácticas de certificación del proveedor con quien se ha contratado. El certificado electrónico para la firma electrónica certificada deberá permitir a quien lo reciba, verificar en forma directa o mediante consulta electrónica, que ha sido emitido por un proveedor acreditado de servicios de certificación, con la finalidad de comprobar la validez del mismo.

		Art. 35-A.- Revocación de Certificados Electrónicos de Usuarios. La revocación de un certificado electrónico implica el cese permanente de los efectos jurídicos de este, conforme a los usos que le son propios e impide su uso. CAPÍTULO VIII SOBRE LA UTILIZACIÓN DE FIRMA ELECTRÓNICA PARA LAS ENTIDADES DEL ESTADO **Art. 36.- Incentivos de los mecanismos de gobierno electrónico.** Con excepción de aquellos trámites que necesariamente requieran la presencia del ciudadano o que este opte por realizarlos de ese modo, todos los órganos del Estado deberán incentivar el uso de documentos electrónicos, firma electrónica, sello electrónico y sello de tiempo, 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. Todos los órganos del Estado y demás instituciones públicas, deberán ajustar sus disposiciones a los principios de neutralidad tecnológica e interoperabilidad. Los documentos electrónicos generados por cualquier actuación, bajo la competencia de cualquier institución del Estado, podrán ser almacenados por medio de la figura del almacenamiento por cuenta propia, debiendo cumplir en este caso, lo dispuesto en los Arts. 13-A y 14 de la Ley y 29 de este Reglamento. Asimismo, podrán llevar a cabo dicho almacenamiento contratando los servicios de un proveedor de servicios de almacenamiento de documentos electrónicos. La Unidad definirá y ejecutará planes de educación, sensibilización e impulso en la adopción de firma electrónica tanto en las instituciones del Estado como en población en general, alineados con las estrategias nacionales de transformación digital trazadas por la Presidencia de la República. **Art. 37. Actos de las Entidades del Estado** Las autoridades, funcionarios y empleados del Estado podrán ejecutar o realizar actos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica, con excepción de lo regulado en el inciso segundo del artículo 30 de la Ley. Para tal efecto, los actos administrativos formalizados por medio de documentos electrónicos y que consten en decretos o resoluciones, en acuerdos de órganos colegiados y la emisión de cualquier otro documento que exprese la voluntad de un órgano o servicio público de las entidades del Estado, en ejercicio de sus potestades legales, y los documentos que revistan la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de estos, deberán suscribirse mediante firma electrónica certificada. No obstante, lo anterior, las instituciones públicas podrán celebrar acuerdos o convenios interinstitucionales, dentro de los cuales podrán determinar, entre otros aspectos, el tipo de firma electrónica que habrá de utilizarse en el intercambio de información entre las instituciones involucradas. **Art. 38. Sobre el uso de firmas electrónicas en la relación con los particulares**

		Las personas que se relacionen con las entidades del Estado por medios electrónicos podrán utilizar firma electrónica simple o certificada. **Art. 39.- Utilización de medios electrónicos** Los órganos de la Administración del Estado podrán relacionarse por medios electrónicos con los particulares, cuando éstos hayan consentido esta forma de comunicación. **Art. 40.- De los documentos electrónicos.** Los documentos electrónicos, por su naturaleza, están destinados a ser creados de forma electrónica, desplegar sus efectos desde el ámbito electrónico y archivarse de forma electrónica. **Art. 41.- Certificados electrónicos para servidores públicos** Los certificados electrónicos emitidos a servidores públicos, además de los requisitos previstos en la Ley, deberán contener un apartado en el cual conste el cargo funcional y el nombre de la institución pública para la cual laboran.

Fuente: Normas de los países señalados
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP)