



República de Guinea Ecuatorial

# BOLETÍN OFICIAL DEL ESTADO

## Leyes Electrónicas

### RESUMEN:

- 1) *Ley Núm. 3/2.015, de fecha 28 de Mayo, de Régimen de Acceso a los Servicios Públicos de la Administración General del Estado por Medios Electrónicos. Pág. 2-15*
- 2) *Ley Núm. 1/2.016, de fecha 22 de Julio, de Protección de Datos Personales. Pág. 15-29*
- 3) *Ley Núm. 2/2.016, de fecha 22 de Julio, de Conservación de Datos en las Comunicaciones Electrónicas y Redes de Comunicación. Pág. 29-34*
- 4) *Ley Núm. 1/2.017, de fecha 10 de Enero, de Comunicaciones Por Internet en la República de Guinea Ecuatorial. Pág.35-52*
- 5) *Ley Núm. 2/2.017, de fecha 10 de Enero, de Firma y Documentos Electrónicos. Pág.52-68*

**IMPRIME:**  
Dirección General del B.O.E.  
Presidencia del Gobierno  
Malabo II  
3ª Planta

***Ley Núm. 3/2.015, de fecha 28 de Mayo, de Régimen de Acceso a los Servicios Públicos de la Administración General del Estado por Medios Electrónicos.***

### **EXPOSICIÓN DE MOTIVOS:**

Las tecnologías de la información y comunicación están afectando muy profunda e intensivamente a la forma y al contenido de las relaciones de las personas y de las sociedades de las que forman parte integrante, y constituyen el rasgo característico del desarrollo y evolución de la humanidad. En este sentido, la Administración General del Estado tiene la obligación de promover todos los medios y recursos necesarios para el uso de las Nuevas Tecnologías en beneficio de los ciudadanos, ya que estos han de ser y son los principales beneficiarios de sus resultados, cuando la Administración General del Estado se transforme en una Administración Electrónica basada en los principios de transparencia, eficacia, eficiencia, proximidad o cercanía, accesibilidad y objetividad; comprometiéndose a ofrecer a los ciudadanos las ventajas y posibilidades que tiene y presente la sociedad de la información y comunicación.

La presente Ley, al consagrar y confirmar el derecho de los ciudadanos a relacionarse con la Administración General del Estado, sus Órganos y Entes Autónomos por medios electrónicos y la obligación de esos, de garantizarlo y hacerlo efectivo, está materializando la previsión de la Ley de Procedimiento Administrativo sobre la utilización de registros informáticos en la actividad administrativa, implicando al propio ciudadano en el proceso de automatización e informatización de la Administración General ecuatoguineana, y estableciendo un nuevo marco jurídico, que desarrolla y garantiza los derechos y libertades previstos en el Artículo 13 de la Ley Fundamental e incorpora a nuestro Ordenamiento Jurídico vigente nuevos conceptos y términos como: la Administración Electrónica, aplicación de fuentes abiertas, autenticación, documento electrónico, sedes y direcciones electrónicas, Interoperabilidad, firma electrónica, Documento de Identidad Personal Electrónico, Ventanilla y otros.

Teniendo en cuenta que las transformaciones que ha experimentado la Administración General Ecuatoguineana, han permitido conseguir resultados positivos en el funcionamiento de sus diferentes Órganos, Instituciones y Entes Autónomos; sin embargo, aquella, al no ser una estructura estática, siempre requiere una atención especial y nuevos diseños para su modernización y actualización, lo que se pretende alcanzar con la implantación e introducción de la Administración Electrónica, que debe implicar e implica la innovación y la aplicación de nuevos métodos, técnicas y procedimientos administrativos, que conlleven la simplificación de muchos de los actuales procedimientos administrativos, materializando así las Resoluciones Sectoriales del Acta Final de la Segunda Conferencia Económica Nacional, en su punto 19.2.7.-b. y su adaptación normativa concordante con los principios de la Ley Fundamental.

En estas circunstancias, la presente Ley tiene por finalidad la regulación exclusiva del Régimen de Acceso Electrónico del ciudadano al Servicio Público de la Administración General del Estado, estableciendo y regulando el régimen jurídico de las comunicaciones electrónicas de la Administración Pública Ecuatoguineana, su naturaleza, eficacia, validez y vigencia, ya que con ello se propone alcanzar las mejores cotas de buena gobernabilidad en todas las esferas de la vida de la sociedad ecuatoguineana.

La presente Ley se estructura en siete (7) Títulos, repartidos en catorce (14) Capítulos, cincuenta y tres (53) Artículos, dos (2) Disposiciones Adicionales, una (1) Transitoria, una (1) Derogatoria y una (1) Final.

En su virtud, a propuesta del Gobierno, y debidamente aprobada por la Cámara de los Diputados y el Senado en su Segundo Periodo Ordinario de Sesiones celebrada en la Ciudad de Bata, del 31 de Julio al 27 de Noviembre del pasado año 2.014, y de conformidad con las prerrogativas que Me confiere el Artículo 40 de la Ley Fundamental, Vengo en Sancionar la presente

***Ley de Régimen de Acceso a los Servicios Públicos de la Administración General del Estado por Medios Electrónicos.***

**TÍTULO I  
DE LAS DISPOSICIONES GENERALES**

**Artículo 1. Objeto.** La presente Ley tiene por objeto el reconocimiento del derecho de los ciudadanos a relacionarse con la Administración General, sus Órganos y Entes por Medios Electrónicos y la regulación de la utilización de las tecnologías de información y comunicación en los procesos y actividades administrativos, en las relaciones entre los diferentes Órganos y Entes de la Administración General del Estado y entre ésta y los ciudadanos con el objetivo de garantizar sus derechos, libertades e intereses, un tratamiento común ante la misma y la validez y eficacia de la actividad administrativa en condiciones de igualdad y seguridad jurídica.

**Artículo 2. Ámbito de Aplicación.** La presente Ley será de aplicación:

- a) A la Administración General del Estado, a las Corporaciones Locales y a los Entes del Derecho Público dependientes de la misma.
- b) A los ciudadanos en sus relaciones con la Administración General del Estado.
- c) A las relaciones entre los diferentes Órganos y Entes de la Administración General del Estado.

**Artículo 3. Exclusión.** La presente Ley no se aplicará a las actividades y relaciones que la Administración General desarrolle y realice en régimen del derecho privado.

**Artículo 4. Principios Generales.** La utilización de las tecnologías de la información y comunicación tendrá la finalidad de facilitar a los ciudadanos el ejercicio de sus derechos y el cumplimiento de sus deberes cívicos por los medios electrónicos, su acceso a la información y a los procedimientos administrativos con la simplificación de estos, la eliminación de las dificultades u obstáculos que se encuentran en los mismos, y

la mejora del funcionamiento de la Administración General en su eficacia, transparencia, confidencialidad y confianza, respetando siempre los derechos y libertades de los ciudadanos, acatando las Leyes vigentes.

Los principios a que se ajusta la presente Ley son los siguientes:

- a) El respeto del derecho al Honor, Dignidad, a la Intimidad, Integridad y a la Protección de Datos Personales y Familiares.
- b) La transparencia y publicidad de procedimientos, facilitando la máxima difusión y publicidad de las actuaciones administrativas.
- c) La igualdad de todos los ciudadanos que se relacionan con la Administración General por los Medios Electrónicos o no, evitando siempre cualquier acto o actuación de discriminación o restricción de los derechos y libertades de aquellos, tanto respecto al acceso a la prestación de los servicios públicos como en cualquier otra actuación o procedimiento administrativo.
- d) La simplificación de los procedimientos administrativos, reduciendo los plazos y términos de los mismos para la efectividad y eficacia de la actividad administrativa.
- e) La responsabilidad y calidad en la veracidad y autenticidad en las informaciones y servicios prestados por la Administración General del Estado a través de los Medios Electrónicos.
- f) La accesibilidad universal a la información y a los servicios públicos por Medios Electrónicos a través de sistemas y aplicaciones seguros, compresibles y fáciles.
- g) La legalidad en la utilización de Medios Electrónicos, velando en todo momento por la seguridad e integridad de las garantías jurídicas de los ciudadanos ante la Administración General del Estado.
- h) La seguridad jurídica en la organización, implementación y uso de los Medios Electrónicos por la Administración General del Estado, evitando la disonancia con

la utilización de los Medios Electrónicos en la actividad administrativa.

- i) La neutralidad tecnológica y de adaptabilidad a las nuevas tecnologías, técnicas y sistemas de comunicaciones electrónicas, garantizando los avances tecnológicos y la elección de las alternativas tecnológicas por los ciudadanos y utilizando los estándares abiertos y de uso generalizado por ellos.
- j) La proporcionalidad de las garantías y medidas de seguridad adecuadas a la naturaleza y a las circunstancias de los trámites y actuaciones administrativas, requiriendo a los ciudadanos los datos estrictamente necesarios al servicio solicitado.

**Artículo 5. Definiciones.** A los efectos de esta Ley y sin carácter limitativo se entenderá por:

- a) **Actuación Administrativa Automatizada:** Aquella que es producida por un Sistema de Información Técnica adecuadamente programado, que incluya la generación o realización de actos resolutorios o de mera comunicación de procedimientos administrativos.
- b) **Aplicación de Fuentes Abiertas:** Aquella que se distribuye con una Licencia que permite ejecutarla, conocer el Código de Fuente, modificarla o mejorarla y redistribuir copias a otros usuarios.
- c) **Autenticación:** Acreditación por medios electrónicos de la identidad de una persona física o jurídica, del contenido de la voluntad expresada en documentos, operaciones, transacciones y de integridad y autoría de éstos.
- d) **Canales:** Estructuras o medios de difusión de los contenidos, servicios e informaciones por vía electrónica, telefónica, presencial y por otros medios y dispositivos.
- e) **Ciudadano:** Cualquier persona física o jurídica y Entes sin personalidad jurídica que mantenga relación con la Administración General del Estado.
- f) **Correo Electrónico:** Mensaje de texto, voz, sonido o gráficos enviado a través de

una red pública de comunicaciones, que puede ser almacenado en la red o en el equipo terminal del receptor hasta que se recoja.

- g) **Dirección Electrónica:** Identificación de un equipo o sistema electrónico desde el cual se provee de información o servicios en una red de comunicaciones.
- h) **Documento Electrónico:** Toda información de cualquier naturaleza en forma electrónica, almacenada o archivada en un soporte electrónico con formato determinado y susceptible de identificación y tratamiento diferenciado.
- i) **Estándar Abierto:** Aquél que sea público y su uso o utilización sea disponible de manera gratuita o no suponga una dificultad de acceso y su aplicación no esté condicionado a pago alguno del derecho de Propiedad Intelectual o Industrial.
- j) **Interoperabilidad:** Capacidad de los sistemas de información y de los procedimientos a los que estos dan soporte, de compartir datos e informaciones y posibilitar el intercambio de los mismos y de conocimientos entre ellos.
- k) **Medio Electrónico:** Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, así como las redes de comunicación abiertas o restringidas como Internet, Telefonía fija y móvil y otras.
- l) **Punto de Acceso Electrónico:** Conjunto de páginas web agrupadas en un dominio de Internet, cuyo objetivo es ofrecer al usuario el acceso a recursos y servicios dirigidos a resolver las necesidades de un grupo de personas o el acceso a la información de una Institución u Órgano Público.
- m) **Sistema de Firma Electrónica:** Conjunto de elementos intervinientes en la creación de una firma electrónica. En caso de Firma Electrónica basada en un Certificado Electrónico, componen el sistema, al menos, el Certificado Electrónico, el soporte, el lector, la aplicación de firma uti-

lizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

- n) **Sellado de Tiempo:** Acreditación de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medio electrónico.
- o) **Espacios Comunes o Ventanillas Únicas:** Modos o canales (oficinas integradas, atención telefónica, página de Internet y otros), a los que los ciudadanos pueden dirigirse para acceder a las informaciones, trámites y servicios públicos determinados por acuerdo entre las Administraciones.
- p) **Actividad de Servicio:** Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.
- q) **Prestador de Actividad de Servicio:** Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

## TÍTULO II

### PARTES EN EL ACCESO A LOS SERVICIOS PÚBLICOS POR MEDIOS ELECTRÓNICOS

#### CAPÍTULO I DE LOS CIUDADANOS

**Artículo 6. Naturaleza y significado del Ciudadano.** A los efectos de la presente Ley, por Ciudadano se entenderá toda persona física o jurídica que solicite de la Administración General del Estado, la prestación de algún servicio público por Medios Electrónicos.

**Artículo 7. Derechos de los Ciudadanos.** Se reconoce a los Ciudadanos el derecho a relacionarse con la Administración General del Estado utilizando los medios electrónicos para el ejercicio de los derechos previstos en las disposiciones legales reguladas de la actividad administrativa. En especial, los Ciudadanos gozarán de los siguientes derechos:

- a) Al acceso a la información sobre los procedimientos y trámites aplicables, así como sobre los datos de las autoridades

competentes en materia de prestación de servicios públicos.

- b) A la obtención de la información deseada de la Administración General del Estado.
- c) A elegir cualquier canal disponible, sistemas y aplicaciones para relacionarse por Medios Electrónicos con la Administración General del Estado.
- d) A la realización de peticiones, solicitudes, pagos, transacciones y consultas.
- e) A la igualdad en el acceso electrónico a los servicios públicos.
- f) A la formulación de quejas, pretensiones y alegaciones, y la interposición de acciones y recursos contra las resoluciones y actos administrativos.
- g) A no aportar los datos, informaciones y documentos personas, que obren en poder de la Administración General del Estado, la cual utilizará los Medios Electrónicos para recabarlos, cuando cuente con el consentimiento del interesado para ello.
- h) A la manifestación voluntaria de consentimiento y declaración de voluntad.
- i) A conocer por Medios Electrónicos el estado de tramitación de los procedimientos, en los que sea interesado, salvo que la Ley establezca limitaciones para el acceso a dicha información.
- j) A obtener los medios de identificación electrónica necesarios, los documentos electrónicos y sus copias electrónicas, utilizando cualquier sistema de Firma Electrónica admitido por la Administración General.
- k) A la conservación en formato electrónico por la Administración General del Estado de los documentos electrónicos que formen parte de un expediente.
- l) A la calidad de servicios públicos prestados por Medios Electrónicos.
- m) A la garantía de seguridad y confidencialidad de los datos e informaciones, que figuren en los ficheros, sistemas, soportes y aplicaciones de la Administración General del Estado.
- n) A obtener y conocer por Medios Electrónicos los trámites y procedimientos necesarios y aplicables para el establecimiento

de las actividades de servicio, el acceso a las mismas y a su ejercicio.

- o) A conocer los datos de las autoridades competentes en materia de actividades de servicios, así como de las Asociaciones Profesionales, Organizaciones e Instituciones o Entes relacionados con las mismas.
- p) A informarse sobre los medios y condiciones de acceso a los registros y Bases de Datos Públicos relativos a los prestadores de servicios y las vías de recurso en caso de litigio entre autoridades, prestadores de servicios y destinatarios o usuarios.

**Artículo 8. Protección de los Derechos del Ciudadano.** Corresponderá al Defensor del Pueblo la Defensa y Protección de los Derechos de los Ciudadanos en el proceso de la utilización de Servicios Públicos por Medios Electrónicos, quien anualmente elaborará un informe sobre las quejas y sugerencias recibidas en el año anterior y las propuestas de mejora de la prestación de servicios, que elevará al Parlamento.

## **CAPÍTULO II DE LA ADMINISTRACIÓN GENERAL**

**Artículo 9. Concepto.** A los efectos de la presente Ley, se entiende por Administración General del Estado todas las Administraciones Públicas de la República de Guinea Ecuatorial.

**Artículo 10. Responsabilidad de la Administración General.**

**10.1.** La Administración General del Estado en la utilización de las tecnologías de la información y comunicación, asegurará y garantizará la disponibilidad, el acceso, la autenticidad, la integridad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestiona y administra en el ejercicio de sus competencias.

**10.2.** A los efectos de lo dispuesto en el párrafo anterior, la Administración General del Estado queda obligada a:

- a) Recabar y difundir la información a la que se refiere esta Ley.

- b) Recibir y dar tramitación a las solicitudes de acceso a la información.
- c) Realizar el seguimiento y control de la correcta tramitación de las solicitudes de acceso a la información.
- d) Llevar un registro de las solicitudes de acceso a la información.
- e) Asegurar la disponibilidad en la respectiva página web o sede electrónica de la información cuyo acceso se solicita con más frecuencia.
- f) Mantener actualizado un mapa de contenidos en el que queden identificados los distintos tipos de informaciones que obren en poder del órgano.
- g) Todas aquellas que sean necesarias para asegurar una correcta aplicación de las disposiciones de esta Ley.

**Artículo 11. Garantía de Prestación de Servicios.** La Administración General del Estado deberá habilitar diferentes canales o medios electrónicos para la prestación de servicios electrónicos, garantizando el acceso a los mismos a todos los ciudadanos sin discriminación alguna con un sistema de varios canales, que cuente con Oficinas de Atención Presencial, Puntos de Acceso Electrónico y Servicio de Atención Telefónica.

**Artículo 12. Oficinas de Atención Presencial.** Las Oficinas de Atención Presencial pondrán a disposición de los ciudadanos de forma libre y gratuita, los medios necesarios para el ejercicio de sus derechos, orientándoles sobre su utilización por el personal de la propia oficina.

**Artículo 13. Puntos de Acceso Electrónico.** Los Puntos de Acceso Electrónico, que serán Sedes Electrónicas gestionadas por los Departamentos Ministeriales y por Entes Públicos, estarán disponibles para los ciudadanos a través de Redes de Comunicación, actuando de coordinación el Punto de Acceso General, a través del cual los ciudadanos pueden acceder a toda la información y a los servicios disponibles en sus relaciones con la Administración General del Estado, y contendrá la relación de todos los servicios existentes y el acceso a los mismos.

**Artículo 14. Servicio de Atención Telefónica.** Los Servicios de Atención Telefónica facilitan a los ciudadanos el acceso a las informaciones y a los servicios electrónicos prestados por la Administración General del Estado.

**TÍTULO III  
RÉGIMEN JURÍDICO DE LA  
ADMINISTRACIÓN GENERAL  
ELECTRÓNICA**

**CAPÍTULO I  
DE LA DIRECCIÓN ELECTRÓNICA**

**Artículo 15. Sede Electrónica.** 1. La Sede Electrónica será aquella Dirección Electrónica disponible para los ciudadanos a través de redes de telecomunicación, cuya titularidad, gestión y administración corresponden a la Administración General del Estado, a un Órgano o Ente de la misma en el marco del ejercicio de sus competencias, y dispone de sistemas que permitan el establecimiento de comunicaciones seguras y permanentes.

2. El establecimiento de una Sede Electrónica conlleva la responsabilidad de su titular sobre la integridad, veracidad, confidencialidad y actualización de la información y de los servicios que se prestan en la misma.

3. Las Sedes Electrónicas utilizarán, para su identificación y garantía de una comunicación segura y confidencial con las mismas, los sistemas de firma electrónica basados en Certificados de Dispositivo seguro o medio equivalente.

4. La publicación de datos, informaciones, servicios y transacciones en las Sedes Electrónicas deberá respetar los principios de accesibilidad y usabilidad, conforme a las normas establecidas, estándares abiertos y usos generalizados por los ciudadanos.

**Artículo 16. Publicación Electrónica del Boletín Oficial del Estado y de los Tablones de Anuncios.** La publicación del Boletín Oficial del Estado, de las Revistas Departamentales e Instituciones y de los Tablones de Anuncios de Actos y Comunicaciones en la Sede Electrónica tendrá

carácter oficial y auténtico, generando los mismos efectos jurídicos que los de en soporte papel.

**CAPÍTULO II  
DE LA IDENTIFICACIÓN Y  
AUTENTICACIÓN DE DOCUMENTOS**

**Artículo 17. Formas de Identificación y Autenticación.** La Administración General del Estado admitirá los sistemas de firma electrónica en sus relaciones por Medios Electrónicos, que resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

**Artículo 18. Sistemas de Autenticación de los Ciudadanos.** Los Ciudadanos podrán utilizar los siguientes Sistemas de Firma Electrónica:

- a) Los Sistemas de Firma Electrónica incorporados al Documento de Identidad Personal.
- b) Los Sistemas de Firma Electrónica avanzada, incluyendo los basados en Certificado Electrónico reconocido, admitidos por la Administración General del Estado.
- c) Otros Sistemas de Firma Electrónica de claves concertadas en un registro previo como usuario.

**Artículo 19. Sistemas de Autenticación de Documentos.** La Administración General del Estado podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca:

- a) Los Sistemas de Firma Electrónica basados en la utilización de Certificados de Dispositivo seguro o medio equivalente que permita identificar la Sede Electrónica y el establecimiento con ella de comunicaciones seguras.
- b) Los Sistemas de Firma Electrónica para la actuación administrativa autorizada.
- c) La Firma Electrónica del Personal al Servicio de la Administración General del Estado.
- d) El intercambio de datos en entornos cerrados de comunicación.

**Artículo 20. Documento de Identidad Personal.**

Las personas físicas podrán utilizar, en caso de necesidad y con carácter universal, los sistemas de firma electrónica incorporados a Documento de Identidad Personal en su relación y comunicación con la Administración General del Estado para su identificación, que producirá los mismos efectos jurídicos que el de en soporte ordinario.

**Artículo 21. Firma Electrónica Avanzada.** 1.

Las personas físicas o jurídicas podrán utilizar los Sistemas de Firma Electrónica Avanzada para identificarles y autenticar sus documentos, usando la relación de sistemas de firma electrónica avanzada admitidos con carácter general por la Administración, que ésta deberá hacer pública y accesible para todos y por los Medios Electrónicos.

2. La referida relación incluirá la información sobre los elementos de identificación utilizados, las características de los Certificados Electrónicos admitidos, los prestadores que los expiden, las especificaciones de firma electrónica que pueden realizarse con dichos certificados y otros elementos que sean necesarios.

3. La Administración General del Estado podrá admitir la utilización de Certificados Electrónicos expedidos a Entidades sin personalidad jurídica y determinar las condiciones de utilización de otros sistemas de Firma Electrónica, como pueden ser las claves concertadas en un registro previo, la aportación de información conocida por ambas partes u otros no criptográficos o secretos, certificando la existencia y el contenido de las actuaciones de los ciudadanos en este tipo de identificación y autenticación, cuando fuere necesario.

4. En los supuestos que se utilicen estos sistemas para confirmar alguna información, propuesta o borradores remitidos o exhibidos por la Administración General del Estado, ésta deberá garantizar la integridad y no rechazo por ambas partes de los documentos concernidos.

**Artículo 22. Actuación Administrativa y Automatizada.** 1.

A los efectos de identificación y autenticación del ejercicio de la competencia en la

actuación automatizada, la Administración General del Estado podrá determinar los supuestos o casos de utilización de los siguientes sistemas de firma electrónica:

- a) Sello Electrónico de la Administración General del Estado, Órgano o Ente Público, basado en Certificado Electrónico que reúna los requisitos exigidos por la Ley de Firma Electrónica.
- b) Código Seguro de Verificación vinculado con dicha Administración Pública, Órgano o Ente Público y a la persona firmante del documento, permitiéndose la comprobación de la integridad del documento mediante acceso a la Sede Electrónica correspondiente.

2. Los Certificados referidos deberán incluir el Número de Identificación Fiscal, la identidad de la persona titular en el caso de sellos de Órganos de la Administración General del Estado y la denominación correspondiente.

3. La Administración deberá hacer pública y accesible para todos y por los Medios Electrónicos, la relación de los Sellos Electrónicos utilizados por la misma, sus Órganos y Entes Públicos, incluyendo las características de los Certificados Electrónicos y los prestadores que los expiden, adoptando las medidas necesarias y adecuadas para la verificación de dichos sellos.

### CAPÍTULO III

#### DE LA INTEROPERABILIDAD DE LA IDENTIFICACIÓN Y AUTENTICACIÓN

**Artículo 23. Identificación y Autenticación de Firma Electrónica del Personal al Servicio de la Administración General del Estado.**

La identificación y autenticación del ejercicio de la competencia de la Administración General del Estado, Órgano o Ente Público, cuando utilice los Medios Electrónicos, se realizará mediante Firma Electrónica del Personal a su servicio, debiendo proveerle de Sistemas de Firma Electrónica que permitan identificar de forma conjunta al titular del puesto de trabajo o cargo y a la propia Administración, Órgano o Ente Público, en que preste sus

servicios, y pudiendo hacer uso de forma electrónica basada en el Documento de Identidad Personal.

**Artículo 24. Intercambio Electrónico de Datos en Entornos Cerrados de Comunicación.** 1. Los Documentos Electrónicos transmitidos en Entornos Cerrados de Comunicaciones, establecidos entre la Administración General del Estado, Órganos y Entes Públicos, serán considerados válidos a efectos de identificación y autenticación de los emisores y receptores.

2. Cuando los participantes en las comunicaciones a que se refieren en el párrafo anterior pertenezcan a una misma Administración General del Estado, Órgano o Ente Público, éstos determinarán las condiciones y garantías por las que se regirán, incluyendo la relación de los emisores y receptores autorizados y la naturaleza de los datos a intercambiar. Si pertenecieran a distintos órganos, las referidas condiciones y garantías se establecerán mediante convenio.

3. En cualquier caso, todos deberán procurar en garantizar la seguridad del entorno cerrado de comunicaciones y la protección de datos que transmitan.

**Artículo 25. Certificados Electrónicos.** 1. Los Certificados Electrónicos reconocidos emitidos por los prestadores de servicios de certificación serán admitidos por la Administración General del Estado como válidos para relacionarse con la misma, siempre que el prestador de servicios ponga a disposición de ella la información precisa, concreta y en condiciones tecnológicamente viables y no suponga coste alguno para aquélla.

2. Los Sistemas de Firma Electrónica utilizados y distintos a los basados en los certificados a que se refieren en el párrafo anterior, también podrán ser admitidos por la Administración General del Estado, conforme a los principios de reconocimiento mutuo y reciprocidad.

3. La Administración General del Estado dispondrá de un mecanismo o plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de la Administra-

ción General del Estado, sus Órganos y Entes Públicos, que será de libre acceso para todos los Departamentos, Instituciones y Entes Públicos.

**Artículo 26. Actuación Administrativa del Funcionario Público.** 1. Cuando para la realización de cualquier operación por Medios Electrónicos se requiera la identificación y autenticación de un ciudadano mediante los medios previstos en los Artículos anteriores, de los que no disponga, el Funcionario Público podrá realizar válidamente dicha identificación y autenticación, utilizando el Sistema de Firma Electrónica del que esté dotado, y quedando obligado el ciudadano de identificarse y prestar su consentimiento expreso para la eficacia de la actuación, de lo que se dejará constancia para los casos de discrepancia o litigio.

2. Cada Departamento, Órgano, Institución o Ente Público mantendrá actualizado un registro o lista de los Funcionarios Públicos habilitados para la práctica de este tipo de identificación y autenticación.

**Artículo 27. Representación Habilitada por la Administración General de los Interesados.** La Administración General del Estado podrá habilitar con carácter general o particular a personas físicas o jurídicas autorizadas para realizar determinadas transacciones electrónicas en representación de los interesados. La habilitación en cuestión deberá especificar las condiciones y las obligaciones de los representantes y determinar la presunción de validez de dicha representación, salvo que la Ley de aplicación establezca otra cosa, cuya acreditación podrá ser requerida en cualquier momento por la Administración General del Estado habilitante.

## TÍTULO IV

### DE LOS REGISTROS, COMUNICACIONES Y NOTIFICACIONES

#### CAPÍTULO I

#### DE LOS REGISTROS Y SUS CÓMPUTOS

**Artículo 28. Registros Electrónicos.** La Administración General del Estado creará un Sistema de Registros Electrónicos y los correspondientes

Registros Electrónicos para la recepción y remisión de escritos, solicitudes y comunicaciones, en especial de:

- a) Documentos Electrónicos Normalizados correspondientes a los servicios, trámites y procedimientos administrativos y cumplimentados de acuerdo con los formatos preestablecidos.
- b) Cualquier escrito, solicitud o comunicación distinta a los anteriores, que sea dirigido a cualquier Órgano, Institución o Ente Público de la Administración General del Estado.

**Artículo 29. Registros Existentes.** En el ámbito de la Administración General del Estado se automatizarán las Oficinas de los Registros Existentes a fin de garantizar la interconexión de todas sus oficinas y facilitar el acceso por Medios Electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

**Artículo 30. Funcionamiento de Registros Electrónicos.** 1. En la Sede Electrónica de Acceso al Registro Electrónico figurará la relación actualizada de los escritos, solicitudes y comunicaciones a que hace referencia el Artículo anterior.

2. Los Registros Electrónicos emitirán automáticamente un recibo consistente en una copia auténtica del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de su presentación y el correspondiente número de entrada o salida.

3. Podrán aportarse documentos que se acompañan al escrito, solicitud o comunicación, siempre que cumplan con los requisitos de seguridad y los estándares de formato, que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad. Los Registros Electrónicos generarán recibos acreditativos de entrega de estos documentos que garanticen la integridad y el no rechazo de los documentos aportados.

**Artículo 31. Cómputo de Plazos.** 1. A los efectos de Cómputo de Plazos procedimentales imputables tanto al interesado como a la Administración General del Estado, los Registros Electrónicos se registrarán por fecha y hora oficial de la Sede

Electrónica de Acceso y permitirán la presentación de escritos, solicitudes y comunicaciones todos los días del año durante las veinticuatro (24) horas del día.

2. La presentación hecha por el interesado en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, cuando el cómputo es fijado en días hábiles o naturales, salvo que una Ley permita la recepción en un día inhábil.

3. El inicio del cómputo de plazos de los Órganos Administrativos y Entes Públicos se registrará por la fecha y hora de presentación de los escritos, solicitudes o comunicaciones en su registro o por fecha y hora de entrada en el registro del destinatario.

## **CAPÍTULO II DE LAS COMUNICACIONES Y NOTIFICACIONES**

**Artículo 32. Las Comunicaciones.** 1. Todo ciudadano podrá elegir en cualquier momento la forma de comunicarse con la Administración General del Estado, sus Órganos o Entes Públicos, sea o no por Medios Electrónicos, salvo que la Ley señale una forma concreta de comunicarse. La opción de comunicarse por uno u otro medio no vincula al ciudadano, que podrá aplicar en cualquier momento un medio distinto al iniciante elegido.

2. La Administración General del Estado utilizará Medios Electrónicos en las comunicaciones con el ciudadano, siempre que éste así lo haya solicitado o consentido expresamente. Dicha solicitud y consentimiento podrá emitirse y recabarse por Medios Electrónicos.

**Artículo 33. Validez de las Comunicaciones.** 1. Las comunicaciones a través de los Medios Electrónicos serán válidas, siempre que exista constancia de la transmisión y recepción de las mismas, de sus fechas, de su contenido íntegro y de la identificación fidedigna del remitente y del destinatario de aquellas.

2. La Administración General del Estado hará público en su propia Sede Electrónica y en el Boletín Oficial del Estado, los Medios Electrónicos que los ciudadanos podrán utilizar en cada supuesto en el ejercicio de su derecho de comunicarse con ella.

**Artículo 34. Práctica de Comunicación por Medios Electrónicos.** 1. Para la práctica de notificaciones por Medios Electrónicos, se requerirá que el interesado haya señalado dichos medios como preferentes o haya consentido su utilización, preferencia y consentimiento que podrán emitirse y recabarse, en todo caso, por Medios Electrónicos.

2. Durante la tramitación del procedimiento, el interesado podrá requerir al Órgano correspondiente que las notificaciones sucesivas no se practiquen por Medios Electrónicos, sino por los medios admitidos por la Ley de Procedimiento Administrativo.

**Artículo 35. Efectos de la Notificación Electrónica.** 1. El Sistema de Notificación Electrónica permitirá acreditar la fecha y hora en que se pone a disposición del interesado del acto jurídico-administrativo objeto de notificación, así como la de acceso a su contenido, actuación a partir de la cual la notificación se entenderá practicada a todos los efectos legales.

2. Producirá los efectos propios de notificación por comparecencia el acceso electrónico por el interesado al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia dicho acceso.

**Artículo 36. Plazos de la Notificación.** Transcurridos quince (15) días naturales sin que el interesado acceda al contenido del acto objeto de notificación, existiendo constancia de su puesta a disposición de aquél, se entenderá que dicha notificación ha sido rechazada, salvo se compruebe, de oficio o a instancia del destinatario, la imposibilidad técnica del acceso.

## TÍTULO V

### DOCUMENTOS Y ARCHIVOS ELECTRÓNICOS

#### CAPÍTULO I

#### DE LOS DOCUMENTOS ELECTRÓNICOS

**Artículo 37. Documento Administrativo Electrónico.** 1. La Administración General del Estado podrá emitir válidamente por Medios Electrónicos los Documentos Administrativos, siempre que incorporen las Firmas Electrónicas legalmente requeridas y que incluirán la referencia temporal garantizada por los Medios Electrónicos, cuando así la naturaleza de los mismos lo requiera.

2. La Administración General del Estado determinará la relación de los prestadores de servicios de certificación electrónica que prestarán el servicio de sellado de tiempo.

**Artículo 38. Copias Electrónicas de Documentos Administrativos.** 1. Las Copias Electrónicas de Documentos Administrativos emitidos por el interesado o por la Administración General del Estado a través de Medios Electrónicos, con o sin formato original, tendrán inmediatamente la consideración de copias auténticas con eficacia, siempre que el Documento Electrónico original se encuentre en poder de la referida Administración, y que la información de firma electrónica y sellado de tiempo permitan comprobar la coincidencia y concordancia del contenido de dicho documento.

2. Las copias realizadas por la Administración General del Estado utilizando los Medios Electrónicos de documentos emitidos originalmente por la propia Administración en soporte papel, tendrán la consideración de copias auténticas, siempre que cumplan las condiciones del apartado anterior.

3. Las copias realizadas en soporte papel de Documentos Administrativos emitidos por Medios Electrónicos y firmados electrónicamente, tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan constatar su autenticidad mediante acceso a los Archivos Electrónicos de la Administración General del Estado, Órgano o Entidad emisora.

**Artículo 39. Imagen Electrónica de Documentos Administrativos.** La Administración General del Estado podrá obtener Imágenes Electrónicas

de los Documentos Privados aportados por los interesados, con la misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del Documento Imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada mediante sellado electrónico.

## **CAPÍTULO II DE LOS ARCHIVOS ELECTRÓNICOS**

**Artículo 40. Archivo Electrónico de Documentos.** Podrán almacenar por Medios Electrónicos todos los documentos utilizados en las actuaciones administrativas, clasificándolos y archivándolos en soportes por sus peculiaridades, tipos, características y naturaleza, debiendo contar dichos medios y soportes con medidas de seguridad que garanticen la autenticidad, integridad, confidencialidad, calidad, protección y conservación de los documentos almacenados, y aseguren la identificación de los usuarios, el control de acceso y las garantías de Protección de Datos Personales y Familiares del individuo.

**Artículo 41. Archivo Electrónico de Documentos relacionados con Particulares.** Los Documentos Administrativos Electrónicos relacionados con los derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro que, asegure la identidad e integridad de la información necesaria para reproducirlo. También se asegurará, en todo caso, la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

## **CAPÍTULO III DE LOS EXPEDIENTES ELECTRÓNICOS**

**Artículo 42. Los Expedientes Electrónicos.** 1. El Expediente Electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contenga.

2. El foliado de los Expedientes Electrónicos se llevará a cabo mediante un Índice Electrónico, firmado por la Administración General del Estado, Órgano o Ente Público actuante. Este índice

garantizará la integridad del expediente electrónico y permitirá su recuperación, siempre que sea necesario, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

**Artículo 43. Remisión de Expedientes Electrónicos.** La Remisión de Expedientes Administrativos en soporte papel podrá ser sustituida a todos los efectos legales por la puesta a disposición de los Expedientes Electrónicos, teniendo los interesados derechos a obtener copias de los mismos.

## **TÍTULO VI DE LA GESTIÓN ELECTRÓNICA DE LOS PROCEDIMIENTOS ADMINISTRATIVOS**

### **CAPÍTULO I DE LA GESTIÓN ELECTRÓNICA**

**Artículo 44. Medios Electrónicos.** La Gestión Electrónica de la Actividad Administrativa respetará la titularidad y el ejercicio de las competencias por la Administración General del Estado, Órgano o Ente Público, así como sus Estructuras Orgánicas y Funcionales y el cumplimiento de los requisitos formales y materiales establecidos en las Leyes que regulen la actividad y el funcionamiento de los mismos. A estos efectos y por necesidad de simplificación de la duración de los procedimientos administrativos se impulsa la aplicación de Medios Electrónicos a los procesos, actuaciones, trámites y actividad administrativos.

**Artículo 45. Criterios para la Gestión Electrónica.** La aplicación de Medios Electrónicos a la Gestión Electrónica de los procedimientos, procesos, actuaciones y servicios estará precedida siempre de la realización de un análisis de diseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los aspectos siguientes:

- a) La supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regularización de su aportación al finalizar la tramitación.

- b) La previsión de medios e instrumentos de participación, transparencia e información.
- c) La reducción de plazos y tiempos de respuesta.
- d) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas.
- e) La efectividad del control de ingresos al fisco.

## **CAPÍTULO II DEL PROCEDIMIENTO ADMINISTRATIVO ELECTRÓNICO**

**Artículo 46.- 1.** La iniciación de un procedimiento administrativo a instancia del interesado por Medios Electrónicos requerirá la puesta a su disposición de los correspondientes modelos o sistemas electrónicos de solicitud en la Sede Electrónica o en el Registro de Entrada y Salida de cada Departamento Ministerial, Órgano o Ente Público.

**2.** El interesado podrá aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original se garantizará mediante la utilización de firma electrónica avanzada. A estos efectos, la Administración General del Estado podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas o, en caso de imposibilidad del cotejo, requerir al interesado la exhibición del documento original.

**3.** Los sistemas normalizados de solicitud podrán incluir la comprobación automática de la información aportada respecto a los datos almacenados en los sistemas propios o pertenecientes a otras Administraciones, Órganos o Entes, y ofrecer el formulario cumplimentado, en todo o en parte al interesado, para que verifique la información contenida en el mismo o la modifique o complete, si fuere necesario.

**Artículo 47. Instrucción del Procedimiento de Gestión Electrónica. 1.** Los sistemas y aplicaciones de información utilizados para la instrucción por Medios Electrónicos de procedimientos administrativos, deberán prever y garantizar el control de plazos y tiempos, la identificación de los órganos responsables de dichos procedimientos y

la tramitación ordenada de los expedientes, facilitando la simplificación y la publicidad de los mismos.

**2.** Los sistemas de comunicación utilizados en la Gestión Electrónica de los procedimientos para las comunicaciones internas entre Órganos y Unidades intervinientes en la emisión y recepción de informes u otras actuaciones, deberán cumplir los requisitos de celeridad, impulso procesal y simplificación de las actuaciones.

**3.** Cuando se utilicen los Medios Electrónicos para la participación del interesado en la instrucción del procedimiento, en ejercicio de sus derechos de presentar alegaciones antes de la resolución o de su puesta o en el trámite de presentación de pruebas o de audiencia, cuando procedan, se emplearán los medios de comunicación y notificación previstos en la presente Ley.

**Artículo 48. Estado de Tramitación. 1.** En los procedimientos administrativos en que se utilicen en su totalidad los medios electrónicos, el Órgano responsable de la tramitación del procedimiento podrá a disposición del interesado un servicio electrónico restringido donde pueda consultar, después de su identificación, la información sobre el estado de tramitación de dicho procedimiento, salvo que la Ley establezca más limitaciones, que incluirá la relación de actos realizados con extracto de sus contenidos y las fechas que fueron dictados o practicados.

**2.** En los demás procedimientos, se habilitarán igualmente servicios de información sobre el estado de tramitación de los mismos, que comprenderá la indicación de la fase en que se encuentra la tramitación y el Órgano o Unidad responsable.

**Artículo 49. Terminación del Procedimiento de la Tramitación. 1.** La Resolución de un procedimiento administrativo utilizando los Medios Electrónicos deberá garantizar la identidad del Órgano competente mediante el empleo de la Firma Electrónica, y se notificará de forma automatizada, cuando así lo disponga la Ley.

**2.** La actuación automatizada requerirá el establecimiento previo del Órgano u Órganos responsa-

bles y competentes para la definición de la especificación, programación, mantenimiento, supervisión y control de calidad y auditoría del Sistema de Información y de su Código Fuente. También se indicará el Órgano que debe ser considerado responsable en caso impugnación.

**TÍTULO VII**  
**DEL ENTE PÚBLICO DE COORDINACIÓN Y**  
**EJECUCIÓN TÉCNICA DE LOS SISTEMAS DE**  
**COMUNICACIÓN ELECTRÓNICA**

**CAPÍTULO I**  
**DE LA NATURALEZA Y ATRIBUCIÓN**

**Artículo 50. Marco Institucional.** 1. El Centro Nacional para la Informatización de la Administración Pública de Guinea Ecuatorial, en anagrama CNIAPGE, es el Organismo encargado de la coordinación, gestión y ejecución técnica del Sistema de Comunicaciones Electrónicas en la Administración General del Estado.

Corresponderá a CNIAPGE, entre otras, el ejercicio de las siguientes atribuciones y funciones:

- a) Garantizar el cumplimiento de las normas, propósitos y principios establecidos en esta Ley.
- b) Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones utilizados por la Administración General del Estado.
- c) Desarrollar programas conjuntos de planes de acción para promover el desarrollo de la Administración Electrónica en Guinea Ecuatorial.
- d) Garantizar la cooperación entre los distintos servicios que forman parte de la Administración General del Estado y ofrecer a los ciudadanos información actualizada sobre el desarrollo de sus actividades en el ámbito de las comunicaciones electrónicas.
- e) Cualesquiera otras derivadas de las anteriores y de la legislación vigente.

2. Las Organizaciones No Gubernamentales, Empresas o Agentes Sociales podrán colaborar en la

materialización y desarrollo de las comunicaciones electrónicas en la Administración General del Estado de Guinea Ecuatorial.

**CAPÍTULO II**  
**DE LA COOPERACIÓN EN MATERIA DE INTER-**  
**OPERABILIDAD DE SISTEMAS**  
**Y APLICACIONES**

**Artículo 51. Interoperabilidad de los Sistemas Informáticos.** 1. La Administración General del Estado utilizará las tecnologías de la información y comunicación en su relación con las demás administraciones y con los particulares, aplicando las medidas informáticas, tecnológicas, organizativas y de seguridad que garanticen un adecuado nivel de interoperabilidad técnica, semántica y de coordinación, y evitando en todo momento la discriminación y el desconocimiento de las nuevas tecnologías.

2. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones a tener en cuenta en el momento de toma de decisiones tecnológicas que garanticen la interoperabilidad.

3. El Esquema Nacional de Seguridad tiene por objeto establecer y trazar la política de seguridad en la utilización de los Medios Electrónicos en la Administración General del Estado, velando por la protección adecuada de la información.

**Artículo 52. Red Tecnológica Exclusiva de Comunicaciones de la Administración General del Estado.** 1. La Administración General del Estado crea y establece una red de comunicaciones, que estará al servicio de la misma, de sus Órganos y Entes para agilizar los procedimientos y actividades administrativos, facilitar la comunicación entre ellos y posibilitar la interconexión con otras redes para una administración efectiva, eficaz, eficiente, transparente y rentable, y no podrá ser objeto de transacciones y ni traspasarse a Entes Públicos o Privados, sino por acuerdo del Consejo de Ministros.

2. La Administración General del Estado deberá implantar los espacios comunes o ventanillas únicas para facilitar el acceso de los ciudadanos a los servicios prestados por aquélla.

**Artículo 53. Acuerdos de Niveles de Servicio.**

Los Servicios de la Administración General del Estado podrán, a través de acuerdos de Niveles de Servicio, habilitar sus puntos de acceso para la recepción recíproca de solicitudes, documentos y comunicaciones presentados por los usuarios, aun cuando no sean de su competencia con el propósito de remitirlos al Órgano o Servicio competente.

**DISPOSICIONES ADICIONALES:**

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

**Segunda.** Contra cualquier infracción que se cometa por incumplimiento de la presente Ley, serán de aplicación las sanciones previstas en la Ley General de Telecomunicaciones, en la del Procedimiento Administrativo y en las demás Disposiciones Legales reguladoras del Gobierno Electrónico en la República de Guinea Ecuatorial.

**DISPOSICIÓN TRANSITORIA:**

Mientras no se implementen totalmente los Sistemas Electrónicos en los Servicios Públicos de la Administración General del Estado, se seguirá aplicando simultáneamente los procedimientos actuales y los electrónicos.

**DISPOSICIÓN DEROGATORIA:**

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente Ley.

**DISPOSICIÓN FINAL:**

La presente Ley entrará en vigor a los veinte (20) días de su publicación en el Boletín Oficial del Estado y en los Medios de Comunicación Nacional.

Dada en la Ciudad de Malabo, a veintiocho días del mes de Mayo del año dos mil quince.



\* \* \*

**Ley Núm. 1/2.016, de fecha 22 de Julio, de Protección de Datos Personales.**

**EXPOSICIÓN DE MOTIVOS:**

El desarrollo que conoce la sociedad ecuatoguineana, así como el auge que tienen en la actualidad las tecnologías de la información y la comunicación, ponen de manifiesto la necesidad de regular con coherencia los derechos y libertades fundamentales de los ciudadanos, recogidos en la Ley Fundamental de Guinea Ecuatorial. Si ello se añade el programa del Gobierno, de implantar la Administración Electrónica en la Administración General del Estado, quedaría justificada la importancia que reviste la presente Ley como instrumento Jurídico Regulador de la Protección de Datos Personales de los ciudadanos.

En este sentido, la presente Ley tiene la finalidad de hacer frente a los riesgos que para los derechos y libertades fundamentales de las personas pueden suponer la obtención, recolección, recogida y tratamiento de sus datos personales, con o sin consentimiento. Por ello, ha de destacarse que la misma trata de garantizar y asegurar el uso de dichos datos, estableciendo los medios y mecanismos para la defensa de los mismos ante los Órganos competentes, regulando jurídicamente el tratamiento automatizado o no de dichos datos y, aportando un conjunto de definiciones que ayudan al correcto entendimiento de esta disposición legal.

La Protección de los Datos Personales es una obligación de los Poderes Públicos, de los Órganos de la Administración, de los Responsables de los Ficheros y del tratamiento de los mismos y de

los propios ciudadanos. De ahí que la presente Ley crea la autoridad con competencia para la protección de los datos personales, con atribuciones para la inspección y sanción a los infractores de sus disposiciones; fija las condiciones y requisitos para los ficheros y el tratamiento de dichos datos, y reconoce al ciudadano no sólo la necesidad de otorgar su consentimiento sino también el derecho de información y notificación sobre el tratamiento de sus datos personales, así como el derecho de certificación, cancelación y oposición a los mismos.

En su virtud, a propuesta del Gobierno, y precia aprobación por el Parlamento Nacional en su Primer Periodo Ordinario de Sesiones celebradas en la Ciudad de Bata del año 2.016, y haciendo uso de las prerrogativas que Me confiere el Artículo 40 de la Ley Fundamental, Sanciono y Promulgo la presente:

## LEY DE PROTECCIÓN DE DATOS PERSONALES

### TÍTULO I DISPOSICIONES GENERALES

**Artículo 1. Objeto.** La presente Ley tiene por objeto garantizar y proteger los derechos y libertades fundamentales de las personas, en especial en lo concerniente al tratamiento de sus datos personales, de su honor, dignidad e intimidad personal y familiar.

**Artículo 2. Ámbito de Aplicación. 1.** La presente Ley será de aplicación a los Datos Personales de todos los ciudadanos registrados en cualquier tipo de soporte, tanto en el Sector Público como en el Privado, que los haga susceptibles de tratamiento o de uso posterior por otras personas físicas o jurídicas o por las Entidades Públicas y Privadas, cuando dicho tratamiento se realice o se utilice en los medios situados en el Territorio Nacional, o al responsable del tratamiento se le aplicare la legislación ecuatoguineana, si no estuviere establecido en el País.

**2.** También se regirán por la presente Ley y por las disposiciones específicas los tratamientos de datos personales relacionados con los ficheros regulados por la Legislación Electoral, los Estadís-

ticos, los del Registro Civil y del Registro de Penados y Rebeldes, y con las imágenes y los sonidos obtenidos por videocámaras de seguridad.

### **Artículo 3. Exclusión del Ámbito de Aplicación.**

La presente Ley no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, a los establecidos para el crimen organizado y terrorismo, ni a los relacionados a materias clasificadas.

**Artículo 4. Definiciones.** A los efectos de la presente Ley, se entenderá por:

- a) **Afectado o Interesado.** Persona física titular de los datos que sean objeto del tratamiento.
- b) **Cesión o Comunicación de Datos.** Toda revelación de datos realizada a una persona distinta del interesado.
- c) **Consentimiento del Interesado.** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de sus datos personales.
- d) **Datos Personales.** Cualquier información, testimonio o reseña concerniente a persona física identificada o identificable concretamente.
- e) **Encargado del Tratamiento.** La persona física o jurídica, Autoridad Pública, servicio o cualquier Órgano o Institución que se dedica al tratamiento o procesamiento de Datos Personales por cuenta del responsable del tratamiento.
- f) **Fichero.** Todo mecanismo o sistema organizado de creación, almacenamiento, archivo, estructuración y acceso de Datos Personales.
- g) **Fuentes Accesibles al Público.** Ficheros de Datos Personales, cuya consulta puede ser realizada por cualquier persona, abonando la correspondiente contraprestación, como pueden ser los repertorios telefónicos, las listas de profesionales, los periódicos y Boletines Oficiales y los Medios de Comunicación.

- h) **Procedimiento de Disposición.** Todo tratamiento de Datos Personales que no permita asociarse la información obtenida a persona identificada o identificable concretamente.
- i) **Responsable del Fichero o del Tratamiento.** Persona física o jurídica, pública o privada, que se dedica al tratamiento de Datos Personales.
- j) **Tratamiento de Datos.** Procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, transmisión, modificación, cancelación y cesión de Datos Personales que resulten de las comunicaciones, interconexiones y transferencias de los mismos.

## TÍTULO II

### PRINCIPIOS RECTORES SOBRE LA PROTECCIÓN DE DATOS PERSONALES

#### CAPÍTULO I

#### DE NORMAS BÁSICAS DE LA PROTECCIÓN DE DATOS

**Artículo 5. El Fundamento Básico de la Protección de Datos.** La persona humana constituye el fundamento básico y el principal componente de la sociedad, que merece respeto y protección a su honor, dignidad, integridad e intimidad personal, en todos los sentidos y en todas las esferas de la vida social.

**Artículo 6. La Protección y la Calidad de Datos.** Para su efectividad, eficacia y eficiencia, la Protección de Datos Personales deberá basarse en la calidad de los mismos. En este sentido, sólo se podrá recoger para su tratamiento los datos personales que sean adecuados, exactos, veraces, pertinentes, completos y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido; quedando prohibida la obtención de los mismos por medios fraudulentos e ilícitos.

**Artículo 7. Almacenamiento y Cancelación de Datos.** 1. Los Datos Personales serán almacenados de forma coherente, de manera que permitan

el ejercicio del derecho de acceso a los mismos, salvo que sean legalmente cancelados.

2. Los Datos Personales serán cancelados cuando hayan de ser necesarios o pertinentes para la finalidad para la que hubieran sido obtenidos y registrados. No serán conservados en forma que permitan la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

3. Si los Datos Personales obtenidos y registrados resultaran ser inexactos, en todo o en parte o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce esta Ley.

#### **Artículo 8. Tratamiento de Datos por Terceros.**

1. La realización de tratamiento de datos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito firmado por las partes, en el que se expresará claramente que el encargado del tratamiento procesará únicamente los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

2. Los Datos Personales deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

**Artículo 9. Obtención de Datos.** Los interesados a los que se soliciten datos personales deberán ser previamente informados de forma expresa, concisa y sin lugar a equivocación, cuando se le soliciten o requieran sus datos personales, debiendo ser informados sobre la finalidad y consecuencias

de la obtención y recogida de sus datos personales, sobre su destino y los destinatarios de la información; sobre el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, sobre los efectos de la negativa de suministrarlas; sobre la existencia de ficheros o de tratamiento de datos personales, así como sobre la persona, identidad y dirección del responsable del tratamiento o de su representante.

**Artículo 10. Consentimiento del Interesado o Afectado.** 1. El Tratamiento de los Datos Personales requerirá el consentimiento claro, innegable e incuestionable del interesado o afectado; salvo se obtenga en el proceso de la actividad administrativa del Órgano competente de la Administración General del Estado, o en cualquier tipo de contrato entre las partes interesadas, o en medios y fuentes al servicio público, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

2. El consentimiento en cuestión podrá ser revocado cuando exista causa justificada para ello y no tendrá efectos retroactivos.

3. Será nulo el consentimiento para la comunicación de los datos personales a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4. Solo con el consentimiento expreso y por escrito del interesado o afectado podrá ser objeto de obtención o tratamiento, los datos personales relacionados a la raza, tribu o etnia, salud, vida sexual; al credo religioso, político o sindical; salvo en los casos de ficheros especialmente establecidos para ello y vinculados con los Partidos Políticos, Confesiones Religiosas, Sindicatos y demás Asociaciones o Fundaciones afines.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de los Órganos de la Administración General del Estado componentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante, lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

7. También podrán ser objeto de tratamiento los datos que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

## CAPÍTULO II

### SEGURIDAD, SECRETO Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES

**Artículo 11. Seguridad de los Datos.** 1. El responsable del fichero, y en su caso, los encargados del tratamiento deberán adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos personales tratados, velando por su conservación y evitando su alteración, pérdida, tratamiento o acceso no autorizado.

2. Los Datos Personales no se registrarán en Ficheros, Centros de Tratamiento, Equipos, Sistemas, Aplicaciones y Programas que no reúnan condiciones de seguridad para la integridad, confidencialidad y garantía de los mismos.

3. Los requisitos y condiciones que deban reunir los Ficheros y las personas que intervengan en el tratamiento de los datos personales serán objeto de una reglamentación específica.

**Artículo 12. Secreto y Confidencialidad de los Datos.** 1. El responsable o el encargado del Fichero y todos los intervinientes en el proceso de tratamiento de los datos personales están obligados a mantener el secreto profesional y la confidencialidad de los mismos en todo momento.

2. Los Datos Personales podrán ser comunicados a un tercero sólo para el cumplimiento de fines

directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado; salvo la cesión esté autorizada por Ley, o sean datos obtenidos por medios al servicio o fuente público, o cuando la comunicación vaya dirigida a un Órgano como los Juzgados o Tribunales, al Ministerio Fiscal y otros; o afecte a la salud pública o a la libre y legítima aceptación de una relación jurídica, o se realice entre los Órganos e Instituciones de la Administración General del Estado a efectos estadísticos y científicos.

### TÍTULO III GARANTÍA Y PROTECCIÓN DE LOS DERECHOS DE LAS PERSONAS

#### CAPÍTULO I DE LOS DERECHOS DE LAS PERSONAS

**Artículo 13. Derechos de los Ciudadanos.** Todos los Ciudadanos tendrán en el proceso de tratamiento de sus datos personales los siguientes derechos:

- a) **Derecho de Acceso a la Información de sus Datos Personales:** Dentro del plazo de doce (12) meses, el interesado tendrá derecho a solicitar y obtener gratuitamente y mediante mera consulta o por escrito, copia o fotocopia, certificada o no, la información de sus datos personales sometidos a tratamiento, el origen de dichos datos y las comunicaciones realizadas o que se prevén hacer de los mismos.
- b) **Impugnación de Valoraciones:** El interesado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración de sus datos personales y de su comportamiento, y el programa utilizado en el tratamiento de los mismos, pudiendo impugnar todo acto administrativo o decisión que implique una valoración de su conducta o comportamiento de sus características o personalidad.
- c) **Derecho de Consulta al Registro General de Protección de Datos:** Cualquier persona podrá consultar, recabar y conocer la información necesaria y deseada

del Registro General de Protección de Datos, la existencia de tratamientos de sus Datos Personales, su finalidad y la identidad del responsable del tratamiento, cuyo servicio será público.

- d) **Derecho de Rectificación y Cancelación:** El interesado tendrá el derecho de rectificar y solicitar la cancelación de sus Datos Personales cuando resulten inexactos e incompletos, quedando el responsable del tratamiento en la obligación de hacerlo efectivo en el plazo de quince (15) días desde la fecha de dicho requerimiento.
- e) **Derecho a Indemnización:** Los interesados tendrán derecho a la indemnización por los daños o lesiones que les causa el responsable o el encargado del tratamiento. Cuando se trate de los ficheros de titularidad privada, la acción se ejercitará ante la Jurisdicción Ordinaria; y en el caso de ficheros públicos, la responsabilidad se exigirá conforme a la legislación que determina el régimen de responsabilidades de la Administración General del Estado.

**Artículo 14. Excepciones a los Derechos de las Personas. 1.** Los responsables de los ficheros, que contengan los datos personales con fines policiales o tributarios, podrán denegar al ciudadano el derecho de acceso, rectificación, oposición o cancelación de los mismos, teniendo en cuenta la gravedad y peligro que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, o para las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias.

**2.** Las personas tampoco tendrán derecho a la información sobre sus Datos Personales, cuando dicha información puede afectar a la defensa nacional, seguridad nacional o a la prevención y averiguación de las infracciones penales y administrativas y a la delincuencia en general, quedándose obligados los responsables de los ficheros a denegar la solicitud formulada al efecto.

3. El afectado al que se deniegue, total o parcialmente el ejercicio de los derechos referidos en los dos apartados anteriores podrá formular la correspondiente Queja o Reposición ante el responsable del Fichero que hubiere decidido el tratamiento de los Datos Personales en cuestión, y sólo tras haber agotado esta vía de Reposición el afectado formulará la correspondiente Reclamación ante el Órgano Rector de Protección de Datos Personales que resolverá motivadamente.

## **CAPÍTULO II**

### **DE LA TUTELA DE LOS DERECHOS DE LAS PERSONAS**

**Artículo 15. Órgano de Tutela de los Derechos de las Personas.** El Órgano Rector de los Datos Personales, que será creado mediante Decreto, es el Órgano de tutela de los derechos derivados de la Protección de los Datos Personales, ante el cual, cualquier interesado al que se deniegue total o parcialmente el ejercicio de los derechos de oposición, acceso, rectificación o cancelación de sus datos, podrá formular todo tipo de reclamación o queja, del que dependerá orgánica y funcionalmente el Registro General de Protección de Datos Personales.

**Artículo 16. Tutela Jurisdiccional de los Derechos de las Personas. 1.** En virtud de la presente Ley, toda persona tendrá derecho a ejercitar acciones ante los Juzgados y Tribunales de la Jurisdicción Ordinaria contra los que violaren lo dispuesto en la misma o le denegaren algún derecho.

2. Procederá la acción a que se refiere el punto anterior, después de la correspondiente reclamación o queja, si la hubiere, ante el Órgano Rector de Protección de Datos Personales o ante el Órgano competente de la Administración General del Estado según los casos, cuya resolución se dictará dentro del término de tres (3) meses contado desde la fecha en que se tuvo conocimiento de los hechos.

## **TITULO IV**

### **FICHEROS DE DATOS PERSONALES**

#### **CAPÍTULO I**

#### **DE LAS DISPOSICIONES COMUNES**

**Artículo 17. Creación de Ficheros de Datos Personales. 1.** Los Ficheros, como mecanismos o sistemas de almacenamiento, archivo, estructuración y acceso de Datos Personales de los Ciudadanos, pueden ser creados por la Administración General del Estado mediante Decreto; o por iniciativa privada mediante la obtención de la correspondiente Concesión o Autorización Administrativa del Órgano competente, bajo las garantías que esta Ley establece para la protección de las personas.

2. Los Ficheros creados por las Fuerzas Armadas y Cuerpos de Seguridad Nacional, que contengan datos personales para fines administrativos, estarán sujetos al Régimen General de la presente Ley.

**Artículo 18. Limitación del Tratamiento de Datos Personales para fines Policiales. 1.** La obtención y el tratamiento de Datos Personales para fines Policiales sin el consentimiento de la persona afectada, se limitarán y se enmarcarán estrictamente en los supuestos necesarios para la prevención de un peligro real para la seguridad pública, para la prevención y represión de la delincuencia o de cualquier otra infracción penal o para la investigación, debiendo ser almacenados en Ficheros Específicos establecidos al efecto y clasificados por categorías en función de su grado de fiabilidad, sin perjuicio del control y de la observancia de legalidad de la actuación administrativa y de la obligación de los Órganos Jurisdiccionales, de resolver las pretensiones formuladas por los afectados e interesados al respecto.

2. Los Datos Personales registrados con fines policiales, a los que se refiere en el apartado anterior, se cancelarán cuando no sean necesarios para las averiguaciones e investigaciones que motivaron su almacenamiento, y teniendo en cuenta la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial absoluta firme, el indulto, la rehabilitación y la prescripción de responsabilidad.

**CAPÍTULO II**  
**DE LOS FICHEROS PÚBLICOS Y PRIVADOS**  
**DE DATOS PERSONALES**

**Artículo 19. Los ficheros Públicos.** Los Ficheros Públicos de Datos Personales son de titularidad de la Administración General del Estado y se crean mediante Decreto, y deberán incluir obligatoriamente la siguiente información:

- a) La finalidad del fichero y los usos previstos para el cumplimiento.
- b) Las personas o grupo de personas de que se pretenda obtener datos personales o que estén obligados a suministrarlos.
- c) La dirección y ubicación del fichero.
- d) La estructura básica y técnica del fichero y la descripción de los tipos de datos personales incluidos en el mismo.
- e) El procedimiento establecido para la obtención de datos personales.
- f) Las condiciones de cesión de datos personales y de las transferencias de los mismos para terceros.
- g) Los Órganos o personas responsables del fichero.
- h) Los servicios ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- i) Las medidas de seguridad con indicación del nivel aplicable, sea básico, medio o alto.

**Artículo 20. Los Ficheros Privados. 1.** Podrán crearse Ficheros Privados que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

**2.** Toda persona o Entidad que quiera proceder a la creación de Ficheros de Datos Personales lo hará en régimen de Concesión Pública, cuyo proyecto deberá ser notificado previamente al Órgano Rector de Protección de Datos Personales, el cual deberá incluir obligatoriamente, además de la información referida en el Artículo anterior, los datos de su inscripción registral y los de su notificación.

**Artículo 21. Comunicación y Cesión de Datos Personales. 1.** Los Datos Personales obtenidos o elaborados en el proceso de su tratamiento no serán comunicados o cedidos por la Administración General del Estado, sus Órganos e Instituciones entre los mismos, para el ejercicio de competencias distintas a las que fueron ejercidas para aquél fin, salvo que la comunicación o la cesión tenga por objeto el tratamiento posterior de dichos datos con fines históricos, estadísticos o científicos.

**2.** No obstante, podrán ser objeto de comunicación, los datos personales que una Administración Pública, Órgano o Institución trate para otra Administración, Órgano o Institución.

**3.** El responsable del Fichero Público, en el momento en que realice la primera comunicación o cesión de Datos Personales, deberá informar de ello a los afectados, indicando su finalidad, la naturaleza de los datos comunicados o cedidos y el nombre y dirección del cesionario.

**4.** Los responsables de los Ficheros Privados tampoco podrán comunicar o ceder los datos personales que hayan tratado, salvo que sea por mandato de la Autoridad Judicial competente, y quedando obligados a cumplir lo dispuesto en el apartado anterior.

**5.** En las comunicaciones y cesiones de datos previstas en el presente Artículo, no será necesario el consentimiento del afectado, salvo que dichos datos fueren obtenidos de fuentes o servicios accesibles al público y se quieran comunicar o ceder a otros Ficheros Públicos o Privados.

**Artículo 22. Datos Personales en Fuentes y Servicios de Acceso Público. 1.** Los Datos Personales que figuren en las listas de grupos profesionales y en la actividad de promoción o publicidad, se enmarcarán y se limitarán a cumplir la finalidad a que se destinan cada listado, debiendo los responsables de dichas fuentes o servicios requerir el consentimiento del interesado para incluir otros datos personales de carácter adicional. El consentimiento así otorgado podrá ser revocado en cualquier momento por el propio afectado.

**2.** Los interesados o afectados tendrán derecho a la exclusión gratuita de sus datos personales en

fuentes o servicios de acceso público o en actividad publicitaria, o que se indique de forma gratuita en dichos servicios y fuentes, que sus datos personales no pueden utilizarse para fines de publicidad, cuestión que será resuelta dentro de cinco días de la recepción de la queja o solicitud.

3. Los Datos Personales que figuren en las guías de servicios de telecomunicaciones disponibles al público, regirán por su normativa específica.

**Artículo 23. Pérdida de Carácter de Fuente o Servicio de Acceso Público.** Las Fuentes o Servicio de Acceso Público, que se editen en forma de libro, de copia de la lista en soporte electrónico o algún soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique, o la nueva copia que se obtenga.

**Artículo 24. Prestación de Servicios de Crédito, Publicidad, Reparto de Documentos y de Exploración Comercial.** 1. Cualquier persona, física o jurídica, que se dedique a la prestación de servicios de recopilación de direcciones, de información sobre créditos y patrimonios, reparto de documentos, publicidad, venta a distancia, exploración comercial y otras actividades análogas, solo podrá tratar datos personales obtenidos de los Registros y Fuentes Accesibles al Público o procedentes de las informaciones facilitadas por los interesados o conseguidos por su consentimiento.

2. Cuando se refiera a la información crediticia o patrimonial, los que se dediquen a la prestación de dichos servicios podrán tratar también datos personales, relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por su representante, notificando al interesado en el plazo de quince (15) días los datos que hubiesen sido incluidos en los ficheros y se le informará de su derecho a recabar información de la totalidad de ellos.

3. A los efectos del punto anterior, sólo se podrán registrar y acceder los Datos Personales, que sean determinantes y veraces para enjuiciar la Solvencia Tributaria, Económica y Patrimonial del interesado y que no se refieran a un periodo de tiempo superior a seis (6) años.

4. Cuando los Datos procedan de fuentes accesibles al público, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

5. En el ejercicio del derecho de acceso, los interesados tendrán derecho a conocer el origen de sus datos personales, las evaluaciones o apreciaciones que sobre los mismos hayan sido comunicadas durante el periodo de tiempo que indique y, los nombres y las direcciones de las personas o entidades a los que se hayan revelado dichos datos.

6. También los interesados tendrán derecho a oponerse al tratamiento de los datos personales que les conciernan, debiendo cancelarse los mismos y darse de baja del tratamiento a su simple solicitud o manifestación gratuita.

**Artículo 25. Códigos Tipo.** 1. Los responsables de tratamientos de Datos Personales, Públicos o Privados, y sus Agrupaciones, mediante Acuerdos y Convenios Administrativos o grupales, o decisiones de sus Instituciones, podrán formular Código Tipo que establezcan las condiciones de organización, régimen de funcionamiento, normas de seguridad de la entidad o del local, de los equipos o programas, reglas operacionales de cada sistema particular y estándares técnicos de aplicaciones y procedimientos aplicables, así como las garantías para el ejercicio de los derechos y libertades de las personas y las obligaciones de los implicados en el tratamiento y del uso de la información personal.

2. Los Códigos Tipo tendrán el carácter de Códigos Deontológicos y deberán ser inscritos en el Registro General de Protección de Datos, cuya inscripción podrá denegarse cuando su contenido no se ajusta a los principios rectores de la Protección de Datos Personales y a las disposiciones legales vigentes en la materia, requiriendo a los solicitantes verificar las oportunas correcciones y adecuaciones.

**Artículo 26. Modificación y Supresión de Ficheros Públicos y Privados.** 1. La Modificación o Supresión de los Ficheros de Datos Personales se realizará mediante el mismo tipo de resolución si

se tratare de Ficheros Públicos, o por medio de una decisión administrativa, si fuere Privado.

2. Cuando se proceda a la supresión de algún Fichero de Datos Personales, se establecerá obligatoriamente el destino del mismo y de los datos que contiene, y se ordenará adoptar las medidas y previsiones para su destrucción.

### **CAPÍTULO III DEL TRATAMIENTO INTERNACIONAL DE DATOS PERSONALES**

**Artículo 27. Comunicación Internacional de Datos Personales.** 1. Los Datos Personales que hayan sido objeto de tratamiento o hayan sido obtenidos para someterlos a tratamiento, no podrán ser comunicados, cedidos o transferidos a otros Países que no proporcionen un nivel de protección jurídica equiparable a la establecida en la presente Ley, salvo que sea mediante Autorización previa del Órgano Rector de Protección de Datos Personales.

2. El nivel de protección que ofrece el País de destino se evaluará atendiendo a todas las circunstancias que concurren en la comunicación, cesión o transferencia, y en la categoría de datos personales solicitados. En particular, se considerará la naturaleza de los datos, la finalidad y la duración del tratamiento de los mismos, el País de origen y el País de destino final, las normas de derecho vigentes y las medidas de seguridad en vigor en dichos Países.

**Artículo 28. Excepciones en la Comunicación Internacional de Datos Personales.** Lo dispuesto en el Artículo anterior no será de aplicación:

- a) Cuando la comunicación, cesión o transferencia internacional de datos personales resulte de la aplicación de Tratados o Convenios Internacionales de las que Guinea Ecuatorial es parte.
- b) Cuando el afectado haya dado su consentimiento inequívoco a la comunicación, cesión o transferencia solicitada.
- c) Cuando la comunicación, cesión o transferencia se haga a efectos de prestar o solicitar auxilio Judicial Internacional, o

para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o para la prevención, tratamiento o diagnóstico médicos, la prestación de asistencia o de Servicios Sanitarios.

- d) Cuando la comunicación, cesión o transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, en especial en el cumplimiento de las competencias fiscales y aduaneras.
- e) Cuando se refiera a transferencias dinerarias, conforme a la legislación específica vigente en la materia.
- f) Cuando la comunicación, cesión o transferencia se efectúe a petición de la persona con interés legítimo desde un Registro Público y sea acorde con la finalidad del mismo.
- g) Cuando la comunicación, cesión o transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero, o para la adopción de medidas precontractuales adoptadas a petición del afectado, o para la ejecución de un contrato celebrado o por celebrar por el responsable del fichero y un tercero en interés del afectado.

### **TÍTULO V ESTRUCTURA ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES**

#### **CAPÍTULO I DEL ÓRGANO RECTOR DE PROTECCIÓN DE DATOS PERSONALES**

**Artículo 29. Naturaleza y Régimen Jurídico.** 1. El Órgano Rector de Protección de Datos Personales ejerce la tutela de los derechos reconocidos por la presente Ley; será creado por un Decreto que fijará su estructura funcional, estará dotado de plena capacidad jurídica y se regirá por lo dispuesto en esta Ley y en las demás Leyes vigentes en la materia.

2. Los puestos de trabajo en el Órgano Rector de Protección de Datos Personales serán ocupados y desempeñados por Funcionarios de la Administración General del Estado, los cuales estarán

obligados a guardar secreto de los datos personales de que tuvieren conocimiento en el ejercicio y desarrollo de sus funciones.

**Artículo 30. Atribuciones del Órgano Rector de Protección de Datos Personales.** El Órgano Rector de Protección de Datos Personales ejerce las funciones que le son atribuidas en el Decreto de su creación para garantizar la efectiva protección de datos de carácter personal, y de manera especial ejerce las siguientes competencias:

- a) Velar por el correcto uso de los datos personales de los ciudadanos.
- b) Tutelar los derechos de las personas en el ámbito de uso de sus datos personales.
- c) Proteger los Datos Personales de los Ciudadanos en todas las esferas.
- d) Recibir quejas, peticiones, reclamaciones y recursos de las personas afectadas por el uso incorrecto de sus datos personales y dictar las resoluciones correspondientes.
- e) Comunicar al Ministerio de Telecomunicaciones y Nuevas Tecnologías, las Resoluciones de cesión de tratamiento de Datos Personales y cancelación de Ficheros de Datos Personales.
- f) Requerir informes y explicaciones de cualquier Órgano, Institución o persona sobre la Protección de Datos Personales.
- g) Cualesquiera otras que se deriven de las anteriores, de la presente Ley y de la legislación vigente, o le fueren sometidas.

## **CAPÍTULO II DE LA SECRETARÍA TÉCNICA DEL ÓRGANO RECTOR DE PROTECCIÓN DE DATOS PERSONALES**

**Artículo 31. Naturaleza y Régimen Jurídico.** El Órgano de Protección de Datos Personales estará dotado de una Secretaría Técnica destinada a asegurar que la Administración de los Ficheros de Datos Personales, cualquiera que fuere su titularidad, se ajusta a lo establecido en la presente Ley y en las demás normas del Ordenamiento Jurídico Nacional que regulan los derechos fundamentales.

**Artículo 32. Funciones de la Secretaría Técnica del Órgano Rector de Protección de Datos Personales.** 1. Son funciones de la Secretaría Técnica del Órgano Rector de Protección de Datos Personales:

- a) Velar por el cumplimiento de la legislación vigente sobre Protección de Datos Personales y controlar su aplicación, preparando las Resoluciones que dicte el Órgano Rector de Protección de Datos Personales sobre la materia de Protección de Datos Personales.
- b) Informar sobre las solicitudes de las Concesiones y Autorizaciones que deba extender el Ministerio de Telecomunicaciones y Nuevas Tecnologías, relativas al tratamiento, ficheros y Protección de Datos Personales.
- c) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los Datos Personales y dictar instrucciones precisas para adecuarlas a los principios y disposiciones de la presente Ley.
- d) Atender las peticiones, quejas y reclamaciones formuladas por las personas afectadas.
- e) Velar por la publicidad de la existencia de los Ficheros de Datos Personales, publicando periódicamente la relación de los mismos y proponiendo al Órgano Rector de Protección de Datos Personales y al Ministerio de Telecomunicaciones y Nuevas Tecnologías, la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a las disposiciones legales.
- f) Controlar las Autorizaciones de los Tratamientos Internacionales de Datos Personales, informando sobre su procedencia o no al Órgano Rector de Protección de Datos Personales y al Ministerio de Telecomunicaciones y Nuevas Tecnologías, así como desempeñar las funciones de Cooperación Internacional en materia de Protección de Datos Personales.
- g) Redactar la Memoria Anual de la Protección de Datos Personales, elevándolo al

Órgano Rector de Protección de Datos Personales para su remisión al Parlamento Nacional.

- h) Ejercer potestades sancionadoras previstas en la presente Ley.
- i) Cualesquiera otras que se deriven de las anteriores y de la legislación vigente en la materia.

2. La Secretaría Técnica ejercerá funciones bajo la directa supervisión del Órgano Rector de Protección de Datos Personales.

**Artículo 33. El Registro General de Protección de Datos.** 1. El Registro General de Protección de Datos será una estructura o Sección del Órgano Rector de Protección de Datos Personales dependiente de su Secretaría Técnica, la cual se encargará de la inscripción de los Ficheros Públicos y Privados de Datos Personales, de las Concesiones y Autorizaciones que se expidan para el tratamiento de Ficheros de Datos Personales, de los Códigos Tipo, de los datos relacionados con el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición, de las resoluciones, así como de los actos de creación, modificación o supresión de ficheros y de cualquier otro dato relevante para la protección de Datos Personales.

2. Se habilitarán Libros Especiales para la Inscripción en el Registro General de Protección de Datos, debidamente foliados y diligenciados por el Juez Primera Instancia, en cuyos folios se harán constar todos los datos del fichero, los nombres y apellidos del responsable del fichero y de los interesados o afectados, sus direcciones, el contenido de los datos personales que se refieren, la infracción cometida, la modificación, cancelación, rectificación u oposición que se solicita y otros datos relevantes para dicho acto.

**Artículo 34. Recursos Económicos y Financieros.** El Órgano Rector de Protección de Datos Personales contará, para el cumplimiento de sus fines, con los medios o recursos económicos y financieros provenientes de las Asignaciones de los Presupuestos Generales del Estado.

## TÍTULO VI RÉGIMEN SANCIONADOR EN LA PROTECCIÓN DE DATOS

### CAPÍTULO I DE LAS DISPOSICIONES COMUNES

**Artículo 35. Competencia.** 1. El Ministerio de Telecomunicaciones y Nuevas Tecnologías, en el marco de sus funciones, ejercerá la potestad sancionadora prevista en esta Ley contra cualquier infractor, previa incoación e instrucción del procedimiento sancionador por la Dirección General de Nuevas Tecnologías, o en su caso por el Órgano Rector de Protección de Datos Personales.

2. 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 (30) días desde la fecha de la notificación de la misma.

3. El Órgano Rector de Protección de Datos Personales también ejercerá la potestad sancionadora dentro del ámbito de sus competencias.

4. El Ministro de Telecomunicaciones y Nuevas Tecnologías y el Órgano Rector de Protección de Datos Personales realizarán inspecciones y control de los ficheros que se dediquen al tratamiento de Datos Personales, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos, requiriendo la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, y accediendo a los locales donde se hallen instalados los equipos, ficheros y lógicos de tratamientos de datos personales para su inspección, cotejo y verificación.

5. Los Funcionarios que ejerzan la referida inspección tendrán la consideración de Autoridad Pública en el desempeño de sus cometidos y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de dichas funciones, incluso después de haber cesado en las mismas.

**Artículo 36. Auxilio y Colaboración.** 1. Las Autoridades Públicas, Civiles y Militares prestarán

la protección y el auxilio necesarios a los Funcionarios para el ejercicio de sus funciones inspectoras, cuando fuere necesario y requerido para ello.

**2.** Los responsables de los Ficheros de Datos Personales y del tratamiento de los mismos deberán atender a los Funcionarios Encargados de la inspección y prestarles la debida colaboración en el desarrollo de sus funciones, compareciendo o personándose por sí o por medio de representante en el lugar, día y hora señalados para la práctica de las actuaciones, facilitándoles el acceso a sus instalaciones y a cualquier lugar que señalen y aportando o presentando los documentos, libros, datos, informes, registro y demás antecedentes solicitados y requeridos para su examen.

**3.** No obstante, lo anterior, para entrar en el domicilio personal de los responsables de los ficheros o de sus empleados, a efectos de inspección o investigación de alguna infracción, se requerirá el consentimiento de aquél o la oportuna Autorización Judicial.

**Artículo 37. Personas Responsables de la Actividad de los Ficheros.** **1.** Los Directores de los Ficheros y los Encargados de Tratamientos de los Datos Personales serán los responsables de la actividad de los mismos y estarán sujetos al régimen sancionador administrativo establecido en la presente Ley, sin perjuicio de las responsabilidades en que pudieran incurrir en relación con las normas civiles, penales, tributarias y de orden social.

**2.** Serán responsables solidarios de la actividad de sus ficheros y de las infracciones cometidas por los empleados en al ámbito de actuación del poder de dirección y mando empresarial, los titulares de los Ficheros de Datos Personales, de los que dependan.

## CAPÍTULO II

### DE LAS INFRACCIONES Y SANCIONES

**Artículo 38. Tipo de Infracciones.** Para efectos sancionatorios, las infracciones que pudieran ser cometidas en la prestación de servicios de Tratamiento de Datos Personales, se clasifican en Leves, Graves y Muy Graves.

**Artículo 39. Infracciones Leves.** Se reputan Infracciones Leves:

- a) No solicitar la Inscripción del Fichero de Datos Personales en el Registro General de Protección de Datos.
- b) La demora en facilitar la información, los documentos, datos, informes o antecedentes requeridos por la Autoridad competente de inspección, cuando no se tenga carácter grave.
- c) El incumplimiento del deber de información, notificación o requerimiento al afectado acerca del tratamiento de sus Datos Personales, cuando sean obtenidos del propio interesado.
- d) La falta de atención adecuada a los interesados y afectados.
- e) La transmisión de los Datos Personales a un encargado del tratamiento sin formalizar el correspondiente contrato o darle las instrucciones a cumplir con la obligación de no utilizarlos para otros fines y comunicarlos a terceras personas.
- f) Cualquier otro incumplimiento de la presente Ley y de la legislación vigente para garantizar el tratamiento eficaz de los datos personales, cuando no sea considerado como Infracción Grave o Muy Grave.

**Artículo 40. Infracciones Graves.** Son Infracciones Graves:

- a) Tratar Datos Personales no especialmente protegidos sin el consentimiento del afectado, cuando el mismo sea necesario, o usarlos posteriormente, infringiendo los principios y garantías de exactitud, veracidad, pertinencia y otros establecidos en la presente Ley, salvo cuando sea calificado de Infracción Muy Grave.
- b) El entorpecimiento, impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición por el interesado o afectado.
- c) El incumplimiento del deber de información, notificación o requerimiento al afectado acerca del tratamiento de sus datos

personales, cuando no hayan sido obtenidos del propio interesado.

- d) El incumplimiento de las debidas medidas y condiciones de seguridad para el mantenimiento de los ficheros, locales, programas o equipos que contengan datos personales.
- e) No atender los requerimientos o apercibimientos de la Autoridad competente de Protección de Datos Personales o no proporcionar a aquélla cuantos documentos, informes, datos e informaciones sean solicitados por la misma.
- f) La comunicación, cesión o transferencia de los datos personales sin contar con la legitimación para ello, salvo que misma sea constitutiva de Infracción Muy Grave.
- g) No atender las solicitudes, quejas y reclamaciones de los interesados o afectados.
- h) La comisión de una de las infracciones previstas en el Artículo siguiente, cuando no se den las circunstancias que permitan calificarla como Muy Grave.
- i) La comisión de dos o más Infracciones Leves sancionadas en un periodo de un año.

**Artículo 41. Infracciones Muy Graves.** Tienen la consideración de Infracciones Muy Graves:

- a) Crear Ficheros o prestar servicios de Tratamiento de Datos Personales o ser titular de Fichero de Datos Personales sin reunir los requisitos exigidos por la presente Ley, ni contar con la Resolución o la Autorización o Concesión Administrativa preceptiva o estar inscrito en el Registro General de Protección de Datos.
- b) La obtención de Datos Personales en forma engañosa o fraudulenta.
- c) El incumplimiento de las obligaciones derivadas del secreto, confidencialidad e inviolabilidad de la Protección de Datos Personales.
- d) Tratar o ceder los Datos Personales relativos a la libertad de conciencia, afiliación o ideología política, salud, vida sexual, raza, tribu o etnia, religión o cualquier

otro que implique discriminación a las personas, sin el correspondiente consentimiento expreso y por escrito del afectado, o crear Ficheros Exclusivos que contengan este tipo de datos.

- e) La negativa, obstrucción o resistencia a ser inspeccionado para establecer hechos relativos a la Protección de Datos Personales.
- f) No cesar en el Tratamiento Ilícito de Datos Personales cuando existe un previo requerimiento por parte de la Autoridad competente para ello.
- g) La comisión de dos o más Infracciones Graves sancionadas en un periodo de un año.
- h) La Comunicación, Cesión o Transferencia Internacional de Datos Personales a Países que no proporcionen un nivel de protección adecuado y sin la debida Autorización.

**Artículo 42. Sanciones. 1.** Las Sanciones aplicables por las Infracciones previstas por la presente Ley son:

- a) Por la comisión de Infracciones Leves:
  - 1. Amonestación
  - 2. Advertencia por escrito
  - 3. Multa de 200.000 hasta 500.000 F. Cfas.
- b) Por la comisión de Infracciones Graves:
  - 1. Multa de 500.001 a 5.000.000 F. Cfas.
  - 2. Suspensión de la actividad del Fichero y Tratamiento de Datos Personales.
  - 3. El precinto del local o de las instalaciones por un periodo no superior a quince (15) días hábiles.
- c) Por la comisión de Infracciones Muy Graves se impondrá una o varias de las siguientes sanciones:
  - 1. Multas de 5.000.001 a 15.000.000 de F. Cfas.
  - 2. La incautación de equipos y demás material.

3. La clausura definitiva del local y de las instalaciones.
4. La inhabilitación del infractor para el ejercicio de la actividad de Fichero y Tratamiento de Datos Personales por el plazo de un año, o la definitiva, según los casos.
5. Cancelación y revocación de la Resolución, Autorización o Concesión Administrativa para la creación de Ficheros y de su asiento en el Registro General de Protección de Datos.

2. En los supuestos de Infracción Grave o Muy Grave, cuando el Tratamiento de los Datos Personales o su comunicación, cesión o Transferencia Internacional pudiera menoscabar los derechos fundamentales de los afectados y su derecho a la Protección de Datos Personales, el Órgano Sancionador podrá requerir a los responsables de Ficheros de Datos de carácter personal, tanto Públicos como Privados, la cesación en la utilización, comunicación, cesión o transferencia ilícita de dichos datos.

3. Si el requerimiento, a que se refiere en el apartado anterior, no fuera atendido, el Órgano Sancionador podrá, mediante Resolución motivada, inmovilizar dichos ficheros a los efectos de restaurar los derechos menoscabados de los afectados.

**Artículo 43. Graduación de las Sanciones.** Para la imposición de las sanciones previstas en el Artículo anterior y la determinación del tipo aplicable, la Autoridad competente deberá tener en cuenta las siguientes circunstancias:

- a) La proporcionalidad del daño causado y su repercusión social o económica.
- b) La intencionalidad en la comisión de la infracción.
- c) El carácter continuado de la infracción.
- d) El volumen de los tratamientos efectuados.
- e) La cuantía del beneficio obtenido.
- f) El grado de participación del infractor en la infracción cometida.
- g) La reincidencia y reiteración en la comisión de infracciones.

- h) La naturaleza de perjuicios causados a los interesados y a terceras personas.

**Artículo 44. Procedimiento Sancionador. 1.** El Procedimiento aplicable para la determinación de las infracciones e imposición de las sanciones se ajustará a los principios, reglas y normas del Procedimiento Administrativo, con audiencia del interesado y protección del denunciante.

2. Las actuaciones de la Inspección podrán desarrollarse, a elección del actuario, en cualquier despacho, oficina o dependencia de la persona o Entidad inspeccionadas o de quien la represente o en los de la Autoridad Inspectora.

3. Los Inspectores documentarán sus actuaciones mediante Actas, Diligencias e Informes, que elevarán a la Autoridad competente.

4. Durante la instrucción del Procedimiento Sancionador se podrán adoptar, a instancia de las partes o de oficio, las medidas cautelares estrictamente necesarias para asegurar la eficacia de la Resolución que pudiera recaer, evitar el mantenimiento de los efectos de la infracción y salvaguardar los intereses generales. Estas medidas tendrán un carácter provisional y podrán consistir en el precinto del local o desinstalación del fichero o de los medios y equipos que se utilizan.

**Artículo 45. Procedimiento Sancionador Específico en relación a los Ficheros Públicos. 1.** Cuando las infracciones previstas en la presente Ley fuesen cometidas en Ficheros Públicos, sea cual fuere la naturaleza de las mismas, el Órgano Sancionador dictará una Resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción, y proponiendo la Incoación del Expediente Disciplinario contra los responsables de la infracción, cuando proceda. Esta Resolución se notificará al responsable del Fichero, al Órgano del que dependa jerárquicamente y a los afectados, si los hubiera.

2. El responsable del Fichero y el Órgano del que dependa jerárquicamente deberán comunicar al Órgano Sancionador las Resoluciones que recaigan en relación con las medidas y actuaciones ordenadas en su resolución.

**Artículo 46. Caducidad. 1.** Se producirá la caducidad del procedimiento de cualquier expediente incoado, cuando la instrucción del mismo quedare paralizada durante cuatro (4) meses por causas imputables al afectado.

2. El término fijado en el párrafo anterior se contará desde la fecha de la última notificación que se hubiera hecho al afectado.

3. No se producirá la caducidad cuando la paralización fuere por fuerza mayor o por otra causa ajena a las partes.

**Artículo 47. Prescripción. 1.** Las Infracciones previstas en esta Ley prescribirán:

- a) Para las Leves, al año
- b) Para las Graves, a los dos años
- c) Para las Muy Graves, a los tres años.

2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido y se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción, si el expediente sancionador estuviera paralizado durante seis (6) meses por causa no imputable al presunto responsable.

3. Las sanciones impuestas prescribirán:

- a) Al año por las Infracciones Leves
- b) A los dos años por Infracciones Graves
- c) A los tres años por Infracciones Muy Graves.

4. El plazo de prescripción de las Sanciones comenzará a contarse desde el día siguiente en que adquiriera firmeza la Resolución por la que se impongan y se interrumpirán por causa imputable al sancionado.

#### **DISPOSICIÓN ADICIONAL:**

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

#### **DISPOSICIÓN TRANSITORIA:**

A los Ficheros de Datos Personales existentes a la fecha de entrada en vigor de la presente Ley, se les concede un plazo de seis (6) meses para

adecuarse a lo dispuesto en la misma, inscribiéndose en el Registro de Protección de Datos Personales. Transcurrido dicho plazo, el Ministerio de Telecomunicaciones y Nuevas Tecnologías y el Órgano Rector de Protección de Datos Personales procederán a la Inspección y Control de los mismos, adoptando las medidas que correspondan en cada caso.

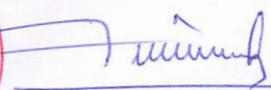
#### **DISPOSICIÓN DEROGATORIA:**

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente Ley.

#### **DISPOSICIÓN FINAL:**

La presente Ley entrará en vigor a los veinte (20) días de su publicación en el Boletín Oficial del Estado, sin perjuicio de su publicación en los demás Medios Informativos Nacionales.

Dada en la Ciudad de Malabo, a veintidós días del mes de Julio del año dos mil dieciséis.

 *POR UNA GUINEA MEJOR,*  
  
-OBIANG NGUEMA MBASOGO-  
PRESIDENTE DE LA REPUBLICA.

\* \* \*

**Ley Núm. 2/2.016, de fecha 22 de Julio, de Conservación de Datos en las Comunicaciones Electrónicas y Redes de Comunicación.**

#### **EXPOSICIÓN DE MOTIVOS:**

La aplicación y el uso de las nuevas tecnologías en la sociedad han supuesto la superación de las formas tradicionales de comunicación, que abarcan no solo la voz, sino también datos en soportes y formatos diversos. La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines no deseados cuando no son delictivos.

Precisamente en el marco de esta visión objetiva, la conservación de datos generados o tratados durante el proceso de la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, tiene por objetivo el desarrollo y la garantía del derecho y libertad de los ciudadanos al secreto de sus comunicaciones, previsto en el Artículo 13 de la Ley Fundamental de Guinea Ecuatorial. Por otra parte, trata de prevenir y evitar las actuaciones, actos y actividades con resultados no deseados, dañinos, perjudiciales o delictivos de los avances tecnológicos y de las comunicaciones por internet, así como de garantizar la seguridad jurídica en las relaciones sociales, protegiendo los derechos individuales de las personas con el respeto de su integridad, intimidad, dignidad, privacidad y personalidad.

Partiendo del aludido objeto, la presente Ley establece la obligación de los operadores de telecomunicaciones, de retener y conservar determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos las autoridades competentes mediante la correspondiente Autorización Judicial previa y con el propósito de obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija, móvil o por Internet.

En su virtud, a propuesta del gobierno, y debidamente aprobada por el Parlamento Nacional, en su Primer Periodo Ordinario de Sesiones celebrada en la Ciudad de Bata del año 2.016, y haciendo uso de las facultades que Me confiere el Artículo 40 de la Ley Fundamental, Sanciono y Promulgo la presente

*Ley de Conservación de Datos en las Comunicaciones Electrónicas y Redes Públicas de Comunicación.*

## **TÍTULO I DISPOSICIONES GENERALES**

### **CAPÍTULO ÚNICO DEL OBJETO, ÁMBITO DE APLICACIÓN Y PRINCIPIOS DE CONSERVACIÓN DE DATOS**

**Artículo 1. Objeto.** La presente Ley tiene por objeto la obligación de los Prestadores y Operadores de Servicios de Comunicaciones Electrónicas y de Redes Públicas de Comunicaciones, de conservar los datos generados, producidos o tratados en sus actividades de Servicios de Comunicaciones Electrónicas o de Redes Públicas de Comunicación, de ceder dichos datos solo por mandamiento o requerimiento de la Autoridad Judicial para detectar, investigar y enjuiciar las infracciones penales.

**Artículo 2. Ámbito de Aplicación.** La presente Ley será de aplicación a los datos de negocio, tráfico y de localización de las personas físicas y jurídicas, generados en las comunicaciones electrónicas y en las redes de telecomunicación, para identificar al usuario registrado.

**Artículo 3. Exclusión del Ámbito de Aplicación.** El contenido de las comunicaciones electrónicas y las informaciones consultadas utilizando una red de comunicaciones electrónicas, se excluyen del ámbito de aplicación de la presente Ley.

**Artículo 4. Principios de Conservación de Datos.** La actividad y el proceso de Conservación de Datos relativos a las Comunicaciones Electrónicas y las Redes Públicas de Comunicación se regirán por principios de seguridad, confidencialidad, autenticidad, integridad, necesidad, sostenibilidad técnica, proporcionalidad y no discriminación.

## **TÍTULO II RÉGIMEN JURÍDICO DE CONSERVACIÓN DE DATOS**

### **CAPÍTULO I DE LOS DATOS DE OBLIGADA CONSERVACIÓN**

**Artículo 5. Datos Objeto de Conservación.** Serán obligados a conservarse por los Prestadores de Servicios de Comunicaciones Electrónicas y por los Operadores de Telecomunicaciones, los siguientes:

- a) *Los datos necesarios para rastrear e identificar el origen de una comunicación con respecto a la telefonía de red fija a la*

*telefonía móvil; al acceso a Internet, correo electrónico y telefonía por Internet:*

1. Número de teléfono de llamada.
2. Nombre y dirección del abonado o usuario registrado.
3. La identificación asignada al usuario.
4. La identificación del usuario y el número de teléfono asignados a toda comunicación que acceda a la Red Pública de Telefonía.
5. El nombre y dirección del abonado o del usuario registrado al que se le ha sido asignado una dirección de Protocolo de Internet (IP), una identificación del usuario o un número de teléfono, en el momento de la comunicación.

*b) Los datos necesarios para identificar el destino de una comunicación con respecto a la telefonía de red fija y a la telefonía móvil; al correo electrónico y a la telefonía por Internet:*

1. El número o números marcados (o de destino) y, el número o números hacia los que se transfieren las llamadas en caso de desvío o transferencia de llamadas.
2. Los nombres y direcciones de abonados o usuarios registrados.
3. La identificación del usuario o el número de teléfono del destinatario o destinatarios de una llamada telefónica por Internet.
4. La identificación de usuario del destinatario de la comunicación.

*c) Los datos necesarios para determinar la fecha, hora y duración de una comunicación:*

1. Con respecto a la Telefonía de Red Fija y a la Telefonía Móvil: la fecha y hora del comienzo y fin de la llamada o, del servicio de mensajería o del servicio multimedia.
2. Con respecto al acceso a Internet, al correo electrónico y a la telefonía por Internet:

- La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado sector horario.
- La fecha y hora de conexión y desconexión del servicio de acceso a Internet, basadas en un determinado sector horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación del usuario o del abonado o del usuario registrado.

*d) Los datos necesarios para identificar el tipo de comunicación:*

1. Con respecto a la telefonía fija y a la telefonía móvil, el servicio telefónico utilizado: tipo de llamada, o transmisión de voz, o buzón vocal, o conferencia, o datos; así como los servicios complementarios, inclusive el reenvío o transferencia de llamadas, o servicios de mensajería o multimedia empleados, inclusive los servicios de mensajes cortos y servicios multimedia avanzados.
2. Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

*e) Los datos necesarios para identificar el equipo de comunicación de los usuarios:*

1. Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2. Con respecto a la telefonía móvil:
  - Los números de teléfonos de origen y de destino.
  - La Identidad Internacional del Abonado a un Móvil (IMSI) del que efectúa la llamada.
  - La Identidad Internacional del Equipo Móvil (IMEI) del que efectúa la llamada.

- La Identidad Internacional del Abonado a un Móvil (IMSI) del que recibe la llamada.
  - La Identidad Internacional del Equipo Móvil (IMEI) del que recibe la llamada.
  - La fecha y hora de la primera activación del servicio y la etiqueta de localización o el identificador de celda desde la que se haya activado el servicio, cuando se trata de casos de servicios anónimos de pago por adelantado como tarjetas de prepago.
3. Con respecto al acceso a Internet, correo electrónico y telefonía por Internet:
- El número de teléfono de origen en caso de acceso mediante marcado de números.
  - La Línea Digital de Abonado (DSL) u otro punto terminal identificador del autor de la comunicación.
- f) *Los datos necesarios para identificar la localización del equipo de comunicación móvil:*
1. La etiqueta de localización o identificador de celda al inicio de la comunicación.
  2. Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones.

**Artículo 6. Revelación del contenido de las Comunicaciones.** Ningún dato que revele el contenido de las comunicaciones podrá conservarse en virtud de la presente Ley en los medios, equipos, sistemas o soportes electrónicos.

## CAPÍTULO II

### DE LA CONSERVACIÓN Y CESIÓN DE DATOS

**Artículo 7. Sujetos Obligados a Conservar los Datos.** Todos los Prestadores y Operadores de Servicios de Comunicaciones Electrónicas y de Redes Públicas de Comunicación, o quienes las exploten, estarán obligados a conservar los datos a los que hace referencia la presente Ley.

**Artículo 8. Obligación de Conservar Datos. 1.** Todos los Prestadores y Operadores obligados

conforme al Artículo anterior deberán adoptar las medidas necesarias para garantizar que los datos señalados en el Artículo 5 de esta Ley se conserven debida y técnicamente en el orden en que sean generados o tratados en el marco de prestación de servicios de comunicaciones de que se trate, no pudiendo aprovechar o utilizar, en ningún caso, los registros generados fuera de lo autorizado por la Ley.

**2.** La referida obligación se extiende a los datos de las llamadas infructuosas, en la medida en que dichos datos sean generados o tratados, registrados o conservados por los Prestadores y Operadores obligados.

**3.** Se entenderá por llamada fructuosa toda aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada, pero sin contestación alguna, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

**Artículo 9. Duración del Periodo de Conservación de Datos.** La obligación de conservación electrónica de datos cesa al año, computada desde la fecha en que se haya producido la comunicación, salvo en aquellos casos y categorías de datos que tengan la consideración e interés especial para la investigación, detección y enjuiciamiento de infracciones penales, cuya duración podrá ampliarse hasta un máximo de dos años por requerimiento judicial. Dichos datos deberán ser verificados y confirmados por el Prestador u Operador.

**Artículo 10. Cesión de Datos. 1.** Los datos conservados solo pueden ser cedidos por requerimiento y Mandamiento de la Autoridad Judicial competente en Resolución motivada y para los fines previstos en el mismo.

**2.** Recibida la Resolución Judicial, el Prestador u Operador estará obligado a acceder al Funcionario, Agente o Autoridad compareciente, los datos conservados que se indican en la referida Resolución y en el plazo de ejecución determinado en la misma. Si no se fija un plazo en la Resolución, la cesión se hará inmediatamente a la recepción de la misma, o a más tardar al día siguiente.

3. Cualquier Autoridad, Órgano o Ente Público, que desee los datos conservados, deberá solicitarlos de la Autoridad Judicial competente. De lo contrario, se rechazará de plano su solicitud.

4. La cesión de datos realizada conforme a lo dispuesto en este Artículo no se comunicará a los afectados ni a terceros.

**Artículo 11. Protección y Seguridad de los Datos.** Los Prestadores u Operadores de Servicios deberán identificar al personal autorizado para acceder a los Datos Conservados o por conservar, y adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos a los iniciales, su destrucción accidental o ilícita y su pérdida, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, velando por garantizar la calidad de los datos, la confidencialidad y seguridad de los mismos, y por mantener el alto nivel de protección de los datos almacenados.

### TÍTULO III RÉGIMEN SANCIONADOR

#### CAPÍTULO I DE LOS ÓRGANOS COMPETENTES

**Artículo 12. Competencias.** 1. El Ministro de Telecomunicaciones y Nuevas Tecnologías, en el marco de sus funciones, ejercerá la potestad sancionadora prevista en esta Ley contra cualquier infractor, previa incoación e instrucción del procedimiento sancionador por la Dirección General de Nuevas Tecnologías, o en su caso por el Órgano Rector de Protección de Datos Personales.

2. 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 (30) días desde la fecha de la notificación de la misma.

3. El Órgano Rector de Protección de Datos Personales, también ejercerá la potestad sancionadora dentro del ámbito de su competencia.

**Artículo 13. Control y Supervisión.** 1. El Ministerio de Telecomunicaciones y Nuevas Tecnologías y el Órgano Rector de Protección de Datos Personales, ejercerán las funciones de Control y Supervisión del funcionamiento de los Sistemas de Conservación de Datos y del cumplimiento de lo dispuesto en la presente Ley, adoptando las medidas que sean procedentes.

2. Los Funcionarios Públicos del Ministerio de Telecomunicaciones y Nuevas Tecnologías y del Órgano Rector de Protección de Datos Personales, en el ejercicio de sus funciones inspectoras y controladoras tendrán la consideración y la calidad de Autoridad Pública.

**Artículo 14. Deber de Colaboración.** 1. Toda Institución, Órgano, o interesado tiene la obligación de facilitar al Ministerio de Telecomunicaciones y Nuevas Tecnologías y al Órgano Rector de Protección de Datos Personales, todo tipo de información y colaboración necesarias para el ejercicio de sus funciones supervisoras y controladoras.

2. Cuando de una actuación inspectora se tuviere conocimiento de hechos que pudieren 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.

#### CAPÍTULO II DE LAS INFRACCIONES Y SUS SANCIONES

**Artículo 15. Infracciones.** Las Infracciones tipificadas por la presente Ley se clasifican en Leves, Graves y Muy Graves.

##### 1. Son Infracciones Leves:

- a) La conservación negligente de los datos de obligada conservación.
- b) El incumplimiento de la obligación de protección y seguridad de datos.
- c) Las Infracciones Muy Graves y Graves previstas en los puntos 2 y 3 de este Artículo, cuando no tengan la calificación o consideración como tales.

##### 2. Son Infracciones Graves:

- a) La conservación de datos por un período inferior al establecido en la presente Ley.
- b) La no conservación por negligencia de los datos de obligada conservación.
- c) El incumplimiento reiterado de la obligación de protección y seguridad de los datos.

**3. Son Infracciones Muy Graves:**

- a) La no conservación de los datos calificados de obligada conservación en esta Ley.
- b) El incumplimiento de la obligación de llevar Registro de Usuarios de la Telefonía de Prepago por los Operadores de Telecomunicaciones, o de llevarlo de forma incompleta e inexacta, y/o la negativa de ofrecer datos sobre los mismos o la demora injustificada en ofrecerlos.
- c) La Conservación de Datos a que se refiere el punto anterior por un período superior al fijado por la presente Ley.
- d) El incumplimiento de la obligación de Protección y Seguridad de los Datos.

**Artículo 16. Sanciones. 1.** Las Infracciones previstas en el Artículo anterior se sancionarán de acuerdo con lo establecido en el Régimen Sancionador de la Ley General de Telecomunicaciones y de las demás Leyes vigentes en la materia, sin perjuicio de las responsabilidades penales a que pueda incurrir el infractor.

2. Corresponde al Ministerio de Telecomunicaciones y Nuevas Tecnologías, imponer las Sanciones por Infracciones Graves y Muy Graves, previa incoación e instrucción del correspondiente expediente por la Dirección General de Nuevas Tecnologías o por el Órgano Rector de Protección de Datos Personales.

3. La competencia de imposición de Sanciones por Infracciones Leves será de la Dirección General de Nuevas Tecnologías o del Órgano Rector de Protección de Datos Personales, cada uno en su ámbito, con notificación al Ministro de Telecomunicaciones y Nuevas Tecnologías.

**Artículo 17. Criterios Determinantes de las Infracciones.** Las Sanciones previstas en el Artículo anterior, que se impongan a los infractores, se graduarán atendiendo a los criterios siguientes:

- a) La existencia de intencionalidad.
- b) La reincidencia y reiteración por la comisión de infracciones de la misma naturaleza, sancionadas mediante Resolución firme.
- c) El beneficio que se haya obtenido el infractor de dicha infracción.

**DISPOSICIÓN ADICIONAL:**

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

**DISPOSICIONES TRANSITORIAS:**

**Primera.** Se concede un plazo de noventa (90) días a partir de la entrada en vigor de la presente Ley, para que los Operadores de Redes Públicas de Comunicación y Prestadores de Servicios de Comunicaciones Electrónicas, obtengan los datos de sus clientes no registrados hasta la fecha, relativos al objeto de la presente Ley.

**Segunda.** Mientras no se consolide los Sistemas Electrónicos en las Comunicaciones de la Administración General del Estado, se seguirá aplicando simultáneamente los procedimientos de Conservación de Datos actuales y los electrónicos.

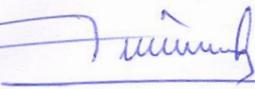
**DISPOSICIÓN DEROGATORIA:**

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

**DISPOSICIÓN FINAL:**

La presente Ley entrará en vigor a los veinte (20) días de su publicación en el Boletín Oficial del Estado, sin perjuicio de su publicación en los demás Medios Informativos Nacionales.

Dada en la Ciudad de Malabo, a veintidós días del mes de Julio del año dos mil dieciséis.


 POR UNA GUINEA MEJOR,  
  
 -OBIANG NGUEMA MBASOGO-  
 PRESIDENTE DE LA REPUBLICA.

*Ley Núm. 1/2.017, de fecha 10 de Enero, de Comunicaciones por Internet en la República de Guinea Ecuatorial.*

### **EXPOSICIÓN DE MOTIVOS:**

En la actualidad la utilización de las nuevas tecnologías de la información y la comunicación, TIC, y de las Comunicaciones por Internet es una realidad en nuestra sociedad, que constituyen un medio importantísimo e indispensable, para transmitir, recibir e intercambiar todo tipo de información. Claro, dicha utilización tanto brinda significantes ventajas, como genera bastantes dificultades y riesgos para todos los sujetos intervinientes en la sociedad de la información, lo que es consecuencia y se deriva en el incremento de las posibilidades de elección de los usuarios y de la ausencia de un marco jurídico que defina los conceptos, términos y figuras, que son de uso frecuente en las Comunicaciones por Internet, y ofrezca garantías jurídicas y confianza a todos ellos en el manejo de las tecnologías de la información y la comunicación y en las Comunicaciones por Internet. Aquello impone la necesidad de elaboración y aprobación de esta Ley.

La presente Ley tiene por objeto la regulación de los diferentes aspectos jurídicos de la sociedad de la información y de la utilización de las tecnologías de información y comunicación, en especial las Comunicaciones por Internet, el comercio electrónico y las medidas sancionatorias aplicables a las conductas que quebranten las relaciones sociales y el orden en dicho sector, que engloban no sólo las administrativas, sino penales, civiles o de cualquier otro tipo, según el bien jurídico afectado, incorporando nuevos conceptos y términos jurídicos al Ordenamiento Jurídico Ecuatoguineano. Así aparece en la presente Ley el concepto de servicios de la sociedad de la información, que integra los de suministro de información por vía electrónica, de la contratación de bienes y servicios por la misma vía, de la provisión de acceso a la red y de la transmisión de datos por redes de telecomunicaciones, de los Prestadores de Servicios por Internet y de los usuarios.

En este contexto, es importante subrayar que la presente Ley introduce dos destacables innovaciones al Ordenamiento Jurídico Ecuatoguineano. Por una parte, establece y regula de manera general la asignación de nombres de dominios de Internet, más concretamente del dominio gq y sus sistemas, que constituye un atributo de la soberanía de la República de Guinea Ecuatorial, es decir, un dominio público. Y por otra, legaliza y regulariza el comercio electrónico, aunque de hecho ya existía en las relaciones entre las diferentes personas en nuestra sociedad que se concretiza en la celebración de contratos por vía electrónica y sus efectos, en las comunicaciones comerciales por Internet, inclusive la publicidad por Internet y sus restricciones.

La presente Ley se estructura en una Exposición de Motivos, cincuenta y seis (56) Artículos, repartidos en seis (6) Títulos y trece (13) Capítulos, siete (7) Disposiciones Adicionales, tres (3) Disposiciones Transitorias, una Derogatoria y una Final. Y en su sentido general, complementa las Disposiciones de la Ley General de Telecomunicaciones, la de Régimen de Acceso a los Servicios Públicos de la Administración General del Estado por Medios Electrónicos y otras Disposiciones Reguladoras del Gobierno Electrónico en la República de Guinea Ecuatorial.

En su virtud, haciendo uso de las prerrogativas que Me confiere la Ley Fundamental; a propuesta del Gobierno y previa aprobación por el Parlamento Nacional en su Segundo Periodo Ordinario de Sesiones correspondiente al año 2.016, Sanciono y Promulgo la presente:

*Ley de Comunicación por Internet en la República de Guinea Ecuatorial.*

## **TÍTULO I**

### **DISPOSICIONES GENERALES**

#### **CAPÍTULO ÚNICO**

#### **DEL OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES**

*Artículo 1. Objeto.* Constituyen objeto de esta Ley:

- 1) La regulación del régimen de la actividad y de los Servicios de la Tecnología de la Información y Comunicación, y de la sociedad de la información en general; de la asignación de nombres de dominios por Internet y de la utilización del dominio gq; de la contratación por vía electrónica, así como de las obligaciones de los Prestadores de los Servicios de Internet y del Régimen Sancionador aplicable a los mismos.
- 2) La regulación de la actividad y las obligaciones de los intermediarios que transmiten diferentes contenidos por las redes de telecomunicación, las comunicaciones comerciales por medios electrónicos y la información sobre los documentos y contratos electrónicos, su validez y eficacia.
- 3) Los Juegos de Azar, que impliquen apuestas de valor económico, y los Servicios de la Sociedad de la Información con finalidad económica, sin perjuicio de lo previsto particularmente en su legislación especial y de la aplicación del principio de libre prestación de servicios.

**Artículo 2. Los Servicios.** Son servicios de la sociedad de la información con finalidad y actividad económica:

- a) La contratación de bienes o servicios por vía electrónica.
- b) La gestión y organización de venta, compra, mercados, centros comerciales virtuales y subastas por vía electrónica y en las redes.
- c) El suministro y envío de comunicaciones comerciales por vía telemática.
- d) Cualquier otra actividad o prestación de servicios relacionados con las anteriores.

**Artículo 3. Ámbito de Aplicación. 1.** La presente Ley se aplicará a los servicios que se prestan en la esfera de la sociedad de la información, de la tecnología de la información y comunicación, de la asignación de nombres de dominio por Internet y del dominio gq, y en el proceso del comercio electrónico y a los prestadores de dichos servicios, los cuales pueden ser:

- a) Prestadores de servicios establecidos en la República de Guinea Ecuatorial.
  1. Se entenderá que un Prestador de Servicios de la Sociedad de la Información está establecido en la República de Guinea Ecuatorial, cuando tenga una residencia o domicilio social en el Territorio Nacional, que coincidan con el lugar en que efectivamente realiza su gestión administrativa y ejerce la dirección de sus negocios.
  2. Se presumirá que el Prestador de Servicios está establecido en la República de Guinea Ecuatorial cuando se hallare inscrito en algún Registro Público oficialmente habilitado para su inscripción y adquisición de la personalidad jurídica o los estuviere una de sus filiales, sucursales o representaciones.
- b) Prestadores de Servicios establecidos en otro Estado, que tengan establecimiento permanente situado en el Territorio de la República de Guinea Ecuatorial, aunque su residencia o domicilio social se encuentre sito en otro Estado, o que dirijan sus servicios específicamente a la República de Guinea Ecuatorial y se quedaren sujetos a las disposiciones de esta Ley sin que quebranten lo previsto en los Tratados y Convenios Internacionales aplicables, o cuando el destinatario de los servicios radique en el Territorio de la República de Guinea Ecuatorial y sus servicios afecten las materias siguientes:
  - 1) Derecho de la Propiedad Intelectual o Industrial.
  - 2) Actividad de Seguro realizada en régimen de libre prestación de servicios o de derecho de establecimiento.
  - 3) Publicidad relacionada con las Instituciones de Inversión o solicitud de Comunicaciones Comerciales por correo u otro medio electrónico.
  - 4) Obligaciones derivadas de los contratos de régimen de elección por las partes de la Ley aplicable a su contrato.

2. Se entenderá que el Prestador de Servicios actúa mediante un Establecimiento Permanente situado en la República de Guinea Ecuatorial, cuando tenga o disponga de instalaciones u oficinas en que realice de forma continuada y habitual parte o toda su actividad.

3. A los efectos de lo dispuesto en los párrafos anteriores, la utilización de medios tecnológicos situados en la República de Guinea Ecuatorial para la prestación de servicios de la sociedad de la información o el acceso a los servicios de la misma, no tendrá la consideración para estimar o determinar por sí solo el Establecimiento de cualquier Prestador en el Territorio de la República de Guinea Ecuatorial.

**Artículo 4. Servicios Excluidos del Ámbito de Aplicación de esta Ley.** 1. Los servicios prestados por los Notarios, Registradores y Abogados quedan excluidos del Ámbito de Aplicación de la presente Ley, rigiéndose por las disposiciones legales que regulan específicamente su actividad.

2. Tampoco tendrán la consideración de servicios prestados por Internet:

- a) Los servicios prestados por vía de telefonía vocal, fax o télex.
- b) Los intercambios de información por correo electrónico u otro medio electrónico de comunicación equivalente sin finalidad económica.
- c) Los servicios de radiodifusión sonora y televisiva, los teletextos y guías electrónicas de programas.
- d) Cualquier otro servicio relacionado con los anteriores.

**Artículo 5. Definiciones.** A los efectos de la presente Ley se entiende por:

- a) **Comunicación por Internet:** Toda información transmitida por vía electrónica o por los medios tecnológicos equivalentes.
- b) **Comunicación Comercial:** Todo tipo de comunicación o información dirigida directa o indirectamente para la promoción de una actividad comercial, industrial, profesional, artesanal, de una persona, empresa u organización, así como de sus

bienes, imagen o servicios. De lo anterior se exceptúan los datos que permiten acceder a la actividad de una persona, empresa u organización, como son el nombre de dominio o la dirección del correo electrónico, y las comunicaciones o informaciones ofrecidas sobre los bienes, servicios e imagen de una persona, empresa u organización, si fueren elaboradas por un tercero y sin contraprestación económica.

- c) **Asignación de Nombres de Dominios por Internet:** Es la actividad realizada por el Órgano o Institución competente para adjudicar a cada usuario un nombre determinado a utilizar en sus comunicaciones por Internet, bajo el Código de País correspondiente.
- d) **Dominio gq:** Es el Código distintivo y propio por Internet que corresponde a la República de Guinea Ecuatorial y constituye su Dominio Público, gestionado por el Órgano competente designado al efecto.
- e) **Servicios de la Sociedad de la Información:** Todo negocio, actividad o producto de estos, prestado por vía electrónica a título oneroso a petición del destinatario o a título no remunerado, siempre que constituya una actividad económica para el prestador de servicios.
- f) **Servicio de Intermediación:** El que facilita la prestación o utilización de los servicios de comunicación por Internet o de la Sociedad de la Información, o provee el acceso a la información por vía electrónica, la transmisión de datos por las redes de telecomunicación, la realización de las copias temporales de las páginas de internet solicitadas por los usuarios, el alojamiento o almacenamiento de dichos datos, aplicaciones o productos (servicios) suministrados por otros servidores o prestadores de servicios y la dotación o provisión de medios e instrumentos de búsqueda, acceso y recopilación de datos o enlaces a otras páginas o sitios web de Internet.
- g) **Prestador de Servicios o Prestador:** La persona física o jurídica que proporciona

un servicio de comunicación o información por Internet o de la Sociedad de la Información.

- h) **Destinatario:** La persona física o jurídica que utiliza un servicio de comunicación o de la Sociedad de la Información por Internet.
- i) **Órgano Competente:** Toda Entidad o Institución Jurisdiccional o Administrativa que actúa en ejercicio de las competencias que le están atribuidas por Ley.
- j) **Contrato Electrónico:** Acuerdo o pacto en el que la oferta y la aceptación de las partes se transmitan y se celebran por vía electrónica, utilizando los equipos electrónicos de tratamiento y almacenamiento de datos mediante conexión a una red de telecomunicaciones.
- k) **Ámbito Normativo Coordinado:** El conjunto de todos los requisitos aplicables a los Prestadores de Servicios, establecidos por la presente Ley y por las demás Leyes generales y especiales respecto al comienzo de la actividad, las titulaciones o cualificaciones profesionales o académicas, Autorizaciones Administrativas o colegiales, a la publicidad registral, a la calidad, seguridad y contenido de los servicios, al régimen de notificaciones y comunicación con las Instituciones Públicas o Privadas, y a la modificación, suspensión o extinción de la actividad.

**Artículo 6. Obligatoriedad del Ordenamiento Jurídico vigente.** 1. Los Prestadores de Servicios por Internet o de la Sociedad de la Información, establecidos en la República de Guinea Ecuatorial, estarán sujetos a todas las disposiciones del Ordenamiento Jurídico vigente, que les sean aplicables en función de la actividad que realizan y con independencia de la utilización de los medios electrónicos.

2. Los Prestadores de Servicios establecidos en otro Estado con el destinatario radicado en la República de Guinea Ecuatorial quedan sometidos a lo establecido por el Ordenamiento Jurídico Nacional vigente en cuanto a la materia a que se dedique.

3. Las disposiciones de esta Ley se entenderán sin perjuicio de lo previsto en las demás normas vigentes, que tratan de la protección de la salud, seguridad y defensa nacional, la competencia desleal, protección de datos personales y otras esferas de la vida social.

4. La constitución, transmisión, modificación y extinción de los derechos reales sobre los bienes inmuebles sitos en la República de Guinea Ecuatorial, se ajustarán a lo dispuesto por la legislación ecuatoguineana en cuanto a los requisitos de su validez y eficacia.

## TÍTULO II DEL RÉGIMEN DE PRESTACIÓN DE SERVICIOS POR INTERNET

### CAPÍTULO I DE LA LIBRE PRESTACIÓN DE SERVICIOS POR INTERNET

**Artículo 7. Principio de Libre Prestación de Servicios por Internet.** La Prestación de Servicios de Comunicación por Internet o de la Sociedad de la Información estará sujeta sólo y únicamente al principio de Libre Prestación de Servicios y al Régimen General de las Autorizaciones Administrativas y de los requisitos registrales establecidos por el Ordenamiento Jurídico vigente, sin sujeción a otros tipos de Autorizaciones previas, excepto en los supuestos previstos en los apartados del inciso b) del Artículo 2 y en las restricciones y exigencias de cooperación de los Artículos 7 y 8 de la presente Ley y en los establecidos en los Acuerdos Internacionales.

**Artículo 8. Restricciones a la Libre Prestación de Servicios.** 1. El Órgano Judicial competente, a instancia de la parte perjudicada, la Administración o el Ministerio Fiscal, podrá adoptar las medidas necesarias de interrupción o de retiro de los Datos Electrónicos, cuando la prestación de servicios de la sociedad de la información atente o pueda atentar contra los derechos y libertades fundamentales de las personas, la seguridad y la defensa nacional, el orden público, la protección de la salud pública y de las personas individualmente, la seguridad y protección de los derechos y educación de la infancia y de la juventud, los derechos de la propiedad, incluida la intelectual e

industrial, o contra la dignidad e integridad de las personas y al principio de no discriminación por motivos de raza, sexo, religión, opinión, discapacidad o cualquier otra circunstancia personal o social, o contra cualquier procedimiento judicial.

**2.** En la adopción de las aludidas medidas se respetarán las garantías, normas y procedimientos previstos en la legislación vigente para proteger los derechos, la libertad de expresión o la libertad a la información, la intimidad personal, familiar y los datos personales de los individuos, cuando estos pudieran resultar afectados.

**3.** Las medidas a que se refiere en el presente Artículo deberán ser objetivas, proporcionadas y no discriminatorias, y se aplicarán de forma cautelar o definitiva en ejecución de la Resolución que se dicte.

**Artículo 9. Cooperación en la Restricción a la Libre Prestación de Servicios.** **1.** El Órgano competente para identificar al responsable de las actuaciones ilícitas previstas en el Artículo anterior podrá requerir la Cooperación de los Prestadores de Servicios, de ceder los datos que permitan su identificación, previa presentación de la Autorización de la Autoridad Judicial, quedándose aquellos obligados a facilitar los datos necesarios para la efectividad de dicho proceso, y de hacer efectivas y garantizar las medidas adoptadas.

**2.** La misma cooperación se podrá requerir a los prestadores de Servicios de Intermediación.

**3.** La adopción de las medidas aludidas a la prestación de servicios de los prestadores establecidos en otro Estado se realizará mediante los procedimientos de Cooperación Internacional, sin perjuicio de lo previsto en las Leyes Procesales y en la Cooperación Judicial.

**4.** En todo caso, el Órgano competente por Vía Diplomática de Asuntos Exteriores remite la petición al Estado del Prestador de Servicios, cuya conducta se considera ilícita, de adoptar las medidas arriba indicadas, o le notifica las medidas adoptadas para que se hagan efectivas. Este será el procedimiento que también aplicará el otro Estado en este tipo de casos.

## CAPÍTULO II DE LA ASIGNACIÓN DE NOMBRES DE DOMINIO BAJO EL CÓDIGO gq

**Artículo 10. Criterios para la Asignación de Nombres de Dominio bajo el Código gq.** **1.** La Asignación de Nombres de Dominio de Internet bajo el Código gq se realizará conforme al Plan Nacional de Nombres de Dominio de Internet de la República de Guinea Ecuatorial, a las prácticas y recomendaciones de los Organismos Internacionales Especializados en la gestión del Sistema de Nombres de Dominio de Internet y a las normas reglamentarias de la presente Ley.

**2.** Las Asignación de Nombres de Dominio bajo el Código gq deberá basarse en criterios que garanticen la seguridad jurídica, los derechos y libertades de las personas, la agilidad y la confianza en los procedimientos de Registro y en las Comunicaciones por Vía Electrónica, diferenciando los niveles de la asignación de cada Nombre de Dominio con la creación de los correspondientes indicativos que permitan identificar su titular, su actividad principal y sus contenidos.

**Artículo 11. El Plan Nacional de Nombres de Dominios bajo el Código gq.** **1.** El Plan Nacional de Nombres de Dominio de Internet se aprobará y se desarrollará de forma reglamentaria, que integrará los diferentes niveles de dominio, los procedimientos para la asignación de los mismos y las demás operaciones indispensables para el Registro de Nombres de Dominio y Direcciones de Internet.

**2.** En el Plan Nacional de Nombres de Dominio de Internet bajo el Código gq se determinarán y se establecerán mecanismos para detectar y prevenir el registro abusivo, fraudulento o especulativo de los mismos, el uso indebido de nombres de dominios que pertenezcan a otras personas, evitando siempre aquellos que puedan llevar a la confusión o conflictos entre usuarios.

**Artículo 12. Autoridad de Asignación de Nombres de Dominio.** **1.** El Órgano que se designe al efecto será la Autoridad de Asignación de Nombres de Dominio bajo el Código gq, al que corresponderá la gestión del registro de los mismos.

2. Corresponderá a la Autoridad de Asignación la incoación de los expedientes de infracciones previstas en la presente Ley, salvo las reservadas a los Órganos Superiores y Judiciales; y para proponer al Gobierno las medidas cautelares de suspensión o cancelación de nombres de dominio gq.

3. Sólo la Autoridad Judicial será competente para requerir la suspensión y cancelación referidas mediante una Resolución motivada.

**Artículo 13. Personas Capacitadas para solicitar la Asignación de Nombres de Dominio bajo el Código gq.** 1. Todas las personas físicas y jurídicas que lo deseen y tengan interés para ello podrán solicitar la Asignación de Nombres de Dominio bajo el Código gq, siempre que cumplan con los requisitos que se establezcan en el Plan Nacional de Asignación de Nombres de Dominios para su obtención.

2. La presentación de solicitudes y las correspondientes notificaciones se realizarán por vía electrónica, salvo se prevea otro supuesto en los procedimientos de asignación.

3. Los Nombres de Dominio bajo el Código gq se asignarán al primer solicitante. Dicha asignación confiere a cada titular del Nombre de Dominio el derecho a su utilización, conforme a los requisitos que en cada caso se establezcan y a la obligación de mantenerlo en el tiempo.

4. Los Titulares y los Registradores de un Nombre de Dominio bajo el Código gq deberán respetar las reglas y condiciones técnicas que establezca la Autoridad de Asignación para el normal funcionamiento del Sistema de Nombres de Dominio bajo el Código gq, los derechos de Propiedad Intelectual o Industrial que correspondan a la persona o Entidad para la que se haya registrado dicho nombre de dominio, así como asumir la responsabilidad en el uso correcto del nombre de dominio.

### **CAPÍTULO III DEL PRESTADOR DE SERVICIOS DE COMUNICACIÓN POR INTERNET**

**Artículo 14. El Prestador de Servicios de Comunicación por Internet.** El Prestador de Servicios de Comunicación por Internet o de la Sociedad de la Información, siendo la persona física o jurídica, cuya actividad principal consiste en proporcionar y facilitar los medios tecnológicos y electrónicos a los destinatarios y a los usuarios el acceso a las redes de telecomunicación para comunicar por Internet, goza de todos los derechos para el ejercicio de su cometido y tiene el deber de cumplir ciertas obligaciones frente aquellos y la sociedad en general, y de asumir responsabilidades por las infracciones que pudiera cometer.

**Artículo 15. El Prestador de Servicios de Comunicación por Internet y los Códigos Deontológicos de su actividad.** 1. Los Prestadores de Servicios de Comunicación por Internet elaborarán los Códigos Deontológicos, que establecerán las conductas voluntarias a acatar y aplicar por todos en la Sociedad de la Información, regulando los procedimientos aplicables para la detección y retirada de contenidos e información nocivos e ilícitos, para la protección de los destinatarios y usuarios de los envíos de comunicaciones comerciales no solicitadas por vía electrónica, y para la Resolución Extrajudicial de conflictos que surjan en el proceso de Prestación de Servicios de Comunicación por Internet.

2. Los referidos códigos de conducta deberán ser accesibles para todos los destinatarios y usuarios por cualquier medio más fácil y directo, en especial por vía electrónica.

3. Los Órganos Competentes y Poderes Públicos velarán por la efectiva elaboración y aplicación de dichos códigos de conducta y la regulación en sus contenidos de las normas que protegen y garantizan los derechos de la juventud, infancia, de la intimidad, dignidad e integridad de la persona, de los discapacitados y de los datos personales y familiares del individuo.

**Artículo 16. Derechos del Prestador de Servicios de Comunicación por Internet.** Todo Prestador de Servicios gozará, además del régimen de libre prestación de Servicios de Comunicación por Internet, de todos los derechos reconocidos por la

presente Ley y por la legislación vigente en relación a su persona y a la actividad que realiza.

**Artículo 17. Obligaciones Generales del Prestador de Servicios de Comunicación por Internet.**

**1.** Todo Prestador de Servicios de la Sociedad de la Información o de Comunicación por Internet deberá disponer de los medios tecnológicos y electrónicos que permitan a los destinatarios o usuarios y a los Órganos Competentes de la Administración, acceder y obtener de forma fácil, gratuita, directa y permanente, la información sobre:

- a) Su nombre o denominación social, residencia o domicilio, sus direcciones de establecimiento y de correo electrónico o página web, o cualquier otro dato que facilite el contacto directo con él.
- b) Los datos de Inscripción en los Registros Públicos a los efectos de determinación y adquisición de su responsabilidad jurídica y de la publicidad y, en su caso, en los Colegios Profesionales, cuando se ejerce una profesión regulada, adjuntando la titulación académica y el Certificado de Homologación.
- c) Los datos relativos a la Autorización Administrativa y al Número de Identificación Fiscal (N.I.F.), que permitan su identificación y supervisión o inspección.
- d) La indicación y facilitación clara y exacta sobre los precios de los servicios o productos que presta, con o sin impuestos.
- e) La indicación sobre el acatamiento de los Códigos Deontológicos y conductuales, precisando la forma de consultarlos electrónica y directamente.

**2.** Si el Prestador de Servicios de Comunicación por Internet incluye toda la información requerida en el punto anterior en su página o sitio web, se tendrá por cumplida dicha obligación.

**Artículo 18. Obligación del Prestador de Comunicación por Internet de informar sobre la Tarificación Adicional al Usuario.**

**1.** Cuando se haya asignado un rango de numeración telefónica a Servicios de Tarificación Adicional, en el que

se permita el acceso a la Comunicación por Internet y se requiera su utilización por parte del Prestador de dichos servicios, esta utilización y la descarga de programas informáticos, que ejecuten las funciones de marcación, deberán realizarse con el consentimiento previo y expreso del usuario, quedando obligado el Prestador de Servicios de proporcionar y facilitar la información sobre:

- a) Las características de los servicios que presta y va a proporcionarle.
- b) Las funciones que efectúan los programas informáticos a descargar y el número de teléfono que se marcará para dicha descarga.
- c) Los procedimientos para dar fin a la conexión de tarificación adicional con explicación precisa del momento concreto en que se producirá el fin, y para restablecer el número de conexión previo a la conexión de tarificación adicional.

**2.** El Prestador de Servicios de Comunicación por Internet deberá disponer la anterior información de manera clara, visible e identificable, lo que se entenderá sin perjuicio de lo previsto en la Ley General de Telecomunicaciones sobre los requisitos aplicables para el acceso por los usuarios a los rangos de numeración telefónica atribuidos a los Servicios de Tarificación Adicional.

**Artículo 19. Colaboración en la lucha contra las Actividades Ilícitas.**

**1.** Los Prestadores de Servicios de la Sociedad de la Información, los Registros y los Agentes Registradores de Nombres de Dominio y los propios titulares, están obligados a prestar la colaboración necesaria con la Autoridad de Asignación y con los Órganos Públicos Competentes en la lucha contra Cibercriminalidad y demás infracciones que pudieran cometerse en las comunicaciones por internet para garantizar la Ciberseguridad en las mismas, facilitando a las Autoridades Públicas los datos solicitados o requeridos en ejercicio de sus competencias de inspección, control y sanción, así mismo, cuando sean necesarios para la investigación de incidentes de Ciberseguridad.

2. En los supuestos referidos, la solicitud deberá formularse mediante escrito motivado en el que se especificarán los datos requeridos, el fin que se persigue y la obligación de facilitar dichos datos y de respetar el secreto de las comunicaciones.

**Artículo 20. Obligación de Colaboración del Prestador de Servicios de Intermediación.** 1. Todo Prestador de Servicios de Intermediación tiene la obligación de suspender o interrumpir la prestación de un determinado Servicio o Comunicación por Internet, y de retirar determinados contenidos provenientes de cualquier prestador de servicios, cuando así lo requiera y exija el Órgano Competente en el ejercicio de sus competencias legales; así como de garantizar la efectividad de la Resolución en la que se acuerde la suspensión o interrupción o la retirada de contenidos procedentes de un prestador establecido fuera de la República de Guinea Ecuatorial a petición de otro Estado.

2. En la adopción y cumplimiento de las aludidas medidas se respetarán las garantías, las normas jurídicas y los procedimientos previstos en la legislación vigente para proteger los datos personales del individuo, los derechos a la intimidad personal y familiar y a la libertad de expresión o a la libertad de la información, cuando estos pudieran resultar afectados, ajustándose siempre a los principios de objetividad, proporcionalidad y a la no discriminación.

3. Las referidas medidas podrán ser adoptadas de forma cautelar o en ejecución de la Resolución que se dicte, conforme al procedimiento administrativo.

4. Solo la Autoridad Judicial será competente para adoptar las medidas arriba indicadas, en especial, la de retirada o secuestro de la página o sitio web.

**Artículo 21. Obligación de Información sobre Seguridad.** 1. Los Prestadores de Servicios de Intermediación estarán obligados a informar a sus clientes, de forma fácil, gratuita, directa y permanente, sobre los diferentes medios técnicos y tecnológicos que aumentan los niveles de seguridad de comunicación y permitan la protección frente

a los virus informáticos y a los programas espías, así como la restricción de los correos electrónicos no deseados.

2. Los Proveedores de Servicios de Acceso a Internet y los Prestadores de Servicios de Correo Electrónico o de Servicios Similares, deberán informar gratuitamente a sus clientes sobre las medidas de seguridad que apliquen en el proceso de provisión de dichos servicios.

3. Aquellos también les informarán sobre las herramientas y medios existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados y nocivos para la juventud y la infancia.

4. Los Prestadores de Servicios de Intermediación, los Proveedores de Servicios de Acceso a Internet y los Prestadores de Servicios estarán obligados a informar a sus clientes sobre las responsabilidades en que pueden incurrir por el uso de la comunicación por internet con fines ilícitos para cometer infracciones legales o contravenir las disposiciones legales vigentes.

5. Si la información referida se incluye en la página web del Prestador o Proveedor de Servicios, se entenderá por cumplida la obligación arriba indicada.

### TÍTULO III

## DEL RÉGIMEN JURÍDICO DEL COMERCIO Y DE LA CONTRATACIÓN POR VÍA ELECTRÓNICA

### CAPÍTULO I

## DE LAS COMUNICACIONES COMERCIALES ELECTRÓNICAS

**Artículo 22. Régimen Jurídico de las Comunicaciones Comerciales Electrónicas.** 1. Las Comunicaciones Comerciales realizadas por Vía Electrónica se registrarán por las disposiciones de la presente Ley y por la legislación vigente en materia comercial, en especial por la Protección de Datos Personales en lo relativo a la obtención, creación y al mantenimiento de ficheros de los mismos.

2. Lo dispuesto en el párrafo anterior será de aplicación en los casos de las ofertas promocionales y de publicidad.

**Artículo 23. Requisitos a reunir por las Comunicaciones Comerciales, Ofertas Promocionales y Concursos por Vía Electrónica.** 1. Las Comunicaciones Comerciales, las Ofertas Promocionales con descuentos, premios o regalos, los Concursos o Juegos Promocionales realizados por vía electrónica y la persona física o jurídica que las efectúa o en nombre de quien se realizan, deberán ser claros e identificables.

2. Si dichas comunicaciones, ofertas, concursos o juegos promocionales se realizaren a través del Correo Electrónico o por otro medio electrónico equivalente, obligatoriamente se incluirá o se indicará al comienzo del mensaje la palabra “Publicidad” o su abreviatura “pub”.

3. En el caso de las Ofertas Promocionales y Publicitarias con descuentos, premios o regalos y de concursos o juegos promocionales y publicitarios, serán requisitos indispensables la previa obtención de la correspondiente Autorización y la garantía de que las condiciones de acceso y de participación sean fáciles y sean expuestas de forma clara e inequívoca, y de que se hagan entrega de lo ganado u obtenido en tiempo más breve posible.

**Artículo 24. Prohibición de Comunicaciones Comerciales Ocultas, disimuladas o no Autorizadas.** 1. Está totalmente prohibido el envío de comunicaciones comerciales en las que se oculte o se disimule la identidad de la persona física o jurídica que efectúe la comunicación o en nombre de quien se realice la misma, y de aquellas en las que se incite o se instruya a los destinatarios a visitar páginas o sitios web que violen lo dispuesto en el Artículo anterior.

2. También está prohibido el envío de comunicaciones promocionales o publicitarias por correo electrónico u otro medio tecnológico equivalente, que no hubiere sido previamente solicitado y expresamente autorizado por los destinatarios de las mismas, y el que no contenga la dirección electrónica válida.

3. Todo Prestador de Servicios deberá ofrecer al destinatario la posibilidad de oponerse o rechazar el tratamiento de sus datos con fines promocionales o publicitarios en cualquier momento mediante un procedimiento sencillo y gratuito, que deberá incluir una dirección electrónica válida para ejercitar este derecho.

**Artículo 25. Derechos del Destinatario de las Comunicaciones Comerciales.** 1. El destinatario gozará del derecho de revocar en cualquier momento el consentimiento prestado a la recepción de la comunicación comercial con la simple notificación de su voluntad al remitente de la oferta.

2. Los procedimientos que establezcan los Prestadores de Servicios para la revocación del consentimiento deberán ser sencillos, accesibles y gratuitos para los destinatarios. Si fuere por correo electrónico, dicho medio deberá incluir la dirección electrónica válida para ejercitar este derecho, y siendo de aplicación lo dispuesto en el segundo párrafo del Artículo anterior.

3. Asimismo, deberán facilitar información accesible por medios electrónicos sobre los procedimientos aludidos en el párrafo anterior.

4. Solo bajo el consentimiento del destinatario y después de facilitar la información necesaria, clara y competente sobre la finalidad de utilización y tratamiento de sus datos, el Prestador de Servicios podrá hacer uso de los dispositivos de almacenamiento y recuperación de los mismos en los equipos terminales del destinatario. Dicho consentimiento de tratamiento de sus datos, cuando técnicamente sea posible y eficaz, podrá ser facilitado mediante el uso del navegador u otro medio aplicable tecnológicamente, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.

5. No obstante, la condición de notificación y expresión de consentimiento del destinatario no impedirá el posible almacenamiento o acceso de carácter técnico con el solo y único fin de realizar la transmisión de una comunicación por vía electrónica o para la prestación de un servicio de comunicación por Internet, solicitado expresamente por el destinatario.

## CAPÍTULO II DE LA CONTRATACIÓN POR VÍA ELECTRÓNICA

**Artículo 26. Régimen Jurídico de la Contratación por Vía Electrónica.** La Contratación entre las partes realizada por Vía Electrónica se regirá por las disposiciones de la presente Ley y por la legislación vigente en la materia de que se trate, en especial en lo relativo al tipo y objeto de cada uno de los contratos celebrados por Vía Electrónica, así como a su validez y eficacia.

**Artículo 27. Validez y Eficacia del Contrato celebrado por Vía Electrónica. 1.** Todo Contrato celebrado por Vía Electrónica producirá todos los efectos previstos por la legislación vigente, cuando concurren el consentimiento y todos los demás requisitos necesarios para su validez, y se regirá por lo dispuesto en el Código Civil, en el Código de Comercio, en la presente Ley y en las demás disposiciones legales sobre los Contratos y la Actividad Comercial.

**2.** Para que sea válido cualquier Contrato Electrónico, será necesario el acuerdo previo de las partes sobre la utilización de medios electrónicos.

**3.** Los Contratos, negocios y demás actos jurídicos, en los que la Ley exige para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de Órganos Jurisdiccionales, Notarios, Registradores de la Propiedad o Mercantiles o de cualquier Autoridad Pública, se regirán por su legislación especial o específica.

**4.** Cuando la Ley exija o requiera que el Contrato o cualquier información relacionada con el mismo consten por escrito, este requisito se entenderá cumplido y satisfecho, si el contrato y la información referida se contienen y se presentan en un soporte electrónico.

**5.** Lo dispuesto en los párrafos anteriores no será de aplicación a los Contratos relativos al derecho de la familia y de sucesiones.

**Artículo 28. Obligaciones previas al Inicio del Procedimiento de Contratación. 1.** El Prestador de Servicios de Comunicación por Internet que

realice la Actividad de Contratación Electrónica, además de cumplir los requisitos exigidos por la legislación vigente, antes del inicio del procedimiento de aquella y mediante técnicas adecuadas al medio de comunicación utilizado, tendrá la obligación de poner a disposición del destinatario, de forma gratuita, fácil y permanente, la información clara, comprensible e inequívoca sobre:

- a) Los distintos trámites que deben seguirse para celebrar el contrato.
- b) Los medios técnicos que pone a disposición para identificar y corregir errores en la introducción de los datos.
- c) El archivo y accesibilidad del documento electrónico en que se formalice el contrato.
- d) Las condiciones generales a las que deba sujetarse el contrato para ser almacenadas y producidas o reproducidas por el destinatario.

**2.** Las referidas obligaciones se entenderán cumplidas, si el Prestador de Servicios las incluye en su página o sitio de Internet, o facilita de manera permanente, fácil, directa y exacta la dirección de Internet que dicha información es puesta a disposición del destinatario.

**3.** No obstante, lo anterior, el Prestador de Servicios no tendrá la obligación de facilitar la información a que se hace referencia en el apartado anterior, cuando:

- a) Ambos contratantes así lo acuerden.
- b) El Contrato se haya celebrado exclusivamente mediante intercambio de Correo Electrónico u otro tipo de Comunicación Electrónica equivalente.

**4.** Las ofertas o las propuestas de contratación realizadas por Vía Electrónica serán válidas durante el periodo que fije el oferente o, en su defecto, durante el tiempo que permanezca accesible a los destinatarios, sin perjuicio de lo dispuesto en la legislación especial o específica.

**Artículo 29. Prueba del Contrato celebrado por Vía Electrónica. 1.** La prueba de celebración de un Contrato Electrónico y la de las obligaciones

que tienen su origen en dicho Contrato, se sujetarán a las disposiciones o reglas generales de la legislación vigente.

2. Cuando el Contrato Electrónico esté firmado electrónicamente, se registrará por lo dispuesto en la Ley de Firma y Documentos Electrónicos.

3. El soporte electrónico en que conste un Contrato Electrónico será admitido en juicio como prueba documental.

**Artículo 30. Lugar de Celebración del Contrato.**

El Contrato Electrónico se presumirá celebrado, en defecto de un acuerdo concreto entre las partes, en la residencia, domicilio o lugar en que esté establecido el Prestador de Servicios, salvo que una legislación especial o específica disponga lo contrario.

**Artículo 31. Intervención de Terceros de Confianza.**

1. Las partes contratantes podrán pactar que un tercero archive las cláusulas contractuales electrónicas y consigne la fecha y hora en que dichas comunicaciones hayan tenido lugar.

2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por Vía Electrónica entre las partes en el tiempo estipulado que, en ningún caso, podrá ser inferior a cinco años.

3. La intervención de terceros no podrá alterar ni sustituir las funciones de los Funcionarios o Personalidades Públicos facultados por el derecho para dar fe pública.

**Artículo 32. Información posterior a la Celebración del Contrato.** 1. El oferente está obligado a confirmar la recepción de la aceptación por uno de los medios siguientes:

- a) El envío de un acuse recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección señalada del aceptante en el plazo de 48 horas siguientes a la recepción de la aceptación.
- b) La confirmación, por cualquier medio electrónico utilizado en el proceso de contratación, de la aceptación recibida en el plazo de 24 horas siguientes al día que

el aceptante haya completado el procedimiento de contratación, siempre que la confirmación pueda ser archivada por el destinatario.

2.- Cuando la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición de aquel alguno de los medios indicados en el punto anterior. Esta obligación será exigible tanto si la confirmación se dirigiera al propio prestador o como lo fuera para otro destinatario.

3.- Se entenderá que se ha recibido la aceptación y su confirmación, cuando las partes, a que se dirijan, puedan tener constancia de ello. Si la recepción de la aceptación se confirma mediante acuse de recibo, se presumirá que su destinatario pueda tener la referida constancia desde que aquel haya sido almacenado en el servicio en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

**Artículo 33. Exclusión de la Confirmación de la Recepción de la Aceptación.** No será necesaria la confirmación de la recepción de aceptación de la oferta a que se hace referencia en el Artículo anterior, cuando:

- a) Ambas partes contratantes así lo acuerden.
- b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, si estos medios no se utilizan con el propósito de eludir el cumplimiento de aquella obligación.

**Artículo 34. Ley Aplicable a los Contratos Electrónicos.** Para la determinación de la Ley Aplicable a los Contratos Electrónicos se sujetará a lo dispuesto en la legislación vigente de la República de Guinea Ecuatorial en consonancia con lo estipulado en el Artículo 3 de esta Ley.

**TÍTULO IV  
DE LAS RESPONSABILIDADES DEL  
PRESTADOR DE SERVICIOS Y EL  
CONTROL DE SU ACTIVIDAD**

## CAPÍTULO I DEL RÉGIMEN DE RESPONSABILIDADES DEL PRESTADOR DE SERVICIOS

**Artículo 35. Las Responsabilidades del Prestador de Servicios.** Todo Prestador o Proveedor de Servicios de Comunicación por Internet y Operadores de Redes están sujetos al régimen de responsabilidades previsto en la presente Ley, sin perjuicio de las establecidas con carácter general en la legislación vigente.

**Artículo 36. Responsabilidad de los Proveedores de Acceso a una Red y Operadores de Redes de Telecomunicación.** 1. Los Proveedores de Acceso a una Red de Telecomunicaciones y los Operadores de Redes de Telecomunicaciones, que presten servicios de intermediación, consistente en transmitir por la misma los datos facilitados por el destinatario del servicio o en facilitar el acceso a esta, serán responsables por la información transmitida, si dicha transmisión fuere de su propia iniciativa, modificando los datos ofrecidos por el destinatario o seleccionándolos para otros destinatarios.

2.- No será modificación la manipulación estrictamente técnica de los archivos de datos que se realice y tenga lugar en el proceso y actividad de transmisión de la información.

3.- La actividad de transmisión y provisión de acceso incluye el almacenamiento automático, provisional y transitorio de los datos, permitiendo exclusivamente su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

**Artículo 37. Responsabilidad del Prestador de Servicios de las Copias Temporales de los Datos solicitados por los Usuarios.** Todo Prestador de Servicios de Intermediación que transmita por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que lo soliciten o los almacenen en sus sistemas de forma automática, provisional y temporal, no será responsable por el contenido de estos datos, ni por la reproducción temporal de los mismos, si:

- a) No modifica la información que contienen.
- b) Permite el acceso a ellos solo a los destinatarios que cumplan las condiciones exigidas e impuestas por el destinatario, cuya información se solicita.
- c) Respeta las normas establecidas aplicables para la actualización de este tipo de información.
- d) Retira la información que haya almacenado o hace imposible el acceso a los datos que contiene, siempre que esté seguro que dicha información ha sido retirada de la red en que se encontraba inicialmente, o que se ha imposibilitado o inhabilitado el acceso a ellos, o que el Órgano Competente Juridicial o Administrativo haya ordenado su retirada o prohibido el acceso a ellos.
- e) No interfiere en la utilización lícita de la tecnología aceptada y empleada con el propósito de obtener datos sobre la utilización de la información.

**Artículo 38. Responsabilidad del Prestador de Servicios de Alojamiento o Almacenamiento de Datos.** 1. Todo Prestador de Servicio de Intermediación consistente en alojar o almacenar los datos proporcionados por el destinatario de este servicio será responsable por la información o datos alojados o almacenados a petición de éste, si tuviera conocimiento efectivo de que dicha información, datos y actividad son lícitos, o de que lesionan los intereses, bienes o derechos de un tercero, o de que no haya actuado con diligencia debida para retirarlos o hacer imposible el acceso a los mismos, o de que el destinatario actuare bajo la dirección, influencia, autoridad, instrucción o control de aquél.

2.- Se entenderá que el Prestador tiene conocimiento efectivo, cuando no haya aplicado los existentes procedimientos de acuerdos voluntarios de detección y de retirada de la información o datos nocivos y perjudiciales, pero con posterioridad a ello y por resolución del Órgano Competente se haya declarado la ilicitud de dicha información o datos, ordenando su retirada, la imposibilidad de acceso a los mismos o la existencia de la lesión a tercero.

**Artículo 39. Responsabilidad de los Prestadores de Servicios de Enlaces o de los Instrumentos de Búsqueda.** 1. Todo Prestador de Servicios de Comunicación por Internet, que facilite contenidos a otros o incluya en los suyos directorios, enlaces o instrumentos de búsqueda de dichos contenidos, será responsable por la información ofrecida a los destinatarios de sus servicios, si tuviera conocimiento efectivo de que dicha información, datos y actividad son ilícitos, o de que lesionan los intereses, bienes o derechos de un tercero, o de que no haya actuado con la diligencia debida para suprimir o inutilizar el enlace o instrumento de búsqueda correspondiente, o de que el proveedor actuare bajo la dirección, influencia, autoridad, instrucción o control de aquél.

2.- Lo previsto en el último párrafo del Artículo anterior será de aplicación y en detrimento para cualquier destinatario.

## **CAPÍTULO II DEL CONTROL Y SUPERVISIÓN DE LA PRESTACIÓN DE SERVICIOS**

**Artículo 40. Control y Supervisión por la Administración General del Estado.** 1. El Ministerio de Telecomunicaciones y Nuevas Tecnologías, sus Órganos y Entes, y demás Instituciones Públicas que correspondan, así como la Autoridad de asignación, controlarán en sus respectivos ámbitos de competencias el cumplimiento por los prestadores y destinatarios de Servicios de las obligaciones, condiciones y demás exigencias derivadas de la prestación de servicios por vía electrónica y la utilización de los medios, sistemas y aplicación electrónicos en dicho proceso.

2.- La competencia a que se hace referencia el apartado anterior, corresponde también a los Órganos Jurisdiccionales que, en cada caso, lo sea por razón de la materia.

3.- En todo caso, cuando las conductas realizadas por los prestadores o destinatarios de servicios de la sociedad de la información estuvieran sujetas, en función de la materia, el ámbito competencial de tutela o de control o supervisión específicos, con independencia de que se utilicen medios electrónicos, informáticos o telemáticos, todos los órganos implicados ejercerán las funciones

que correspondan a cada uno de ellos en el marco de sus competencias, y podrán llevar a cabo acciones coordinadas y conjuntas de inspección y control.

4.- Los Funcionarios Públicos de los referidos Órganos, Entes e Instituciones, que ejerzan las funciones de supervisión, inspección y control, tendrán la consideración de Autoridad Pública en el desempeño de su cometido.

**Artículo 41. Obligación de Información a los Prestadores y Destinatarios de Servicios.** Los Prestadores y Destinatarios de Servicios por Vía Electrónica podrán dirigirse a cualquier Órgano o Ente competente en materia de la sociedad de la información y de la Administración General del Estado, por los medios electrónicos reconocidos, para:

- a) Corregir la información general sobre los derechos y obligaciones contractuales en el marco de la legislación aplicable a la contratación electrónica.
- b) Informarse sobre los procedimientos de Resolución Judicial y Extrajudicial de Conflictos.
- c) Obtener los datos de las Autoridades, Asociaciones y Organizaciones que puedan facilitarlos, y la información adicional o asistencia práctica.

**Artículo 42. Deber de Colaboración de los Prestadores y Destinatarios de Servicios.** 1. Los Prestadores y Destinatarios de Servicios tendrán la obligación de facilitar al Ministerio de Telecomunicaciones y Nuevas Tecnologías y a los demás Órganos, Entes e Instituciones referidos en el Artículo 40 de esta Ley, toda la información y colaboración para el ejercicio de sus competencias legales, permitiendo a sus Agentes y Personal Inspector o Controlador el acceso a sus instalaciones, la consulta de cualquier documentación y la manipulación de sus equipos, sistemas y aplicaciones electrónicos.

2.- Cuando, como consecuencia de una actuación supervisora, inspectora o de control, se tuviera conocimiento de hechos que pudieran constituir infracciones tipificadas en las demás Leyes, se dará cuenta de los mismos al Órgano Competente

y al Ministerio Fiscal para su verificación, incoación del correspondiente expediente y sanción.

## **TÍTULO V DE LA SOLUCIÓN JUDICIAL Y EXTRAJUDICIAL DE LITIGIOS**

### **CAPÍTULO I DE LAS DISPOSICIONES COMUNES**

**Artículo 43. Solución de Conflictos o Litigios.** Los Conflictos y Divergencias, que puedan suscitarse entre los Prestadores de Servicios, entre estos y los destinatarios o cualquier persona física o jurídica en relación a la realización y cumplimiento de las disposiciones de esta Ley, se resolverán extrajudicial o judicialmente.

**Artículo 44. Derechos de las partes en Litigio.** Las partes en conflicto podrán elegir cualquier medio de solución que establece la presente Ley para la solución de sus litigios y diferencias o controversias. Así mismo, podrán determinar cualquier otro medio, siempre que lo hayan pactado previamente y no contradiga a lo dispuesto en esta Ley.

### **CAPÍTULO II DE LA SOLUCIÓN JUDICIAL DE LITIGIOS**

**Artículo 45. Competencia Judicial en la Solución de Litigios. 1.** Contra las conductas contrarias y violadoras de los preceptos de la presente Ley y de las demás Leyes, además de ejercitar las acciones previstas en las Leyes ordinarias o específicas, se podrá promover la acción de cesación, que se tramitará conforme a la Ley de Enjuiciamiento Civil.

**2.-** La acción de cesación se formulará para obtener una Resolución o Sentencia que condene al demandado a cesar de su conducta ilícita y a prohibir su reiteración.

**Artículo 46. Legitimidad Activa y Pasiva. 1.** Están legitimadas activamente para ejercitar la acción de cesación todas las personas físicas o jurídicas, asociaciones, usuarios y otros titulares de un derecho e interés legítimo, que fuere lesionado o pudiera ser lesionado por la conducta infractora de las disposiciones de esta Ley o de las demás

Leyes Reguladores de las relaciones previstas por aquella.

**2.-** El Ministerio Fiscal también estará legitimado para ejercitar la acción de cesación en cumplimiento de su competencia legal, consistente en velar por la legalidad y estricta observancia de las Leyes.

**3.-** Están legitimadas pasivamente todas las personas físicas o jurídicas, cuya conducta contraviene a lo dispuesto en esta Ley y en las demás Leyes.

## **CAPÍTULO III DE LA SOLUCIÓN EXTRAJUDICIAL DE CONFLICTOS**

**Artículo 47. Marco Extrajudicial de Solución de Conflictos. 1.** Los Prestadores y Destinatarios de Servicios, así como todas las personas físicas o jurídicas usuarias o servidoras de comunicación por vía electrónica, podrán solucionar sus controversias o conflictos, sometiéndolos a la Autoridad de Asignación o a los Arbitrajes, mediaciones o amigables componendas previstos por la legislación vigente, cuya Resolución será obligatoria para las partes implicadas.

**2.-** En los procedimientos de Solución Extrajudicial de Conflictos podrá hacerse uso de los medios, soportes y documentos electrónicos como prueba, conforme a la presente Ley y a las demás Leyes vigentes en la materia, y será de aplicación lo dispuesto en el Artículo 46 anterior para los Órganos Arbitrales y responsables de Procedimientos Extrajudiciales en la Administración Pública.

## **TÍTULO VI DEL RÉGIMEN SANCIONADOR Y CAUTELAR**

### **CAPÍTULO I DE LAS INFRACCIONES, SUS SANCIONES Y RESPONSABILIDADES**

**Artículo 48. Infracciones.** Las Infracciones que pueden cometer los Prestadores y los Destinatarios o usuarios, se clasifican en Leves, Graves y Muy Graves.

### **1. Son Infracciones Leves:**

- a) Presentar de forma negligente e incompleta los datos solicitados por el Órgano Competente.
- b) La identificación errónea del nombre o denominación por el prestador de servicios.
- c) El envío negligente masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente sin su consentimiento ni solicitud.
- d) Poner a disposición del destinatario del servicio las condiciones generales a que deben sujetarse los contratos electrónicos de forma parcial o incompleta.
- e) Cualquier otra infracción que no sea grave.

### **2. Son Infracciones Graves:**

- a) La no identificación del nombre o denominación por el prestador de servicios.
- b) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a un mismo destinatario sin su consentimiento ni solicitud.
- c) El incumplimiento no habitual de la obligación de confirmar la recepción de la aceptación, cuando no se haya pactado su exclusión por las partes.
- d) No poner a disposición del destinatario del servicio las condiciones generales a que deben sujetarse los contratos electrónicos.
- e) La negativa o excusa sin resistencia a la actuación inspectora de los Órganos Competentes.
- f) La falta de colaboración o de establecimiento de procedimiento de rechazo de tratamiento de datos y de suministro de información solicitada por el Órgano Competente.
- g) La reiteración de dos Infracciones Leves, al menos dentro de un mismo año.

### **3. Son Infracciones Muy Graves:**

- a) El incumplimiento de la obligación de suspender la transmisión de datos y de comunicaciones.
- b) La no retirada de datos dañinos y nocivos para la juventud e infancia.
- c) El alojamiento, el acceso a la red o la prestación de cualquier servicio equivalente de intermediación, incumpliendo la orden del Órgano Competente.
- d) El incumplimiento de la obligación de conceder al destinatario los procedimientos de revocación del consentimiento.
- e) El incumplimiento habitual de la obligación de confirmar la recepción de la aceptación, cuando no se haya pactado su exclusión por las partes.
- f) La reiteración de dos infracciones graves, al menos, dentro de un mismo año.
- g) La resistencia a la actuación inspectora de los Órganos Competentes.

**Artículo 49. 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 hasta veinticinco millones (25.000.000) de F. Cfas.*
- 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 (1) año.*
  - b)** *Inhabilitación de las personas responsables de la infracción por un periodo de tiempo no superior a dos (2) años.*
  - c)** *Multa por un importe entre cincuenta millones uno (50.000.001) de F. Cfas., hasta cien millones (100.000.000) de F. Cfas.*
- 3.** Por las Infracciones Muy Graves se impondrán una o varias de las medidas siguientes:

- a) Suspensión de la actividad objeto de la infracción y, en su caso, otras medidas conexas, por un periodo de tiempo superior a un (1) año e inferior a cuatro (4) años.
- b) Inhabilitación de las personas responsables de la infracción por un periodo de tiempo superior a dos (2) años e inferior a cuatro (4) años.
- c) Multa por un importe entre cien millones uno (100.000.001) de F. Cfas., y quinientos millones (500.000.000) de F. Cfas.
- d) Incautación de equipos y demás material en las instalaciones del prestador.
- e) Clausura definitiva del local y de las instalaciones.

**II).** Las Sanciones Graves y Muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la Resolución firme en el Boletín Oficial del Estado o en la página o sitio de Internet del Prestador de Servicios sancionado.

Para la aplicación de la anterior medida, se tomará en consideración la repercusión social de la infracción cometida, el número de usuarios y de contratos afectados y la gravedad del ilícito.

**III).** Cuando las infracciones previstas en esta Ley fueren cometidas por un Prestador de Servicios establecido fuera del Territorio de la República de Guinea Ecuatorial, se ordenará a los Prestadores de Servicios de Intermediación establecidos en la República de Guinea Ecuatorial impedir el acceso a los servicios ofrecidos por aquél, por el periodo que estime suficiente el Órgano Competente.

**Artículo 50. Responsables de las Infracciones.** Los Prestadores y Destinatarios o usuarios de servicios de la sociedad de la información y la comunicación están sujetos al régimen sancionador establecido en la presente Ley, cuando haya cometido alguna de las infracciones previstas en la misma.

**Artículo 51. Graduación de las Sanciones.** Las Sanciones que se impongan a los infractores, se graduarán atendiendo a los criterios siguientes:

- a) La intencionalidad
- b) Reincidencia o reiteración

- c) Plazo de tiempo durante el cual se haya vendido cometiendo la infracción.
- d) Los beneficios obtenidos por la infracción
- e) La naturaleza y la cuantía del perjuicio causado.

**Artículo 52. Prescripciones.1.** Las Infracciones se prescribirán: a los seis meses las Leves; a los dos años las Graves; y a los tres años las Muy Graves.

**2.-** Las Sanciones se prescribirán: al año las impuestas por las Leves; a los dos años por las Graves; y a los tres años las impuestas por las Infracciones Muy Graves.

## **CAPÍTULO II DE LA APLICACIÓN DE MEDIDAS CAUTELARES**

**Artículo 53. Medidas Cautelares. 1.** Se podrán adoptar por las Infracciones Graves y Muy Graves, las medidas de carácter cautelar que se estimen pertinentes para asegurar la Resolución definitiva y evitar las posibles defraudaciones, desviaciones y ocultación de efectos y medios utilizados en la comisión de la infracción. A estas medidas se relacionan:

- a) La suspensión temporal de la actividad del Prestador de Servicios o, en su caso, el cierre provisional de su establecimiento.
- b) El precinto, incautación o depósito de registro, soportes y archivos informáticos y de documentos en general, así como de sus aparatos y equipos informáticos de todo tipo por un periodo no superior a seis (6) meses.
- c) La advertencia a los destinatarios, usuarios y al público en general sobre la incoación del correspondiente expediente sancionador por supuesta comisión de infracción de las disposiciones legales vigentes, y sobre las medidas cautelares adoptadas a efecto.
- d) Cualesquiera otras medidas que sean aplicables, conforme a la legislación vigente.

2.- En la adopción y cumplimiento de las referidas medidas cautelares se respetarán las garantías jurídicas establecidas en la presente Ley y en las demás Leyes sobre la Protección de los Derechos a la intimidad personal y familiar y de los datos personales, sobre la Libertad de Expresión y sobre la Libertad de Información, cuando estos pudieran ser afectados.

3.- Así mismo, en la adopción de las mismas se deberá respetar el principio de proporcionalidad entre ellas y el objetivo que se pretende alcanzar.

**Artículo 54. Competencia Exclusiva de la Autoridad Judicial.** Solo la Autoridad Judicial será competente para adoptar las medidas cautelares recogidas en el Artículo anterior. No obstante, en caso de urgencia y para la inmediata protección de los intereses de los afectados, el Órgano Administrativo Competente podrá adoptar dichas medidas, solicitando inmediatamente el acuerdo de la Autoridad Judicial para su confirmación o modificación dentro de los 15 días siguientes al de su adopción, transcurridos los cuales sin pronunciamiento alguno se quedarán sin efectos las adoptadas y se procederá a su levantamiento sin ulterior recurso.

### **CAPÍTULO III DEL PROCEDIMIENTO Y COMPETENCIAS SANCIONADORES**

**Artículo 55. Concurrencia de Procedimientos.**

1. Cuando haya identidad de sujetos, hechos y fundamentos de derecho y haya recaído Sentencia Penal, no será de aplicación la potestad sancionadora de esta Ley. No obstante, cuando se tramita procedimiento penal por los mismos hechos o por otros, cuya separación sea racionalmente imposible, se suspenderá el procedimiento previsto en esta Ley hasta que recaiga Sentencia Firme de la Autoridad Judicial, reanudándose después con la obligación de respetar los hechos declarados probados en la Sentencia Judicial.

2.- La imposición de las sanciones establecidas en la presente Ley no impedirá la tramitación, Resolución y Sanción por otros Órganos y Entes, cuando la conducta infractora esté tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3.- Cuando del procedimiento sancionador se tuviera conocimiento de hechos que pudiera constituir infracción tipificada en otras Leyes, se dará cuenta de los mismos al Ministerio Fiscal y a los Órganos o Entes competentes para su investigación y sanción.

**Artículo 56. Competencia Sancionadora. 1.** Corresponde al Ministerio de Telecomunicaciones y Nuevas Tecnologías, la potestad sancionadora establecida en esta Ley por las Infracciones Graves y Muy Graves, previa incoación del correspondiente expediente por la Dirección General de Nuevas Tecnologías, o en su caso, por la Autoridad de asignación; así como por los Órganos Jurisdiccionales en los casos determinados por esta disposición legal.

2.- Por las Infracciones Leves, la potestad sancionadora corresponderá a la Autoridad de Asignación, previa notificación al Ministerio de Telecomunicaciones y Nuevas Tecnologías.

3.- Las Resoluciones dictadas por el Ministerio 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 (30) días desde la fecha de notificación de la misma.

#### **DISPOSICIONES ADICIONALES:**

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

**Segunda.** Se establecerá una Tasa por asignación del recurso limitado de nombres de dominio y direcciones de Internet bajo el Código de País, gq, cuya regulación será por Ley.

#### **DISPOSICIONES TRANSITORIAS:**

**Primera.** Mientras no se implementen totalmente los Sistemas Electrónicos en los Servicios Públicos de la Administración General del Estado, se seguirá aplicando simultáneamente los procedimientos actuales y los electrónicos.

**Segunda.** Los Prestadores de Servicios que, a la entrada en vigor de esta Ley, estuvieran utilizando algún nombre de dominio o direcciones de Internet bajo el Código gq, deberán solicitar su anotación en el Registro Público habilitado en la Autoridad de Asignación en el plazo de seis (6) meses desde la entrada en vigor de la presente Ley.

**Tercera.** CNIAPGE elaborará el Plan Nacional de Nombres de Dominio de Internet, y ejercerá las funciones y competencias de la Autoridad de Asignación hasta tanto el Gobierno no tome otra decisión al respecto.

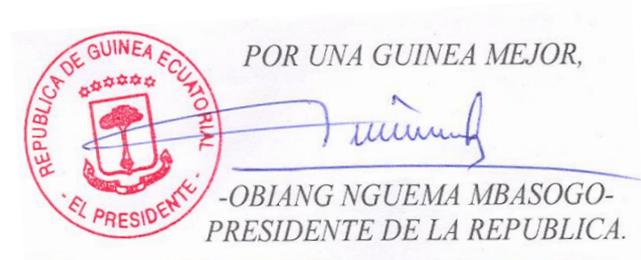
#### ***DISPOSICIÓN DEROGATORIA:***

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

#### ***DISPOSICIÓN FINAL:***

La presente Ley entrará en vigor a los veinte (20) días de su publicación en el Boletín Oficial del Estado y en los Medios Informativos Nacionales.

Dada en Malabo, a diez días del mes de Enero del año dos mil diecisiete.



**Ley Núm. 2/2.017, de fecha 10 de Enero, de Firma y Documentos Electrónicos.**

#### **EXPOSICIÓN DE MOTIVOS:**

Las Nuevas Tecnologías de Información y la Comunicación han creado y fomentado la utilización de las comunicaciones y transacciones electrónicas en la actividad de la Administración General del Estado y en su relación con los ciudadanos y demás sujetos del derecho, lo que requiere obligatoriamente el establecimiento de un marco jurídico que regule dicha utilización y garantice la seguridad jurídica y confianza en los participantes de las referidas comunicaciones y transacciones electrónicas por Internet. En este sentido, la Administración General del Estado, velando por ofrecerá todas las personas y a la población en general, unos servicios públicos seguros, accesibles, efectivos y eficientes, implementa y desarrolla la práctica de las tecnologías de la información y la comunicación en la actividad administrativa de sus Órganos, Instituciones y Entes Autónomos, propagando y difundiendo los efectos positivos de las mismas y generalizando la debida seguridad y confianza en el uso de las informaciones, comunicaciones y transacciones electrónicas.

Como consecuencia de garantizar y propiciar la referida seguridad y confianza, surge la necesidad de establecer y crear los elementos y medios protectores para dichos fines. Este es el caso de la Firma Electrónica y demás Documentos Electrónicos.

La Firma Electrónica constituye un instrumento o medio protector capaz de permitir la comprobación de la procedencia, veracidad y de la integridad de los datos, informaciones y comunicaciones utilizados a través de Internet y de redes de telecomunicaciones, ofreciendo los fundamentos y bases para evitar y controlar cualquier tipo de falsedad o defraudación, basándose en fechas, horas, elementos, códigos y medios electrónicos, que están en poder de cada uno de los usuarios y permiten distinguir e individualizar la identidad personal de cada uno y reconocerle como el firmante. Esta actuación es realizada por los Prestadores de Servicios de Certificación, que expiden

los Certificados Electrónicos relacionados con la Firma Electrónica, denominados también Documentos Electrónicos.

La presente Ley define y determina los diferentes Certificados Electrónicos que se expidan o se pueden expedir, destacando los Certificados Avanzados y reconocidos, que cumplen con los requisitos legales y se ajustan a los procedimientos de comprobación de la identidad del firmante y la fiabilidad y garantías de la actividad de certificación electrónica, formando una pieza fundamental la Firma Electrónica reconocida, generada mediante un dispositivo seguro de creación de firma. Cabe señalar que la Firma Electrónica reconocida tiene la equivalencia legal y funcional con la Firma Manuscrita respecto de los datos consignados en la información y comunicación electrónica. Por otra parte, el dispositivo de creación de Firma Electrónica debe ser avalado y garantizado por una certificación técnica de dicho dispositivo expedido por el Órgano Competente.

Otro aspecto importante que regula esta Ley es el Documento de Identidad Personal Electrónico, que constituye un Certificado Electrónico reconocido destinado a generalizar el uso de medios e instrumentos seguros de comunicación y autenticidad, precisando que el D.I.P. Electrónico acredita la identidad de su titular en cualquier procedimiento administrativo y permite la Firma Electrónica de Documentos Administrativos.

La presente Ley se estructura en una Exposición de Motivos, treinta y nueve (39) Artículos, repartidos en cuatro (4) Títulos y nueve (9) Capítulos, una Disposición Adicional, dos (2) Disposiciones Transitorias, una Disposición Derogatoria y una Final.

En uso de las prerrogativas que Me otorga el Artículo 40 de la Ley Fundamental; a propuesta del Gobierno y debidamente aprobada por el Parlamento Nacional en su Segundo Periodo Ordinario de Sesiones correspondiente al año 2.016, Sanciono y Promulgo la presente:

### ***Ley de Firma y Documentos Electrónicos***

## **TÍTULO I DE LAS DISPOSICIONES GENERALES**

**Artículo 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.

**Artículo 2. Ámbito de Aplicación. 1.** La presente Ley se aplicará a los Prestadores de Servicios de Certificación establecidos en la República 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 República 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 el lugar en que está 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 esté 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 sí sola, el establecimiento del Prestador en la República de Guinea Ecuatorial.

**Artículo 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, como Códigos o Claves Criptográficas 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 como Códigos o Claves Criptográficas que se utilizan para verificar la Firma Electrónica.
- h) **Certificado Electrónico:** Todo documento firmado electrónicamente por un Prestador de Servicios de Certificación, que vincula unos datos de verificación de firma con el firmante y confirma su identidad.
- i) **Certificado Electrónico Reconocido:** Aquél 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 medio 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:** Documento 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 Electrónicos o presta otros servicios en relación con la Firma Electrónica.
- m) **Documento 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 caso, lo siguiente:

- 1) Estar firmados electrónicamente por Funcionarios que tengan legalmente atribuida la facultad de dar Fe Pública, Judicial, Notarial o Administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la Ley en cada caso.
- 2) Ser expedidos y firmados electrónicamente por Funcionarios o Empleados Pú-

blicos 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.

**Artículo 4. Valor Jurídico del Soporte Electrónico con Datos Firmados.** 1. El Soporte en que se halle los datos firmados electrónicamente, será admisible como prueba documental en juicio. Si se impugnara la autenticidad de la Firma Electrónica Reconocida con la que se hayan firmado los datos incorporados al Documento 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 y, si hubiere actuado de forma temeraria, se le impondrá una multa dineraria.

3.- Si se impugnara la autenticidad de la Firma Electrónica Avanzada, con la que se hayan firmado los datos incorporados al Documento Electrónico, se estará a lo dispuesto en el párrafo anterior en consonancia con las disposiciones de la Ley de Enjuiciamiento Civil.

4.- Cuando la Firma Electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellos.

**Artículo 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 como 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.

**Artículo 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, transparencia y no discriminación.

## TÍTULO II DE FIRMA Y CERTIFICADOS ELECTRÓNICOS

### CAPÍTULO I DEL CONTENIDO DE LA FIRMA ELECTRÓNICA Y EL FIRMANTE

**Artículo 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 en la presente Ley son: la Firma Electrónica Avanzada, la Firma Electrónica Reconocida y la Firma Digital.

**Artículo 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 II DEL CERTIFICADO ELECTRÓNICO Y SUS EFECTOS**

**Artículo 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 como detectar los cambios habidos en los mismos y determinar el origen o la Entidad que haya generado dicho dato o mensajes, según el tipo de Certificado y de la Firma Electrónica.

2.- Toda persona física o jurídica podrá solicitar del Prestador de Servicios 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.

**Artículo 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 firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

5.- Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubieren celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de la firma, 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.

**Artículo 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 éste, 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 firma del firmante o del Prestador de Servicios de Certificación o utilización indebida de dichos datos por un tercero.

- d) Resolución Judicial o Administrativa 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 de la actividad del Prestador de Servicios de Certificación, salvo que, previo consentimiento expreso del firmante, la gestión de los Certificados Electrónicos expedidos por aquél 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 lícita puesta en la declaración de prácticas de certificación.

**Artículo 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 (4) 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.

**Artículo 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 éste, 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 a cerca 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 lícita 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.

**Artículo 14. Actuaciones y Efectos relativos a la Extinción y Suspensión de la Vigencia de Certificados Electrónicos.**

1. El Prestador de Servicio 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 o 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 III DEL CERTIFICADO ELECTRÓNICO RECONOCIDO Y SU EXPEDICIÓN**

**Artículo 15. *El Certificado Electrónico Reconocido y su Contenido.*** Todo Certificado Electrónico Reconocido, que fuere expedido por un Prestador de Servicios de Certificación, deberá integrar los siguientes datos:

- a) La indicación de que se expiden como tales.
- b) El Código indicativo único del Certificado.
- c) La identificación del Prestador de Servicios de Certificación que expide el Certificado y de su domicilio.
- d) La Firma Electrónica Avanzada del Prestador de Servicios de Certificación que expide el Certificado.
- e) La identificación del firmante, en el caso 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, NIF.
- f) Los datos de verificación de Firma Electrónica que correspondan a los datos 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 límites de uso del Certificado Electrónico, 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 documento.

- k) Cualesquiera otros datos, circunstancias y rasgos peculiares del firmante significativos para fines del certificado, si lo solicita.

**Artículo 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.

**Artículo 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 sido 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 exige.

4.- La comprobación o la identificación, a que se hace referencia en el apartado anterior, también podrá realizarse 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, éstas deberán comprobarse mediante los Documentos Oficiales que las acrediten.

6.- No serán exigibles los datos, la identificación y las circunstancias a que se refieren los apartados 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 otro con idéntico formato y le conste al Prestador de Servicios de Certificación en un periodo de tres meses desde la vigencia de aquél.

7.- Las comprobaciones e identificaciones señaladas en los párrafos anteriores, podrán realizarse por los Prestadores de Servicios de Certificación por sí o por medio de otras personas físicas o jurídicas, privadas o públicas, en cuyo caso, siempre será el responsable.

**Artículo 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 sido 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 IV DEL RÉGIMEN JURÍDICO DEL DOCUMENTO DE IDENTIDAD PERSONAL**

**Artículo 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 documentos firmados con los dispositivos de Firma Electrónica incluidos en dicho documento.

**Artículo 20. Requisitos para la Expedición del Documento de Identidad Personal Electrónico. 1.** Los Órganos Públicos Competentes para la expedición del Documento de 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, excepto 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 Documento de Identidad Personal Electrónico será desarrollado mediante Decreto.

### **TÍTULO III DEL SISTEMA DE FIRMA ELECTRÓNICA Y PRESTACIÓN DEL SERVICIO DE CERTIFICACIÓN**

#### **CAPÍTULO I DE LOS DISPOSITIVOS DE FIRMA ELECTRÓNICA Y DE SU VERIFICACIÓN**

**Artículo 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 de 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 documento que deba firmarse, ni impide que éste muestre al firmante antes del proceso de firma.

**Artículo 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 esta verificación se presente correctamente.
- c) Que la persona que verifique 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 el resultado de la verificación.
- e) Que pueda detectarse cualquier cambio relativo a la seguridad.

**Artículo 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 documento por el que se comprueba que el 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 con los Dispositivos Seguros de Creación de Firma Electrónica serán modificados o, en su caso, 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 comunicaciones sociales.

#### **CAPÍTULO II DE LA PRESTACIÓN DE SERVICIOS DE CERTIFICACION**

**Artículo 24. Certificación del Prestador de Servicios de Certificación.** 1. La Certificación del 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.

**Artículo 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 el Prestador de Servicios 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 éstos:
  - 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.

**Artículo 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 éstos, sujetándose a lo 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 los firmantes y de sus demás datos personales por

requerimiento de la Autoridad Judicial en el ejercicio de sus funciones legales.

**Artículo 27. Declaración de Prácticas de Certificación. 1.** Todos los Prestadores de Servicios formularán una declaración de prácticas de certificación en la que detallarán 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 caso, 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 Documento de Seguridad, conteniendo todos los requisitos legalmente exigidos para dicho documento, y estará disponible al público de manera accesible, gratuita y por vía electrónica.

**Artículo 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 uso 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 e impedir que personas no autorizadas alteren los datos, restrinjan su capacidad 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 el 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 (10) años contados desde la fecha de su expedición, de manera que se pueda verificar las firmas efectuadas en el mismo.

**Artículo 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, otro Prestador de Servicios de Certificación que los asuma o, en caso contrario, extinguir su vigencia.

**2.-** La comunicación del cese se llevará a cabo con una antelación mínima de tres (3) 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 de Telecomunicaciones y Nuevas Tecnologías, y a la Autoridad Pública autorizada y cualificada, con una antelación de tres (3) 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 III DE LA RESPONSABILIDAD DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN**

**Artículo 30. Responsabilidad de los Prestadores de Servicios de Certificación.** **1.** Los Prestadores de Servicios 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 deleguen la 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 uso de dicho certificado.

**Artículo 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 circunstancias 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 caso 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 Electrónico sobre sus posibles usos y al importe individualizado de

las transacciones que puedan realizarse con él, 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.

**Artículo 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 Servicios de Certificación probar y justificar que no actuó de forma negligente.

## TÍTULO IV DEL RÉGIMEN SANCIONADOR Y ÓRGANOS COMPETENTES

### CAPÍTULO I DE LAS INFRACCIONES Y SUS SANCIONES

**Artículo 33. Infracciones.** Las Infracciones tipificadas por la presente Ley se clasifican en 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 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 Pública autorizada y cualificada en su función inspectora.
- d) El incumplimiento negligente de las obligaciones en relación a la Protección de Datos Personales recogidos de forma general en esta Ley y particularmente en el

Artículo 26, cuando no sean constituyas 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 Pública 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 el 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 afectada.
- 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 el Artículo 26.
- d) La comisión de dos o más Infracciones Graves en un periodo de un año.

**Artículo 34. Sanciones. I).** Por la comisión de 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 hasta cinco millones (5.000.000) de F. Cfas.
- d) Rectificación, en todo caso, de la situación creada como 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 (1) año.

- b) Inhabilitación de las personas responsables de la infracción por un periodo de tiempo no superior a dos (2) 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 cinco millones uno (5.000.001) de F. Cfas y veinticinco millones (25.000.000) de F. Cfas.

**3. *Por las Infracciones Muy Graves:*** Se impondrán una o varias de las medidas siguientes:

- a) Suspensión de la actividad objeto de la infracción y, en su caso, otras conexas, por un periodo de tiempo superior a un (1) año e inferior a cuatro (4) años.
- b) Inhabilitación de las personas responsables de la infracción por un periodo de tiempo superior a dos (2) años e inferior a cuatro (4) 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 veinticinco millones uno (25.000.001) de F. Cfas y cien millones (100.000.000) de F. Cfas.
- 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 (3) años podrá dar lugar, en función de los criterios de graduación del Artículo siguiente, a la sanción de prohibición de actuación en la República de Guinea Ecuatorial durante un tiempo máximo de dos (2) 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 los Datos Personales recogidas de forma general en esta Ley y particularmente en el Artículo 26, así como las contempladas en la Ley Orgánica sobre 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.

**Artículo 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 perjuicios causados.
- d) El tiempo durante el que se haya venido cometiendo la infracción.
- e) El beneficio que hay obtenido el infractor por dicha infracción.
- f) El volumen de la facturación a que afecte la infracción cometida.

**Artículo 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 Registros, Soportes y Archivos Informáticos

y de Documentos en general, así como de aparatos y equipos informáticos de todo tipo por un periodo de tiempo no superior a seis (6) 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 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 (10) 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 encuentren.

**4.-** Dichas medidas quedarán sin efecto, si no se inicia el Procedimiento Sancionador dentro del plazo señalado en el párrafo anterior o no haya pronunciamiento expreso sobre las medidas adoptadas.

**Artículo 37. Procedimiento Sancionador. 1.** Corresponde al Ministro de Telecomunicaciones y Nuevas Tecnologías, la potestad 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 caso por la Autoridad Pública autorizada y cualificada.

2.- Por las Infracciones Leves, la potestad 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 el Recurso de Alzada ante el Consejo de Ministros dentro del término de treinta (30) días desde la fecha de la notificación de la misma.

## **CAPÍTULO II DE LOS ÓRGANOS COMPETENTES**

**Artículo 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 la expedición de Certificación de Dispositivos seguros de creación de Firma, así como 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.

**Artículo 39. Deber de Información y Colaboración. 1.** 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 de la Administración Pública de Guinea Ecuatorial, en anagrama CNIAPGE, de modo transitorio y por un periodo improrrogable de un (1) año, ejercer las funciones certificadoras de dicha Entidad.

***DISPOSICIÓN DEROGATORIA:***

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

***DISPOSICIÓN FINAL:***

La presente Ley entrará en vigor a los noventa (90) días de su publicación en el Boletín Oficial del Estado y en los Medios Informativos Nacionales.

Dada en Malabo, a diez días del mes de Enero del año dos mil diecisiete.

