Guinée Equatoriale

Signature et documents électroniques

Loi n°2/2017 du 10 janvier 2017

[*NB - Ley n°2/2017, de fecha 10 de enero, de firma y Documentos Electrónicos*]

Título 1 - De las disposiciones generales

Art.1.- Objeto

La presente Ley tiene por objeto la regulación de la firma electrónica, su creación y eficacia jurídica, así como de los demás documentos electrónicos, de la actividad de prestación de servicios de certificación y de sus prestadores.

Art.2.- Ámbito de aplicación

1. La presente Ley se aplicará a los prestadores de servicios de certificación establecidos en la Republica de Guinea Ecuatorial y a los servicios que los prestadores acreditados o domiciliados en otro Estado ofrezcan a través de establecimiento permanente situado en la Republica de Guinea Ecuatorial, así como el uso de firma y documentos electrónicos en la Administración General del Estado, sus Órganos y Entes Públicos y en las relaciones que mantengan ésta entre sí y con los particulares.

2. Se entenderá que un prestador de servicios de certificación está establecido en la República de Guinea Ecuatorial, cuando su residencia o domicilio social se halle en el territorio de la República de Guinea Ecuatorial, coincidiendo con et lugar en que esta efectivamente centralizado la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

3. Se considerará que está permanentemente situado en la República de Guinea Ecuatorial, cuando disponga de forma continuada y habitual, de instalación o lugar de trabajo en los que realiza toda o parte de su actividad y está establecido conforme a la legislación vigente en la materia.

4. La mera utilización de medios tecnológicos situados en la República de Guinea Ecuatorial no implicará, por si sola, el establecimiento del prestador en la República de Guinea Ecuatorial.

Art.3.- Definiciones

A los efectos de la presente Ley se entenderá por :

a) Firma electrónica : conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante ;

b) Firma electrónica avanzada : aquella firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

c) Firma electrónica reconocida : es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tiene respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita.

d) Firma digital : mecanismo criptográfico que permite detectar y determinar el origen o la entidad generadora del dato o del mensaje y confirmar que el mismo no ha sido alterado, verificando la autenticidad e integridad del dato.

e) Firmante : toda persona que posee un dispositivo de creación de firma electrónica y que actúa en nombre propio o de otra persona física o jurídica a la que representa.

f) Dispositivo de creación de firma electrónica : programa o sistema informático que sirve para aplicar los datos de creación de firma, los cuales son únicos, coma códigos o claves criptográficos privadas o particulares que el firmante utiliza para crear la firma electrónica.

g) Dispositivo de verificación de firma electrónica : programa o sistema informático que sirve para aplicar los datos de verificación de firma, los cuales son como códigos o claves criptográficos públicos que se utilizan para verificar la firme electrónica.

h) Certificado electrónico : todo documente firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firme con el firmante y confirma su identidad.

i) Certificado electrónica reconocido : aquel que fuere expedido por un prestador de servicios de certificación y cumpla con los requisitos de autenticación, verificación y de la comprobación de identidad y demás circunstancias de los solicitantes, así como de la fiabilidad y garantías de los prestadores que los prestan.

j) Fecha electrónica : el conjunto de datos en forma electrónica utilizada como media para constatar el momento en que se ha efectuado una actuación sobre otros datos a los que estén asociados.

k) Declaración de prácticas de certificación : documenta de seguridad que contiene las manifestaciones personales de todo prestador de servicios de certificación, asumiendo y especificando todas sus obligaciones en el proceso de la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, así como las condiciones aplicables, las medidas técnicas y organizativas de seguridad y demás circunstancias para la efectividad de su actividad.

l) Prestador de servicio de certificación : toda persona física o jurídica que expide certificados electrónicas o presta otros servicios en relación con la firma electrónica.

m) Documenta electrónico : la información de cualquiera naturaleza en forma electrónica, archivada en un soporte electrónico con un formato determinado y susceptible de identificación y tratamiento diferenciado.

No obstante lo anterior, para que un documento electrónico tenga la naturaleza de documento público o documento administrativo, éste deberá cumplir los requisitos establecidos en la ley aplicable y, en su casa, la siguiente :

1) Estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial a administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la Ley en cada caso.

2) Ser expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a las disposiciones legales.

3) Ser documentos privados con el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte aplicable.

Art.4.- Valor jurídico del soporte electrónico con datos firmados

1. El soporte en que hallen los datos firmados electrónicamente, será admisible coma prueba documental en juicio. Si se impugnara la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documente electrónico, se procederá a comprobar que trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidas en la Ley para este tipo de certificado, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

2. La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento con firma electrónica reconocida. Si de dichas comprobaciones obtienen un resultado positivo, se presumirá de la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico, siendo los gastos, costes y deudas que origine la comprobación exclusivamente a cargo de quien hubiera

formulado la impugnación y, si hubiere actuado de forma temeraria, se le impondrá una multa dineraria.

3. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estaría a lo dispuesto en el párrafo anterior en consonancia con las disposiciones de la Ley de Enjuiciamiento Civil.

4. Cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta la estipulado entre ellos.

Art.5.- Empleo de la firma electrónica en el ámbito de la Administración General del Estado

1. La Administración General del Estado, con el objetivo de mantener y proteger las garantías de cada procedimiento, podrá establecer las condiciones adicionales a la utilización de la firma electrónica en los procedimientos coma pueden ser la imposición de fecha electrónica sobre los documentos electrónicos entregados en un expediente administrativo.

2. Las condiciones adicionales serán objetivas, proporcionadas, transparentes y no discriminatorias, y no deberán establecerse en la prestación de servicios de certificación al ciudadano cuando intervengan distintas administraciones públicas.

3. El Ministerio de la Función Pública y Reforma Administrativa y el Ministerio de Telecomunicaciones y Nuevas Tecnologías, previo informe del Centro Nacional para la Informatización de la Administración Pública de Guinea Ecuatorial, CNIAPGE, elaborarán las normas que establezcan las condiciones adicionales.

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

Art.6.- Régimen de prestación de servicios de certificación

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrá establecerse restricciones para dichos servicios que procedan de otro Estado.

2. La prestación de servicios de certificación por la Administración General del Estado, sus órganos o Entes Públicos, se realizará con arreglo a los principios de objetividad, trasparencia y no discriminación.

Título 2 - De firma y certificados electrónicos

Capítulo 1 - Del contenido de la firma electrónica y el firmante

Art.7.- Firma electrónica y sus modalidades

1. La firma electrónica constituye un dispositivo o mecanismo electrónico que contiene los datos del firmante y hace posible la expedición de certificados electrónicos. Dichos datos permiten identificar al firmante.

2. Las modalidades de firmas electrónicas establecidas por la presente Ley son : la firma electrónica avanzada, la firma electrónica reconocida y la firma digital.

Art.8.- El firmante

A los efectos de lo dispuesto en el artículo anterior, el firmante es ante todo persona que sea titular o posea un dispositivo o mecanismo electrónico para la creación de firma electrónica, en su nombre propio o en nombre y representación de otra.

Capítulo 2 - Del certificado electrónico y sus efectos

Art.9.- Finalidad del certificado electrónico

1. El certificado electrónico, siendo un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de firma con el firmante, permite verificar, autenticar, comprobar y confirmar su identidad, así coma detectar los cambios habidos en los mismos y determinar el origen o la entidad que haya generado dicho dato o mensaje, según el tipo de certificado y de la firma electrónica.

2. Toda persona física o jurídica podrá solicitar del prestador del servicio de certificación, la expedición de certificados electrónicos conforme a lo dispuesto en la presente Ley, garantizando siempre los derechos y la identidad del firmante.

3. A los efectos de la presente Ley, el certificado electrónico de personas físicas será la referencia o el modelo.

Art.10.- Obtención y utilización de Certificados electrónicos de personas jurídicas

1. Podrán solicitar certificados electrónicos de personas jurídicas, sus administradores y sus representantes legales o voluntarios con poderes bastantes para ello, que no podrán afectar al régimen de representación regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firmas solo podrán ser utilizados cuando se admitan en las relaciones que mantengan las personas jurídicas con la Administración General del Estado, o en la contratación de bienes o servicios que sean propias o concernientes a su actividad o tráfico ordinario. Así mismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán como realizados por la persona jurídica, los actos o contratos en los que su firme se hubiera empleado dentro de los limites previstos en el apartado anterior.

5. Si la firma se utiliza transgrediendo los limites mencionados, la persona jurídica quedará vinculada frente a terceros solo si los asume como propios o se hubieren celebrado en su interés. En casa contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de la firme, quien podrá repetir, en su caso, contra quienes los hubiera utilizado.

6. Lo dispuesto en este artículo no se aplicará a los certificados que sirven para verificar la firma electrónica del prestador de servicios de certificación con la que firma los certificados electrónicos que expida. Tampoco se hará para los certificados que se expidan a favor de la Administración General del Estado.

Art.11.- Extinción de vigencia de los certificados electrónicos

Son causas de extinción de la vigencia de un certificado electrónico :

- a) expiración del periodo de validez que figura en el certificado ;
- b) renovación formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica ;
- c) violación o puesta en peligro de los datos de creación de firme del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero ;
- d) resolución judicial o administrative que lo ordene ;
- e) fallecimiento o la extinción de personalidad jurídica del firmante o del representado, terminación de la representación, incapacidad sobrevenida total o parcial del firmante o de su representado, disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a favor de una persona jurídica ;
- f) cese en la actividad del prestador de servicios de certificación, salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por actual sea transferida a otro prestador de servicios de certificación ;

- g) la alteración de los datos aportados para la obtención del certificado o la modificación de las circunstancias verificadas para la expedición del certificado como las relativas al cargo o a las facultades de representación, de manera que estén disconformes con la realidad ;
- h) cualquier otra causa licita puesta en la declaración de prácticas de certificación.

Art.12.- Periodo de validez de los certificados electrónicos

1. Los certificados electrónicos tendrán la validez de acuerdo a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos, este periodo no podrá ser superior a cuatro años.

2. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su periodo de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Art.13.- Suspensión de la vigencia de certificados electrónicos

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos, si concurre alguna de las siguientes causas :
- a) solicitud del firmante, persona física o jurídica representada por este, un tercero autorizado o la persona física solicitante de un certificado electrónico de una persona jurídica ;
- b) resolución judicial o administrativa que lo ordene ;
- c) la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados previstos en los párrafos c) y g) del artículo 11 de la presente Ley ;
- d) cualquiera otra causa licita prevista en la declaración de prácticas de certificación.

2. La suspensión de vigencia de un certificado electrónico surtirá efecto desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Art.14.- Actuaciones y efectos relativos a la extinción y suspensión de la vigencia de certificados electrónicos

1. El prestador de servicios de certificación hará constar inmediatamente, de forma clara e indudable, la extinción o suspensión de la vigencia de certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes para la extinción o suspensión de su vigencia.

2. A efectos de extinción y suspensión de la vigencia del certificado electrónico, el prestador de servicio de certificación informará al firmante acerca de esta circunstancia de manera previa a simultánea, especificando los motivos, fecha y hora en que se quedará sin efecto dicho certificado electrónico.

3. En caso de suspensión, se indicará, además, la duración máxima, transcurrida la cual, se extinguirá la vigencia del referido certificado electrónico, si no se modifica o se levanta dicha suspensión dentro del plazo indicado.

4. El certificado electrónico en estado de extinción o suspensión se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados hasta la fecha y hora de finalización del periodo inicial de su validez.

5. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

Capítulo 3 - Del certificado electrónico reconocido y su expedición

Art.15.- El certificado electrónico reconocido y su contenido

Todo certificado electrónica reconocido, que fuere expedido por un prestador de servicios de certificación, deberá integrar los siguientes datos :

- a) la indicación de que se expiden coma tales ;
- b) el código identificativo única del certificado.
- c) la identificación del prestador de servicios de certificación que expide el certificado y de su domicilia ;
- d) la firma electrónica avanzada del prestador de servicios de certificación que expide el certificado ;
- e) la identificación del firmante, en el casa de personas físicas, por su nombre y apellidos y su número del Documento de Identidad Personal, y, en el caso de las personas jurídicas, por su denominación o razón social y el número de identificación fiscal ;
- f) los datos de verificación de firma electrónica que correspondan a los datas de creación de firma que se encuentren bajo el control del firmante ;
- g) el inicio y fin del periodo de validez del certificado electrónico ;
- h) el marco y los limites de usa del certificado electrónica, si se fijan ;
- i) los límites del valor de las transacciones para los que puede utilizarse el certificado, si se establecen ;
- j) la indicación de los datos del firmante que actúa en representación de una persona física o jurídica, si el certificado reconocido lo admite. En este caso, se incluirá el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de dicha persona física o jurídica y los datos registrales, en caso de ser obligatoria la inscripción de dicho documenta ;
- k) cualesquiera otros datos, circunstancias y rasgos peculiares del firmante significativos para los fines del certificado, si lo solicita.

Art.16.- Obligaciones previas a la expedición de certificados electrónicos reconocidos

Los prestadores de servicios de certificación, antes de expedir cualquier certificado reconocido, deberán cumplir previamente las siguientes obligaciones :

- a) comprobar la identidad y circunstancias personales del solicitante ;

- b) verificar que la información contenida en el certificado es exacta e indudable y que incluye toda la información necesaria requerida para un certificado electrónico reconocido ;
- c) asegurarse de que el firmante está en posesión de los datos de creación de firma electrónica, los cuales corresponden a los de su verificación ;
- d) garantizar la complementariedad de los datos de creación y verificación de firma electrónica, siempre que ambos sean generados por el prestador de servicios de certificación.

Art.17.- Comprobación de la identidad del solicitante

1. La identificación de la persona física solicitante de un certificado electrónico reconocido requerirá la personación de la misma ante el encargado de verificación y se acreditará mediante el Documento de Identidad Personal, pasaporte o cualquier otro medio admitido en derecho, cuyo régimen de personación o presentación se regirá por lo dispuesto en el procedimiento administrativo.

2. Se podrá prescindir de la personación, a que se refiere el párrafo anterior, si su firma en la solicitud de expedición de certificado reconocido haya sida legitimada por el Notario.

3. La identificación de la persona jurídica requerirá que el prestador de servicios de certificación recabe los datos de constitución, personalidad jurídica y la extensión y vigencia de las facultades del representante del solicitante mediante los documentos públicos que acrediten de forma fehaciente la legalidad de dicha representación y su inscripción en el registro público, si así se exigiere.

4. La comprobación o la identificación, a que se hace referencia en el apartado anterior, también podrá realizarse mediante consulta directa en el registro público en el que estén inscritos los documentos de constitución o de apoderamiento, empleando los medios telemáticos y electrónicos facilitados por dicho registro público.

5. Si el certificado reconocido requiere o admite otras circunstancias personales del solicitante, como su cargo o empleo, pertenencia a un colegio profesional o titulación académica, estas deberán comprobarse mediante los documentos oficiales que las acreditan.

6. No serán exigibles las datos, la identificación y las circunstancias a que se refieren los párrafos anteriores, cuando la identidad y otras circunstancias del solicitante del certificado constan ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que se hubieran utilizado los medios señalados en un periodo de tiempo de dos años, o se utilice un certificado reconocido vigente para la expedición de un otro con idéntico formato y le conste al prestador de servicios de certificación en un periodo de tres meses desde la vigencia de aquel.

7. Las comprobaciones e identificaciones señaladas en los párrafos anteriores podrán realizarse por los prestadores de servicios de certificación por si o por medio de otras

personas físicas o jurídicas, privadas o públicas, en cuyo caso siempre será el responsable.

Art.18.- Equivalencia internacional de certificados electrónicos reconocidos

Los certificados electrónicos expedidos al público por los prestadores de servicios de certificación de otros Estados, como certificados reconocidos, conforme a su legislación aplicable, se considerarán equivalentes a los expedidos por los prestadores de dichos servicios en la República de Guinea Ecuatorial, siempre que cumplan las siguientes condiciones :

- a) que el prestador de servicios de certificación reúna los requisitos legales y la legalidad vigente en dicho Estado sobre la firma electrónica y haya sida expedido conforme a un sistema voluntario de certificación ;
- b) que el prestador de servicios de certificación y el certificado expedido al efecto estén reconocidos en virtud de acuerdos bilaterales o multilaterales o por un organismo internacional ;
- c) que el certificado electrónico reconocido esté garantizado y avalado por un prestador de servicios de certificación establecido en la República de Guinea Ecuatorial.

Capítulo 4 - Del régimen jurídico del documento de Identidad Personal Electrónico

Art.19.- Documento de Identidad Personal Electrónico

1. El Documento de Identidad Personal electrónico es un documento personal que acredita electrónicamente la identidad personal de su titular y le permite o avala la firma electrónica de documentos.

2. Todos los poderes públicos y todas las personas físicas o jurídicas están obligados a reconocer la validez y la eficacia del Documento de Identidad Personal electrónico para acreditar la identidad y los demás datos personales de su titular que consten en el mismo, y para autenticar la identidad del firmante y la integridad de los documentas firmados con los dispositivos de firma electrónica incluidos en dicho documento.

Art.20.- Requisitos para la expedición de Documento de Identidad Personal Electrónico

1. Los órganos públicos competentes para la expedición de Documento Identidad Personal electrónico deberán cumplir las mismas obligaciones previas impuestas por la presente Ley a los prestadores de servicios de certificación que expidan certificados reconocidos, excepta lo relativo a la constitución de la garantía o aval.

2. Para la eficacia del Documento de Identidad Personal electrónico, la Administración General del Estado se queda en la obligación de implementar los sistemas que garanticen la compatibilidad de los instrumentos y medios de firma electrónica incluidos en el Documento de Identidad Personal electrónico con los dispositivos y productos de firma electrónica generalmente aceptados.

3. El procedimiento de expedición del Documenta de Identidad Personal Electrónico sera desarrollado mediante Decreto.

Título 3 - Del sistema de firma electrónica y prestación del servicio de certificación

Capítulo 1 - De los dispositivos de firma electrónica y de su verificación

Art.21.- Dispositivos de creación de firma electrónica

Todo dispositivo de creación de firma electrónica, siendo un programa o sistema informático que sirve para aplicar los datos de creación de firma, deberá cumplir las garantías siguientes :

- a) que asegura razonablemente el secreto de la utilización de los datos para la generación de firma, los cuales puede producirse una sola vez ;
- b) que los datos utilizados para la generación de firma electrónica no pueden ser derivados de los de la verificación de firma o de la propia firma, protegiéndola de cualquier falsificación ;
- c) que los datos de creación de firma electrónica pueden ser protegidos por el firmante de forma fiable en evitación de su uso por terceros ;
- d) que el dispositivo utilizado no altera los datos o el documenta que deba firmarse, ni impide que este muestre al firmante antes del proceso de firma.

Art.22.- Dispositivos de verificación de firma electrónica

Cualquier dispositivo de verificación de firma electrónica, siendo un programa o sistema informático que sirve para aplicar los datos de verificación de firma, deberá cumplir los requisitos siguientes :

- a) que los datos utilizados para verificar la firma correspondan a los mostrados a la persona que verifica la firma ;
- b) que la firma, la autenticidad y validez del certificado electrónico correspondiente se verifiquen de forma fiable y el resultado de esa verificación se presente correctamente ;
- c) que la persona que verifica la firma electrónica pueda establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados ;
- d) que se muestren correctamente la identidad del firmante y et resultado de la verificación ;
- e) que pueda detectarse cualquier cambio relativo a la seguridad.

Art.23.- Certificación de dispositivos seguros de creación de firma electrónica

1. La certificación de dispositivos seguros de creación de firma electrónica será el procedimiento o documenta por el que se comprueba que et dispositivo de creación de firma electrónica cumple los requisitos establecidos en las disposiciones legales vigentes para su consideración como un dispositivo seguro de creación de firma, que será

expedida por una institución pública o privada autorizada y cualificada a solicitud del fabricante o de importador de dichos dispositivos.

2. Los certificados de conformidad de los dispositivos seguros de creación de firma electrónica serán modificados o, en su casa, revocados cuando dejen de cumplir los requisitos y condiciones para su obtención, cuya decisión se comunicará inicialmente al interesado y se hará pública por los medios de comunicación sociales.

Capítulo 2 - De la prestación de servicios de certificación

Art.24.- Certificación del prestador de servicios de certificación

1. La certificación de prestador de servicios de certificación será el procedimiento obligatorio por el que la entidad pública autorizada y cualificada emite un informe o dictamen a favor del prestador de servicios de certificación, a petición de éste, sobre el reconocimiento de sus capacidades y de cumplimiento de los requisitos establecidos para la prestación de dichos servicios, expidiendo el correspondiente certificado.

2. En los procedimientos referidos de certificación podrán utilizarse las normas técnicas y otros criterios que gocen de amplio reconocimiento en este ámbito de actividad y tecnología, que permitan esclarecer y determinar las capacidades del prestador de servicios de certificación que lo solicita.

Art.25.- Obligaciones del prestador de servicios de certificación de certificados electrónicos

Todo prestador de servicios de certificación, que expida certificados electrónicos, deberá cumplir las obligaciones siguientes :

- a) no almacenar ni copiar los datos de creación de firma electrónica de la persona física o jurídica a la que hayan prestado sus servicios ;
- b) proporcionar al solicitante antes de la expedición del certificado electrónico, de forma gratuita y por escrito o por medio electrónico, la información sobre :
  - 1° las obligaciones del firmante en cuanto a la custodia de los datos de creación de firma electrónica, al procedimiento aplicable en la pérdida, suspensión o posible utilización indebida de dichos datos y de determinados dispositivos de creación o verificación de firma electrónica, que sean compatibles con los datos de firma y con el certificado expedido ;
  - 2° los mecanismos para garantizar la fiabilidad de firma electrónica de documentos a lo largo del tiempo ;
  - 3° el método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado electrónico ;
  - 4° las condiciones precisas de utilización del certificado, sus posibles limitaciones de uso y la forma de garantizar la responsabilidad por el prestador de servicios de certificación ;

- 5° las certificaciones que haya obtenido et prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de conflictos que pudieran surgir en el ejercicio de su actividad ;
- 6° las demás informaciones contenidas en la declaración de prácticas de certificación ;
- 7° la información que sea relevante para terceros afectados por los certificados electrónicos deberá estar disponible a instancia de estos.

- a) mantener un directorio actualizado de certificados electrónicos, en el que se indicarán los certificados expedidos, su vigencia, precisando si están ya suspendidos o extinguidos. La integridad del directorio se protegerá mediante la utilización de los mecanismos adecuados de seguridad ;
- b) garantizar la disponibilidad de un servicio rápido y seguro de consulta sobre la vigencia de los certificados electrónicos.

Art.26.- Obligación de protección de datos personales

1. Para la expedición de certificados electrónicos al público y tratamiento de los datos personales, los prestadores de servicios de certificación y los órganos administrativos para el ejercicio de sus funciones, únicamente podrán recabar los datos personales directamente de los firmantes o previo consentimiento expreso de estos, sujetándose a la establecido en la Ley de Protección de Datos Personales.

2. Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado y para la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación solo estarán obligados a revelar la identidad de las firmantes y de sus demás datos personales por requerimiento de la autoridad judicial en el ejercicio de sus funciones legales.

Art.27.- Declaración de prácticas de certificación

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallaran las obligaciones que asumen en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas técnicas y organizativas de seguridad, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su casa, la existencia de procedimientos de coordinación con los registros públicos correspondientes que permitan el intercambio de información de forma inmediata sobre la vigencia de los poderes y facultades recogidos en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación tendrá la consideración de documente de seguridad, conteniendo todos los requisitos legalmente exigidos para dicho documenta, y estará disponible al público de manera accesible, gratuita y por vía electrónica.

Art.28.- Obligaciones del prestador de servicios de certificación, que expida certificado reconocido

Los prestadores enunciados deberán cumplir las siguientes obligaciones :

- a) demostrar la fiabilidad necesaria para prestar el servicio de certificación, constituyendo una garantía de seguro de posible responsabilidad civil en la cuantía que determine el órgano competente para los posibles daños y perjuicios que pudiera causar el usa de los certificados que expida. Dicha garantía de seguro podrá ser sustituida total o parcialmente por un aval bancario o seguro de caución ;
- b) garantizar que puede determinar con precisión la fecha y hora en que se expidió el certificado, o se extinguió o se suspendió su vigencia ;
- c) emplear personal cualificado con conocimiento y experiencia para la prestación de los servicios de certificación y los procedimientos de seguridad y de gestión adecuados en el ámbito de firma electrónica ;
- d) utilizar los sistemas y productos fiables que estén protegidos contra alteraciones y que garanticen la seguridad técnica y, en su caso, criptografía de los procesos de certificación a los que sirven de soporte, así como para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad o introduzcan cambios que afecten a las condiciones de seguridad ;
- e) tomar medidas contra la falsificación de certificados y de garantía de confidencialidad de datos de creación de firma electrónica durante et proceso de su generación y de su entrega por un procedimiento seguro al firmante ;
- f) conservar registrados por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante diez años contados desde la fecha de su expedición, de manera que se pueda verificar las firmas efectuadas en el mismo.

Art.29.- Cese de la actividad de un prestador de servicios de certificación y sus efectos

1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos expedidos por él, así como a los solicitantes de certificados expedidos a favor de personas jurídicas ; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca, a otro prestador de servicios de certificación que los asuma o, en casa contrario, extinguir su vigencia.

2. La comunicación del cese se llevara a cabo con una antelación mínima de tres meses al cese efectivo de la actividad e informará también, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados electrónicos.

3. También deberá comunicar el cese y el destino de la gestión de los certificados al Ministerio Telecomunicaciones y Nuevas Tecnologías, y a la autoridad autorizada y cualificada, con una antelación de tres meses, que mantendrá accesible al público un servicio de consulta especial y temporal, donde figurará la indicación sobre dichos certificados durante el periodo que estime suficiente.

Capítulo 3 - De la responsabilidad del prestador de servicios de certificación

Art.30.- Responsabilidad de los prestadores de servicios de certificación

1. Los prestadores de servicio de certificación responderán por los daños y perjuicios que causen a cualquier persona física o jurídica en el ejercicio de su actividad, cuando no cumplan las obligaciones contractuales ; en especial, por los perjuicios causados al firmante o a terceros de buena fe por falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados, de la extinción o suspensión de la vigencia de certificado electrónico, así como por la actuación de las personas en las que deléguenla realización de alguna de sus funciones.

2. La responsabilidad referida en el apartado anterior será exigible conforme a los acuerdos y cláusulas contractuales y extracontractuales, correspondiendo al responsable probar que actuó con la diligencia profesional debida. Dicha responsabilidad se entiende sin perjuicio de lo establecido en las leyes vigentes en la materia.

3. Si el prestador de servicios de certificación incumpliere las obligaciones derivadas de la garantía de un certificado electrónico expedido por un prestador de servicios de certificación establecido fuera de la República de Guinea Ecuatorial, será responsable por los daños y perjuicios causados por el usa de dicho certificado.

Art.31.- Limitaciones de la responsabilidad de los prestadores de servicios de certificación

Todo prestador de servicios de certificación no será responsable de los daños y perjuicios causados al firmante o a terceros, si se dan los siguientes supuestos :

- a) no haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición, extinción o suspensión de la vigencia, cuando no se haya podido ser detectado por dicho prestador ;
- b) la falta de comunicación sin la demora del prestador de servicios de certificación, de cualquier dato o circunstancia reflejado en el certificado electrónico ;
- c) negligencia no imputable al prestador en la conservación de los datos de creación de firma electrónica, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación ;
- d) no solicitar la suspensión o revocación del certificado electrónico en casa de duda en cuanto al mantenimiento de la confidencialidad de los datos de creación de firma electrónica ;

- e) la inexactitud derivada de los datos que constan en un documento público ;
- f) utilizar los datos de creación de firma electrónica fuera del periodo de validez del certificado electrónico o tras la notificación de la extinción o suspensión de su vigencia por el prestador de servicios de certificación ;
- g) superar los límites establecidos para el uso del certificado electrónico o para el importe individualizado de las transacciones que puedan realizarse con él, o no utilizarlo conforme las condiciones fijadas ;
- h) la no solicitud de la revocación o suspensión de la vigencia del certificado electrónico que contenga poder de representación.
- i) cuando el destinatario de los documentos firmados electrónicamente actúa de forma negligente sin comprobar ni tener en cuenta las restricciones previstas en el certificado electrónica sobre sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con el, y la suspensión o pérdida de vigencia publicada en el servicio de consulta sobre la vigencia del certificado o falta de verificación de firma electrónica.

Art.32.- La obligación de probar la actuación diligente

La exención de la responsabilidad frente a terceros, a que se refiere el artículo anterior, obliga al prestador de servicio de certificación probar y justificar que no actúa de forma negligente.

Título 4 - Del régimen sancionador y órganos competentes

Capítulo 1 - De las infracciones y sus sanciones

Art.33.- Infracciones

Las infracciones tipificadas por la presente Ley se clasifican leves, graves y muy graves.

1. Son infracciones leves :
- a) el incumplimiento negligente de las obligaciones establecidas en relación a la expedición de certificados electrónicos y certificados electrónicos reconocidos en esta Ley, siempre que no se hayan causado daños graves a los usuarios, o la seguridad de los servicios de certificación se haya visto afectada, y siempre y cuando que tal incumplimiento no fuera constitutivo de una infracción grave ;
- b) el incumplimiento negligente de las obligaciones derivadas del cese de su actividad o la producción negligente de circunstancias que impidan la continuación de dicha actividad ;
- c) la presentación negligente de la información solicitada por el Ministerio de Telecomunicaciones y Nuevas Tecnologías o por la Autoridad publica autorizada y cualificada en su función inspectora ;
- d) el cumplimiento negligente de las obligaciones en relación a la protección de datos personales recogidas de forma general en esta Ley y particularmente en el artículo 26, cuando no sean constitutives de una infracción grave ;

- e) cualesquiera otras que no sean constitutivas de infracción grave.

2. Son infracciones graves :
- a) el incumplimiento de las obligaciones establecidas en relación a la expedición de certificados electrónicos y certificados electrónicos reconocidos en esta Ley, siempre que se haya causado daños graves a los usuarios, o la seguridad de los servicios de certificación se haya visto gravemente afectada, y siempre y cuando que tal incumplimiento no fuera constitutivo de una infracción muy grave ;
- b) la falta de constitución de la garantía económica prevista en esta Ley ;
- c) el incumplimiento de las obligaciones derivadas del cese de su actividad o la producción de circunstancias que impidan la continuación de dicha actividad ;
- d) la resistencia, excusa, obstrucción o negativa injustificada de la actuación inspectora de los órganos competentes de supervisión y control.
- e) la falta de presentación de la información solicitada por el Ministerio de Telecomunicaciones y Nuevas Tecnologías o por la Autoridad publica autorizada y cualificada en su función inspectora ;
- f) la expedición de certificados reconocidos sin realizar la correspondiente comprobación previa, cuando aquello afecte a una parte relativamente pequeña de los certificados reconocidos expedidos ;
- g) el incumplimiento de las resoluciones dictadas por el Ministerio de Telecomunicaciones y Nuevas Tecnologías para el buen funcionamiento de los servicios y sistemas de certificaciones, así como en relación a cualquier aspecto dentro del objeto de la presente Ley ;
- h) el incumplimiento de las obligaciones en relación a la protección de datos personales recogidas de forma general en esta Ley y particularmente en el artículo 26, cuando no sean constitutivas de una infracción muy grave ;
- i) la comisión de tres infracciones leves en et transcurso de un año.

3. Son infracciones muy graves :
- a) el incumplimiento de las obligaciones establecidas en relación a la expedición de certificados electrónicos y certificados electrónicos reconocidos en esta Ley, salvo la obligación de constitución de garantía económica, siempre que se haya causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectadas ;
- b) la expedición de certificado reconocido sin realizar la correspondiente comprobación previa, cuando aquello afecte a la mayoría de certificados reconocidos expedidos ;
- c) el incumplimiento de las obligaciones en relación a la protección de datos personales recogidas de forma general en esta Ley y particularmente en et artículo 26 ;
- d) la comisión de dos o más infracciones graves en un periodo de un año.

Art.34.- Sanciones

I) Por la comisión de las infracciones recogidas en esta Ley se impondrán las siguientes sanciones :
- 1. por las infracciones leves se impondrá una o varias de las siguientes medidas :

- a) amonestación ;
- b) advertencia por escrito ;
- c) multa por un importe de hanta 5.000.000 FCFA ;
- d) rectificación, en todo caso, de la situación creada coma consecuencia de la infracción, si ello fuera posible.

- 2. por las infracciones graves se impondrá una o varias de las siguientes medidas :
  - a) suspensión de la actividad objeto de la infracción y, en su caso, otras conexas, por un periodo de tiempo no superior a un año ;
  - b) inhabilitación de las personas responsables de la infracción por un periodo de tiempo no superior a dos años ;
  - c) suspensión o pérdida de la vigencia de los certificados afectados gravemente por la seguridad de los sistemas empleados por el prestador de servicios de certificación ;
  - d) multa por un importe entre 5.000.001 FCFA y 25.000.000 FCFA.
- 3. por las infracciones muy graves se impondrá una o varias de las siguientes medidas :
  - a) suspensión de la actividad objeto de la infracción y, en su caso, otras conexas, por un periodo de tiempo superior a un año e inferior a cuatro años ;
  - b) inhabilitación de las personas responsables de la infracción por un periodo de tiempo superior a dos años e inferior a cuatro años ;
  - c) suspensión o pérdida de la vigencia de las certificados afectados gravemente por la seguridad de los sistemas empleados por el prestador de servicios de certificación ;
  - d) multa por un importe entre 25.000.001 FCFA y 100.000.000 FCFA ;
  - e) incautación de equipos y demás material en las instalaciones del prestador ;
  - f) clausura definitiva del local y de las instalaciones.

II) La comisión de dos o más infracciones muy graves en el plazo de tres años podrá dar lugar, en función de los criterios de graduación del Articulo siguiente, a la sanción de prohibición de actuación en la República de Guinea Ecuatorial durante un tiempo máxima de dos años, al prestador, así como a las personas físicas responsables de la infracción.

III) Las sanciones por las infracciones derivadas del incumplimiento de las obligaciones en relación a la protección de datos personales recogidas de forma general en esta Ley y particularmente en el artículo 26, así como las contempladas en la Ley Orgánica sobre la Protección de datos Personales, se sancionarán de acuerdo a lo establecido en esta última Ley.

IV) Las sanciones graves y muy graves podrán llevar aparejadas, a costa del sancionado, la publicación de la resolución sancionadora por los medios informativos nacionales o en el Boletín Oficial del Estado, una vez que aquella tenga carácter firme.

Para la imposición de esta sanción se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

Art.35.- Graduación de las sanciones

Las sanciones previstas en el artículo anterior, que se impongan a los infractores, se graduarán atendiendo a los criterios siguientes :

- a) la intencionalidad ;
- b) la reincidencia y reiteración por la comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme ;
- c) la naturaleza y cuantía de los prejuicios causados ;
- d) el tiempo durante el que se haya venido cometiendo la infracción ;
- e) el beneficio que haya obtenido el infractor por dicha infracción ;
- f) el volumen de la facturación a que afecte la infracción cometida.

Art.36.- Medidas cautelares

1. En el procedimiento sancionador por infracciones graves y muy graves, el Ministerio de Telecomunicaciones y Nuevas Tecnologías, previo informe de la Autoridad pública autorizada y cualificada, podrá adoptar las medidas cautelares que estime necesarias para asegurar la eficacia de sus resoluciones, el buen fin del procedimiento y evitar el mantenimiento de los efectos de la infracción. Así mismo podrá acordar las siguientes medidas cautelares :

- a) suspensión provisional de la actividad del prestador de servicios o cierre temporal de sus establecimientos ;
- b) precinto, depósito o incautación de registras, soportes y archivos informáticos y de documentas en general, así como de aparatos y equipos informáticos de todo tipo por un periodo de tiempo no superior a seis meses ;
- c) la suspensión o pérdida de vigencia de los certificados afectados gravemente por la seguridad de los sistemas empleados por el prestador de servicios de certificación ;
- d) advertencia al público de la existencia de posibles conductas irregulares del prestador, de la incoación del expediente sancionador y de las medidas adoptadas para el cese de dichas conductas.

2. En la adopción de las medidas indicadas se respetarán las normas, garantías y procedimientos previstos por la legislación vigente sobre la protección de los datos personales y de la intimidad personal y familiar, así como el principio de proporcionalidad de la medida a adoptar con los objetivos a alcanzar.

3. En caso de urgencia y para la inmediata protección de los intereses implicados, las referidas medidas cautelares podrán ser adoptadas antes del inicio del expediente sancionador, y deberán ser confirmadas, modificadas o levantadas en el acuerdo o resolución de iniciación de procedimiento dentro de los diez días siguientes de su adopción. El referido acuerdo o resolución podrá ser objeto del recurso que proceda, cuya admisión a trámite suspende las actuaciones en el estado en que se encuentren.

4. Dichas medidas quedarán sin efecto, si no se inicia el procedimiento sancionador dentro del plazo señalado en el párrafo anterior o no baya pronunciamiento expreso sobre las medidas adoptadas.

Art.37.- Procedimiento sancionador

1. Corresponde al Ministro de Telecomunicaciones y Nuevas Tecnologías, la protestad sancionadora establecida en esta Ley por las infracciones muy graves y graves, previa incoación del correspondiente expediente por la Dirección General de Nuevas Tecnologías, o en su casa por la Autoridad pública autorizada y cualificada.

2. Por las infracciones leves, la protestad sancionadora corresponderá a la Autoridad pública autorizada y cualificada, con notificación al Ministerio de Telecomunicaciones y Nuevas Tecnologías.

3. Las Resoluciones dictadas por el Ministro de Telecomunicaciones y Nuevas Tecnologías en el procedimiento sancionador deberán ser motivadas y fundamentadas, contra las cuales procederá recurso de alzada ante el Consejo de Ministros dentro del término de treinta días desde la fecha de la notificación de la misma.

Capítulo 2 - De los órganos competentes

Art.38.- Competencia ministerial

1. El Ministerio de Telecomunicaciones y Nuevas Tecnologías, en el marco de sus funciones legales, ejercerá las siguientes competencias :

- a) controlar el cumplimiento de las obligaciones establecidas en esta Ley y las demás disposiciones legales por parte de los prestadores de servicios de certificación que expidan certificados electrónicos al público ;
- b) supervisar el funcionamiento de los sistemas de certificación de dispositivos seguros de creación de firma electrónica y de las instituciones autorizadas para su expedición.
- c) adoptar las medidas necesarias para el cumplimiento de las obligaciones contraídas por el prestador de servicios de certificación y por las instituciones autorizadas para expedición de certificación de dispositivos seguros de creación de firma, así coma de las disposiciones de la presente Ley ;
- d) cualesquiera otras competencias derivadas de las anteriores no previstas por la legislación vigente.

2. La Autoridad pública autorizada y cualificada será el órgano competente para supervisar y controlar técnicamente todos los procesos de prestación de servicios de certificación.

Art.39.- Deber de información y colaboración

Todo prestador de servicios de certificación, institución o particular interesado tiene la obligación de facilitar al Ministerio de Telecomunicaciones y Nuevas Tecnologías y a la Autoridad pública autorizada y cualificada, todo tipo de información y colaboración necesarias para el ejercicio de sus funciones, en especial :

- a) comunicar el inicio de su actividad, sus datos de identificación, inclusive la fiscal y registral, los datos de comunicación, inclusive el nombre de dominio de Internet, los

de atención al público, las características de los servicios a prestar y las certificaciones correspondientes ;

- b) actualizar periódicamente la información indicada en el punto anterior y publicarla en la dirección de Internet de dicho Ministerio ;
- c) permitir a sus agentes o personal inspector el acceso a sus instalaciones y a la consulta de cualquier documentación e información.

2. Cuando de una actuación inspectora se tuviera conocimiento de hechos que pudieran constituir infracciones tipificadas en otras leyes, se dará cuenta de los mismos al órgano competente de supervisión y control y al Ministerio Fiscal para los correspondientes efectos.

Disposición adicional

Se faculta al Gobierno dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de la presente Ley.

Disposiciones transitorias

Primera : Mientras no se haya establecido los sistemas electrónicos de Documento de Identidad Personal electrónico en los servicios públicos de la Administración Pública, se seguirá utilizando las copias o fotocopias de los originales en los procedimientos y tramitaciones de la Administración pública electrónica.

Segunda : Mientras no se haya constituido la Autoridad pública autorizada y cualificada de certificación, ni atribuidas sus funciones a otro órgano concreto, se designa al Centro Nacional para la informatización Publica de Guinea Ecuatorial, CNIAPGE, de modo transitorio y por un periodo improrrogable de un año, ejercer las funciones certificadoras de dicha entidad.

Disposición derogatoria

Quedan derogadas cuantas disposiciones de igual e inferior rango se opongan a la presente Ley.

Disposición final

La presente Ley entrará en vigor a los noventa días de su publicación en el Boletín Oficial del Estado y en los medios informativos nacionales.