



REPUBLICA DE GUINEA ECUATORIAL  
P R E S I D E N C I A

=====

LEY NÚM. 7/2024, DE FECHA 23 DE  
DICIEMBRE, POR LA QUE SE REGULA EL  
USO DE LAS REDES SOCIALES, DELITOS  
INFORMÁTICOS Y LA  
CIBERDELINCUENCIA EN LA  
REPÚBLICA DE GUINEA ECUATORIAL.



REPUBLICA DE GUINEA ECUATORIAL

PRESIDENCIA

**Ley Núm. 7 /2024, de fecha 23 de diciembre, por la que se Regula el Uso de las Redes Sociales, Delitos Informáticos y la Ciberdelincuencia en la República de Guinea Ecuatorial.....**

### EXPOSICIÓN DE MOTIVOS

La informática y el ciberespacio constituyen una oportunidad para el desarrollo de los países y personas físicas y jurídicas. A tal efecto, el Gobierno de la República de Guinea Ecuatorial ha hecho de estos instrumentos un vector de desarrollo con la inversión en la fibra óptica, que permite al país beneficiarse de las ventajas del internet, y la creación de instituciones de gestión y comercialización de las nuevas tecnologías de la información y comunicación.

Sin embargo, el mal uso de estas plataformas de progreso ha llevado a la creación de espacios que propician la comisión de delitos y de atentados contra la intimidad, el honor, la reputación y la imagen de las personas, tanto físicas como jurídicas.

Esta amenaza, que representa el uso inadecuado de la informática y el ciberespacio, no puede ser combatida solo por la legislación penal vigente en la Republica de Guinea Ecuatorial por imperativo del principio de legalidad que establece el artículo 13.1 s) de la Ley Fundamental, el cual dispone que “Todo ciudadano goza del derecho a no ser castigado por un acto u omisión que en el momento de cometerse no estuviese tipificado ni castigado como infracción penal; ni se le puede aplicar una pena no prevista en la ley.”

Con la presente Ley, inspirada en la Convención de Budapest de 2001 Y la Convención de Malabo de 2014 de la Unión Africana, el Gobierno dota al país de un instrumento legal que regula la utilización de las redes sociales y reprime los delitos cometidos con soportes informáticos y en las redes sociales.

En su virtud, a propuesta del Gobierno y debidamente aprobada por la Cámara de los Diputados y el Senado en su Segundo Período Ordinario de Sesiones, celebrado en la Ciudad de Malabo, del 30 de julio al 30 de noviembre del año 2024, vengo en sancionar y promulgar la presente,



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

**LEY POR LA QUE SE REGULA EL USO DE LAS REDES SOCIALES,  
DELITOS INFORMATICOS Y CIBERDELINCUENCIA EN LA REPUBLICA  
DE GUINEA ECUATORIAL.**

**DISPONGO**

**TÍTULO I  
DISPOSICIONES GENERALES**

**CAPÍTULO I  
OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES**

**Artículo 1.- Objeto**

La presente Ley tiene por objeto regular el uso responsable de las redes sociales por los usuarios y la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación (TIC), en perjuicio de personas físicas o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.

**Artículo 2.- Ámbito de aplicación**

La presente Ley es de orden público y se aplicará a quienes utilicen de manera irresponsable las redes sociales y cometan los delitos informáticos y los ciberdelitos previstos en esta Ley, dentro o fuera del territorio nacional.

**Artículo 3.- Definiciones**

A los efectos de la presente Ley se entenderá por:

- 1. Acceso a sistemas de redes informáticos;** la entrada a dichos sistemas, incluyendo los accesos remotos.
- 2. Acceso a la información contenida en un dispositivo que permita el**



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

**almacenamiento de datos;** la lectura, copia, extracción, modificación o eliminación de la información contenida en dicho dispositivo.

**3. Ciberdefensa;** la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

**4. Cyberbullying o ciberacoso;** el uso de redes sociales para acosar a una persona o grupo de personas mediante ataques personales, divulgación de información confidencial o falsa.

**5. Cibercriminos;** *las acciones* u omisiones, típicas, antijurídicas, continuas o aisladas de carácter penal, cometidas en contra de personas físicas y/o jurídicas, utilizando como método, como medio o como fin, la *red* que podrá ser abierta, cerrada o de acceso restringido, y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima.

**6. Ciberseguridad;** la capacidad del Estado para reducir el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

**7. Copia de datos;** la reproducción total o parcial de la información digital.

**8. Contenido en redes sociales;** las imágenes, citas inspiradoras, ideas o conceptos, grabaciones creadas para orientar, entretener, informar, educar y ayudar a las personas dentro del conjunto elegido como público objetivo.

**9. Datos informáticos;** cualquier representación de hechos, información o conceptos en un formato digital o analógico, que puedan ser generados, almacenados, procesados o transmitidos a través de las Tecnologías de la Información y la Comunicación.

**10. Datos relativos al tráfico;** Todos los datos relativos a una comunicación realizada a través de cualquier medio tecnológico, generados por este último, que indiquen el origen, el destino, la ruta, la hora, la fecha y el tipo de servicio o protocolo utilizado, tamaño y la duración de la comunicación.

**11. Datos personales;** la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

**12. Datos personales sensibles;** toda información privada que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra que pueda ser motivo de discriminación.

**13. Delito informático;** las acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas físicas y/o jurídicas, utilizando sistemas informáticos, con el fin de lesionar bienes jurídicos, personales o patrimoniales.

En los delitos informáticos la presencia o utilización de la red es secundaria.

**14. Dispositivo;** Cualquier mecanismo, instrumento, aparato o medio que se utiliza para ejecutar cualquier función de la Tecnología de la Información y la Comunicación.

**15. Dispositivos de almacenamiento de datos informáticos;** Cualquier medio a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo.

**16. Entrega de datos y archivos informáticos;** la transferencia de informaciones, documentos o datos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.

**17. Empresa Tecnológica;** son aquellas industrias que tienen como actividad fabricar, genera y utilizar productos tecnológicos mas avanzados con el fin de promover todo lo relacionado con las redes sociales, servicios telemáticos y programas de todo tipo que garantiza las aplicaciones inherentes a la informática y servicios análogos.

**18. Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) o Equipo de Respuesta de Emergencias Informáticas (CERT);** equipo que monitoriza y controla las redes para detectar los posibles incidentes o emergencias, difundir alertas sobre cualquiera de ellos y dar respuesta a los mismos para solucionarlo o mitigar sus efectos.



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

- 19. Identidad informática;** Información, datos o cualquier otra característica que individualice, identifique o distinga una persona de otra o a un usuario de otro usuario, dentro de un sistema informático.
- 20. Incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos;** la ocupación física y su aseguramiento por las autoridades competentes.
- 21. Infraestructura crítica;** La instalación, redes, sistemas, dispositivos y equipos físicos y lógicos de las Tecnologías de Información y Comunicación y demás estructuras y elementos, cuya perturbación, amenaza, paralización o destrucción puede impactar grave y negativamente sobre el funcionamiento normal de los servicios indispensables y esenciales de la sociedad.
- 22. Interceptar; acción** de apropiarse o interrumpir datos informáticos contenidos o transmitidos por medio de las Tecnologías de la Información y la Comunicación antes de llegar a su destino.
- 23. Interferir;** Obstaculizar, perturbar u obstruir por medio de las Tecnologías de la Información y la Comunicación los sistemas informáticos, públicos o privados.
- 24. Intervención de comunicaciones a través de las Tecnologías de la Información y la Comunicación;** la captación, escucha o grabación en tiempo real del contenido de dichas comunicaciones sin interrupción de las mismas, así como de los datos de tráfico.
- 25. Página Web;** al Conjunto de información que se encuentra en una dirección determinada de internet.
- 26. Pornografía infantil;** cualquier transmisión de la imagen o voz de un niño, niña o adolescente, realizando actividades sexuales o eróticas, implícitas o explícitas, reales o simuladas, así como la exposición de sus partes genitales, con fines sexuales, por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

**27. Persona con discapacidad necesitada de especial protección;** aquella persona con discapacidad que tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus limitaciones intelectuales o mentales de carácter transitoria o permanente.

**28. Proveedor de servicios;** la persona natural o jurídica, pública o privada, que suministre a los usuarios servicios de comunicación, seguridad informática, procesamiento o almacenamiento de datos, a través de las Tecnologías de la Información y la Comunicación.

**29. Programa informático;** la herramienta o instrumento elaborado en lenguaje informático que ejecuta una secuencia de procesos en un sistema informático.

**30. Redes sociales;** formas de interacción social definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Consisten en un sistema abierto y en construcción permanente que involucran a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

**31. Redes Sociales de Internet – RSI;** el resultado de la utilización de los servicios de internet, para reproducir las relaciones sociales y establecer otras nuevas. Esta plataforma digital solo cobra vida a través del uso de las redes sociales de internet, que emerge como resultado de un híbrido entre un elemento social (redes sociales) y otro tecnológico (servicios de internet).

**32. Requerimiento de preservación inmediata de datos que se hallan en poder de terceros;** la imposición a *personas naturales* o jurídicas del deber de conservación íntegra de la información digital que obre en su poder o sobre la que tenga facultades de disposición.

**33. Sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos;** el bloqueo o la imposibilidad de su utilización conservando la integridad de su contenido.



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

**34. Servicios de Red Social – SRS;** plataformas digitales que permiten reproducir las estructuras de relaciones en un espacio digital que sigue un diseño determinado.

**35. Sistema informático;** Todo dispositivo aislado, conectado o relacionado a otros dispositivos mediante enlaces de comunicación o la tecnología que en futuro la reemplace, y cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa informático.

**36. Tarjeta inteligente;** todo dispositivo electrónico que permite la ejecución de cierta lógica programada para el almacenamiento de información y/o datos, que se utiliza como instrumento de identificación o de acceso a un sistema, para realizar gestiones electrónicas al titular autorizado.

**37. Tecnologías de la Información y la Comunicación;** el conjunto de medios de comunicación y las aplicaciones de información que permiten la captura, producción, reproducción, transmisión, almacenamiento, procesamiento, tratamiento, y presentación de información, en forma de imágenes, voz, textos, códigos o datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros, por medio de protocolos de comunicación, transmisión y recepción.

**38. Usuario;** individuo que utiliza una red social de internet, sistema operativo o servicio para interactuar con los demás.

**39. Usuario víctima;** la persona que sufre un daño o perjuicio provocado por información o contenido publicado en las redes sociales de internet.

**40. Usuario victimario;** aquella persona que le infringe daño o perjuicio a otra por publicar sobre esta, información o contenido en las redes sociales de internet.

**41. Ciberterrorismo;** uso de las Tecnologías de Información y la Comunicación (TIC), para llevar a cabo actos terroristas o para facilitarlos. esto pueden incluir ataques a sistemas informáticos, redes de computadoras o infraestructuras críticas con el objetivo de causar daño, interrupción o pánico en la sociedad.

**42. Ciberespacio;** Entorno virtual creado por la interconexión global de redes de computadoras. Es un espacio digital de la información fluye y se comparte a



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

través de internet, incluyendo sitios de web, redes sociales, correos electrónicos entre otros medios digitales.

## CAPÍTULO II

### PRINCIPIOS RECTORES, PROHIBICIONES, OBLIGACIONES Y DEBERES

#### Artículo 4.- Los principios rectores.

En el desarrollo, interpretación y aplicación de la presente Ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) **Respeto:** Cuando se participa en las redes sociales se debe tener presente que se trata de un terreno propio de la ciudadanía, donde cada usuario tiene su opinión, que no siempre debe ser compartida, pero sí respetada.

b) **Transparencia:** Es la norma básica de los medios sociales y la capacidad que tiene un ser humano para que los otros entiendan claramente sus motivaciones, intenciones y objetivos, y que se enfoca en llevar a cabo prácticas y métodos a la disposición pública, sin tener nada que ocultar.

c) **Corresponsabilidad:** Comunicar a través de las cuentas en redes sociales es una gran responsabilidad, por ello se debe tener claro bajo qué línea de mensaje y bajo qué orientación los usuarios deben comunicarse.

d) **Veracidad o calidad:** La información o contenidos que se publiquen en las redes sociales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

e) **Inmediatez de la información o comunicación:** La comunicación circula con rapidez, permitiendo una interacción más rápida.

f) **Libertad de opinión y de expresión:** Todas las personas tienen derecho a la libertad de opinión y de expresión; esto incluye el derecho a mantener una opinión sin interferencias y a buscar, recibir y difundir información e ideas, a través de cualquier medio de difusión.



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

**Artículo 5.- Prohibiciones.**

Para garantizar el buen uso de las redes sociales, se prohíbe a los usuarios:

- a) Ser menor de 14 años para acceder y pertenecer a las redes sociales sin el consentimiento de los padres, tutores o representantes legales.
- b) Pedir o publicar datos de un menor de 14 años, sin el consentimiento expreso de sus padres, tutores o representantes legales.
- c) Publicar cualquier tipo de dato, información, archivo, fotos, videos de otras personas de cualquier edad, sin el consentimiento expreso o escrito de las mismas.
- d) Descargar libre y gratuitamente contenidos que tengan derechos de autor.
- e) Usurpar la identidad de otro, crear perfiles que no representen a una persona real para incurrir en la comisión de conductas punibles reprochables penalmente.
- f) Publicar comentarios o expresiones insultantes o amenazantes acerca de otras personas, grupos o comunidades que agravien, afecten u ofendan su buen nombre, honra, intimidad, integridad personal, libertad de expresión o ejercer acoso por internet.
- g) Exponer su intimidad o revelar información personal y sensible dentro del perfil, como información económica, financiera, salud, dirección de residencia, teléfono o información sentimental.
- h) Acceder a información personal y reservada sin orden judicial.
- i) Acceder a contenidos inadecuados o ilegales.
- j) Usar lenguaje violento que incite al odio o discriminación en alguna de sus formas.
- k) Difundir noticias falsas para atacar a terceros.

**Artículo 6.- Obligaciones.**

Los usuarios de las redes sociales, tendrán las siguientes obligaciones:

- a) Observar las recomendaciones más comunes de seguridad.
- b) Ser discretos con lo que publican.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

c) Actuar con diligencia en las declaraciones, publicaciones y evitar *el odio* o atribuir hechos falsos a otros usuarios o a terceros.

d) No compartir publicaciones que puedan afectar a terceros sin comprobar previamente su veracidad.

**Deberes y Obligaciones de retractación**

**Artículo 7.- Deberes.**

Sin perjuicio de la obligación de denuncia consagrada por las leyes vigentes en la materia, los proveedores, administradores y usuarios de redes sociales en internet deberán:

a) Denunciar ante las autoridades competentes un presunto acto criminal del cual tengan conocimiento a través de las redes sociales en internet.

b) Abstenerse de usar las redes sociales en internet para divulgación de contenidos ilícitos.

c) Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de contenidos ilícitos, ofensivos, abusivos o indeseables.

d) Permitir solamente el acceso al perfil a personas bien identificadas.

e) Emplear términos adecuados en la publicación de información o contenidos para evitar errores inequívocos en su interpretación.

**Artículo 8.- Obligación de retractación.**

El usuario de redes sociales en internet o plataformas digitales que publique información, o use expresiones y mensajes que afecten derechos fundamentales de otras personas usuarias o no de las mismas, estará obligado mediante orden judicial a la retractación por el mismo medio mediante el cual efectuó la publicación. Salvo que, de forma voluntaria, quiera retractarse, en ese caso, podrá hacerlo en el mismo medio o en otro de mayor difusión.



REPUBLICA DE GUINEA ECUATORIAL

PRESIDENCIA

**TÍTULO II**  
**DE LA PROTECCIÓN, MEDIOS DE VIGILANCIA Y SANCIÓN DE LA VIOLACIÓN DE LOS DERECHOS FUNDAMENTALES DE LOS USUARIOS**  
**CAPÍTULO I**

**DE LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES**

**Artículo 9.- La obligación de respeto de los derechos fundamentales.**

Los usuarios de plataformas digitales y de las redes sociales de internet tienen la obligación de respetar los derechos fundamentales de las personas, en especial los derechos fundamentales de los niños, niñas y los adolescentes, consagrados en los artículos 13 y 14 de la Ley Fundamental.

Los administradores de plataformas digitales y redes sociales de internet, dentro de las cláusulas del contrato de adhesión o códigos de conducta incorporarán un apartado relacionado con el respeto de los derechos fundamentales de terceros.

**Artículo 10.- La obligación de respeto de los derechos fundamentales de las niñas, niños y adolescentes.**

En las redes sociales, en internet, se *asegura* el respeto a los derechos fundamentales de los niños, niñas y adolescentes.

Es tarea del Gobierno, a través de sus poderes e instituciones, departamentos competentes, agentes sociales, entidades educativas, la familia, así como las empresas tecnológicas y las proveedoras de servicios de Internet, capacitar, concienciar y proteger a los niños, niñas y adolescentes sobre los posibles riesgos a los que se enfrentan por el uso de las redes sociales en internet al realizar publicaciones de información, contenidos y proveer conocimiento acerca del uso responsable y seguro de las mismas.



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

**Artículo 11.- Obligatoriedad de las *instituciones* públicas y privadas de la formación.**

Es de obligado cumplimiento la formación en todas las instituciones educativas del país en la enseñanza primaria, secundaria, centros profesionales, universitarios, así como las empresas tecnológicas y las proveedoras de servicios de Internet, que incluye:

- a) La adopción en los planes de estudios del buen uso de las redes sociales, articulada en las áreas del conocimiento de Tecnología, Informática, Educación ética y en Valores Humanos impartidas en las aulas de clase.
- b) El fomento del proceso de aprendizaje y competencias relacionadas con formación en la enseñanza, preparando a los estudiantes para participar en el nuevo mundo en las plataformas digitales y Redes Sociales.
- c) La generación de un efecto de refuerzo positivo en la población crítica, aumentando conciencia y cuestionamiento crítico de lo que implica estar conectado en este espacio social.

**Artículo 12.- El contenido de la enseñanza.**

La enseñanza que se implemente en cada institución estará orientada a generar aprendizaje en los siguientes componentes:

- a) **Riesgo de compartir información:** A través de las redes los niños se exponen a sufrir acoso de otros compañeros (cyberbulling), es por ello que, es importante que conozcan el efecto viral que tiene Internet. La rapidez con que un comentario o una opinión es transmitida por las redes sociales y lo pronto que llega sobre todo al círculo de personas más cercanas y que más daño podrían causar.
- b) **Buena educación en la red:** Enseñarles a los niños a actuar con educación como en el mundo real; enseñarles la importancia de ser amables y bien educados también en internet. En Internet hay que comportarse con respeto y educación. No hacer a otros lo que no quieras que te hagan a ti.
- c) **Saber con quién se conecta:** Los niños, *niñas* y *adolescentes* tratan a menudo a un amigo de una red social como si fuera un amigo de toda la vida y le pueden enviar información que no debería llegarle. Deben saber que hay asuntos que no deben compartirse y que no todo lo que hagan o vayan a hacer



REPUBLICA DE GUINEA ECUATORIAL

---

PRESIDENCIA

---

tiene que ser conocido por todo el mundo. Es por ello, que hay que saber que no todos los contactos de la red tienen que ser buenos amigos y no pueden dirigirse a ellos con la misma confianza.

d) **Precaución al acceder a ciertas páginas de internet:** Educar a los niños sobre los diferentes tipos de páginas a las que pueden acceder en internet catalogándolas de acuerdo a la importancia según la edad, en: Académicas, educativas, científicas, culturales, deportivas, relaciones sociales, sexuales, pornografía, entre otras.

e) **Retos virtuales:** Metas, desafíos o pruebas entre usuarios de Redes Sociales.

Hoy día son frecuentes las noticias de suicidios y muertes publicadas en las redes sociales de adolescentes y jóvenes como consecuencia de los retos virtuales en los que quedan atrapados y no encuentran una mejor forma de salir que quitándose la vida, situación que nos hacen pensar lo dañada que está siendo la sociedad por el mal uso de la tecnología.

f) **Relaciones sentimentales mediante el uso de las redes sociales:** Casi todo el que tenga acceso a una conexión de Internet, utiliza alguna red social (o varias), con diferentes fines como acercar a personas que están lejos, promocionar su producto o marca, encontrar pareja, enterarse de noticias de todo tipo, o simplemente compartir su día a día. Sin embargo, también pueden tener efectos negativos en las relaciones de pareja. El uso de estas redes se ha tergiversado al punto de que *se llega* a compartir información sumamente personal, para luego arrepentirse de haberlo hecho por diferentes razones. Y es allí, donde principalmente se originan los conflictos en las relaciones, especialmente las relaciones de pareja.

g) **Identificación de pedófilos en las redes sociales:** El Ministerio de Educación en colaboración con la Seguridad Nacional, así como las empresas tecnológicas y las proveedoras de los servicios de Internet, impartirá esta formación, teniendo en cuenta que la Seguridad Nacional se encuentra actualizada en estos asuntos relacionados con las redes sociales.



REPUBLICA DE GUINEA ECUATORIAL

PRESIDENCIA

## CAPÍTULO II

### DE LOS MEDIOS DE VIGILANCIA Y SANCIÓN

#### **Artículo 13.- Códigos de conducta.**

El Gobierno, a través del Ministerio encargado de las Nuevas Tecnologías de la Información y Comunicación, deberá suscribir acuerdos o códigos de conducta con las compañías de las redes sociales o plataformas digitales que surjan, en virtud de los cuales estas compañías asuman la responsabilidad de implementar una serie de mecanismos y procedimientos personalizados que permitan suspender publicaciones, contenidos o expresiones ilegales, ofensivas, abusivas o indeseables; sexuales; de terrorismo; de odio por condiciones de género, político, religioso o de raza; de violencia física o moral, de forma rápida y eficaz para proteger a los usuarios víctimas de los mismos.

En caso de la suspensión de contenidos o desactivación de cuentas, el usuario victimario será correctamente informado o notificado y podrá a su vez utilizar mecanismos de impugnación como consumidor. El Gobierno reglamentará esta materia.

Todas las plataformas sociales deberán crear, estipular o reformar todas sus políticas o reglas a una forma sencilla o práctica de lectura y comprensión para sus usuarios, categorizándolos de manera simple en materia de seguridad, información privada, autenticidad, entre otros.

#### **Artículo 14.- Políticas de uso de las redes sociales.**

Los Organismos Públicos y las personas físicas o jurídicas privadas con domicilio en la República de Guinea Ecuatorial que tengan a su cargo empleados, podrán establecer las políticas de uso de las redes sociales al interior de su establecimiento, mediante reglamento interno u obligación contractual, respetando sus derechos fundamentales y laborales.

#### **Artículo 15.- Estructura orgánica de Ciberseguridad.**

El sistema de ciberseguridad y de infraestructuras críticas estará integrado por los órganos e instituciones de la Administración Pública que tengan incidencia importante sobre el funcionamiento de los servicios y actividades



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

esenciales de la sociedad y la protección de derechos, libertades y la seguridad de las personas y sus bienes.

A los efectos de lo dispuesto en el párrafo anterior, integran la estructura orgánica de ciberseguridad e infraestructuras críticas los órganos y entidades siguientes:

Ministerio encargado de Telecomunicaciones y Nuevas Tecnologías.

Ministerio de Seguridad Nacional

Ministerio de Defensa.

Ministerio de Justicia (Fiscalía General de la Republica).

Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC).

**Artículo 16.- Funciones generales de los órganos competentes de Ciberseguridad.**

Los órganos competentes a que se refiere el artículo anterior y cada uno dentro de sus competencias, ejercerán las funciones siguientes:

- a) Gestionar la ciberseguridad e infraestructuras críticas.
- b) Asignar responsabilidad y funciones.
- c) Supervisar el cumplimiento de las normas, directrices y obligaciones de ciberseguridad y seguridad de las infraestructuras críticas.
- d) Investigar las infracciones administrativas y penales.
- e) Recibir notificaciones sobre los incidentes y decidir sobre las medidas aplicables en cada caso.
- f) Establecer y aplicar los protocolos de actuación de todas las partes implicadas, promoviendo el uso de las normas y especificaciones técnicas relativas a la ciberseguridad y a la seguridad de las infraestructuras críticas.
- g) Dictar instrucciones y guías técnicas para la prevención, mitigación y respuesta de un incidente, estableciendo obligaciones específicas para la ciberseguridad y la seguridad de las infraestructuras críticas.



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

- h) Establecer los mecanismos y vías de comunicación y notificación entre las partes participantes.
- i) Coordinar las actuaciones de los Equipos de Respuesta a Incidentes de Seguridad Informática (CERT/CSIRT) en el marco de sus competencias.
- j) Determinar los puntos de contacto y coordinar las actuaciones de los mismos, informándoles las notificaciones de incidentes que hayan recibido.
- k) Publicar, difundir e informar a la población o a los interesados sobre determinados incidentes cuando fuere necesario, para evitar o prevenir un posible incidente o gestionar mejor el ya producido.
- l) Colaborar y cooperar con los demás órganos en materia de seguridad nacional, seguridad ciudadana, salud pública, seguridad jurídica, entre otras.
- m) Promover la colaboración y cooperación con los órganos competentes de otros países y con los organismos internacionales en materia de ciberseguridad y ciberdelincuencia.
- n) Ejercer la potestad sancionadora en el marco de competencia de cada uno.
- o) Cualesquiera otras que se establezcan legal y reglamentariamente.

**Artículo 17.- Ministerio encargado de las Telecomunicaciones y Nuevas Tecnologías.**

El Ministerio encargado de las Telecomunicaciones y Nuevas Tecnologías, será la autoridad competente en materia de ciberseguridad para la protección de los operadores, proveedores y prestadores de servicios de comunicaciones electrónicas.

**Artículo 18.- Ministerio de Seguridad Nacional.**

Además de las funciones por esta Ley, el Ministerio de la Seguridad Nacional es el órgano competente en materia de seguridad pública, ciudadana y nacional, investigación criminal y de la protección de los operadores críticos, cuyas funciones ejercerá bajo la supervisión de la Fiscalía General de la República, y en colaboración con el Ministerio de Defensa Nacional, Ministerio de Interior y Corporaciones Locales, Ministerio de Justicia, Culto e Instituciones Penitenciarias, Ministerio de Información, Prensa y Radio, órganos del Poder



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

Judicial y demás órganos competentes, así como las entidades públicas y privadas y operadores económicos, impulsando la colaboración entre todos ellos y la cooperación internacional.

En materia de investigación criminal, se creará una unidad de policía especial para la protección de ciberseguridad e infraestructuras críticas en el Ministerio, que funcionará bajo la supervisión de un Fiscal especial de la Fiscalía General de la República.

**Artículo 19.- Ministerio de Defensa Nacional.**

Además de las funciones asignadas por esta Ley, el Ministerio de Defensa Nacional ejercerá la función de coordinación de los órganos competentes y de los Equipos o Sistemas CERT/CSIRT, alertando sobre los incidentes, amenazas, riesgos y contingencias que puedan tener lugar.

**Artículo 20.- Ministerio de Justicia, Culto e Instituciones Penitenciarias (Fiscalía General de la Republica).**

La Fiscalía General de la Republica, será la autoridad competente en materia de persecución y acusación sobre los delitos informáticos y cibercrimitos, de conformidad con la legislación vigente.

**Artículo 21.- Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC).**

Se crea la Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC) como ente autónomo de derecho público con personalidad jurídica y presupuesto propio dependiente orgánica y funcionalmente de la Presidencia del Gobierno, y cuyo patrimonio dependerá de los recursos financieros y económicos que le fueren asignados en los Presupuestos Generales del Estado.

La Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC) será competente para ejercer las funciones siguientes:

a) Impulsar el proceso de implementación del sistema de protección de Ciberseguridad y seguridad de las Infraestructuras Críticas en todo el territorio Nacional.

b) Gestionar la Ciberseguridad y seguridad de las Infraestructuras Críticas a través de equipos CERT/CSIRT, coordinándolos.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

c) Supervisar y controlar las actividades y servicios relacionados con la Ciberseguridad y seguridad de las Infraestructuras Críticas.

d) Coordinar las actuaciones y actividades de los órganos y entidades públicas y privadas que se encargan de la protección de datos personales y de la asignación y certificación digital.

e) Velar por la prevención de los incidentes, amenazas, riesgos y contingencias a la Ciberseguridad y la seguridad de las Infraestructuras Críticas.

f) Proteger la Ciberseguridad y las Infraestructuras Críticas a nivel Nacional.

g) Adoptar medidas necesarias y adecuadas o proponer su adopción para dar respuesta a los incidentes, amenazas, riesgos y contingencias a la Ciberseguridad y la seguridad de las Infraestructuras Críticas.

h) Analizar y estudiar el impacto de los incidentes, amenazas, riesgos y contingencias a la Ciberseguridad y la seguridad de las Infraestructuras Críticas.

i) Alertar sobre los posibles ciber incidentes, ciber amenazas y demás contingencias.

j) Analizar y estudiar los indicadores de Ciberseguridad, informando sobre los mismos a los afectados y demás personas, cuando proceda conforme a la Ley.

k) Ejercer la potestad sancionadora.

l) Estudiar, informar y proponer la inclusión o no de las infraestructuras en la lista o Nomenclatura Nacional de Infraestructuras Críticas, o sobre la modificación de la situación de las mismas, determinando el nivel o grado de su criticidad.

m) Asesorar al Gobierno sobre la Ciberseguridad e Infraestructuras Críticas, a las autoridades competentes y a los demás partes implicados.

n) Cooperar con otras agencias y Organismos Internacionales de Ciberseguridad.

o) Cualesquiera otros que se deriven de las anteriores y se establezcan legal y reglamentariamente.



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

**Artículo 22.- Dirección de la Agencia Nacional de Ciberseguridad e Infraestructuras Críticas.**

La gestión y la administración de la Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC), estará a cargo de un Director General, asistido de un Director General Adjunto, que serán nombrados por el presidente de la Republica, a propuesta del Primer/a Ministro/a del Gobierno.

Las competencias y la estructura orgánica de la Agencia Nacional de Ciberseguridad e Infraestructuras Críticas serán establecidas reglamentariamente.

**Artículo 23.- Medios de información.**

El Ministerio encargado de Telecomunicaciones y Nuevas Tecnologías dispondrá, dentro 30 días después de la entrada en vigor de la presente ley, una línea telefónica que servirá como punto de información para proveedores y usuarios de redes globales de información, acerca de las implicaciones legales de su uso en relación con esta ley.

Así mismo, creará una página electrónica en las redes globales, a la cual puedan remitirse los usuarios para formular denuncias contra conductas lesivas o ilícitas publicadas en las redes sociales y señalar las páginas electrónicas; así como, señalar a los autores o responsables de tales publicaciones. En caso de que el Ministerio encargado de Telecomunicaciones y Nuevas Tecnologías reciba por vía telefónica o electrónica denuncias que puedan revestir carácter penal, las mismas deberán ser remitidas de inmediato a las autoridades competentes, con el fin de que se inicie la investigación que corresponda, prevaleciendo siempre lo dispuesto en la Ley de Enjuiciamiento Criminal y el Código Penal en materia de denuncias y persecución de delitos.

Cuando la víctima de la publicación abusiva sea menor de edad, las denuncias o informes recibidos, junto con las acciones correctivas tomadas, deberán ser informadas dentro de las veinticuatro (24) horas siguientes a su recibo.

**Artículo 24.- Denuncia y sanciones.**

La Agencia Nacional de Ciberseguridad e Infraestructuras Críticas (ANCIC) se encargará de tomar medidas a partir de las denuncias formuladas y



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

elevará a la Presidencia de Gobierno, la propuesta de sanción contra los usuarios o administradores responsables de infracciones que operen dentro o fuera del territorio ecuatoguineano, por un monto no superior a VEINTE MILLONES (20.000.000) F. CFA.

Para la imposición de estas sanciones, se aplicará el procedimiento establecido en la Ley de Procedimiento Administrativo vigente, con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

Las infracciones referenciadas en el baremo primero del presente artículo 24, serán recogidas en el Reglamento Orgánico y Funcional de la Agencia Nacional de Ciberseguridad e Infraestructuras Críticas, cuyos montos oscilarán de entre cincuenta mil (50.000) F. CFA y veinte millones (20.000.000) F. CFA; dependiendo de la gravedad de los hechos determinados en el mismo Reglamento.

**TÍTULO III**  
**DE LOS DELITOS INFORMÁTICOS Y CIBERDELITOS**  
**CAPÍTULO I**

**DE LOS DELITOS INFORMÁTICOS**

**Artículo 25.- Acceso indebido a sistemas, programas o datos informáticos.**

1.- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o haga uso parcial o total de un sistema informático que utilice las Tecnologías de la Información y la Comunicación, será sancionado por el órgano jurisdiccional competente con prisión de uno a tres años y una multa de entre 500.000 F. CFA. Y 50.000.000 F. CFA.

2.- El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información y la Comunicación, accediera directa o indirectamente, parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado por el órgano jurisdiccional competente con prisión de dos a cuatro años y una multa de entre 500.000 F. CFA. Y 50.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

3.- Las penas para las conductas descritas en los numerales 1 y 2 del presente artículo, se incrementarán de dos a cuatro años y de tres a cinco años respectivamente, cuando se cometan con fines comerciales o en contra de:

a) Oficinas públicas o bajo su tutela.

b) Instituciones públicas, privadas o mixtas que prestan un servicio público.

c) Bancos, instituciones de micro finanzas, almacenes generales de depósitos, grupos financieros, compañías de seguros y demás instituciones financieras y bursátiles supervisadas y/o reguladas en Guinea Ecuatorial.

**Artículo 26.-Interceptación de comunicaciones y transmisiones entre sistemas de las Tecnologías de la Información y la Comunicación.**

La persona que ilegítimamente intercepte cualquier tipo de comunicación escrita que no le esté dirigida, o que utilizando las Tecnologías de la Información y la Comunicación intercepte cualquier transmisión, hacia, desde o dentro de un sistema informático o cualquier medio tecnológico que no esté disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionada por el órgano jurisdiccional competente con prisión de uno a tres años y multa de entre 500.000 F. CFA y 50.000.000 F. CFA.

**Artículo 27.- Captación indebida de comunicaciones ajenas a través de las Tecnologías de la Información y la Comunicación.**

Quien ilegítimamente, haciendo uso de las Tecnologías de la Información y la Comunicación, o de cualquier otro medio, grabe o capte las palabras o conversaciones ajenas, sean éstas video, imágenes, códigos, audio o texto, no destinadas al público, escuche o intervenga comunicaciones privadas que no estén dirigidas, será penado por el órgano jurisdiccional competente con prisión de uno a tres años y multa de entre 500.000 F C. FA. Y 50.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

**PRESIDENCIA**

**Artículo 28.- Interferencia del sistema informático o datos.**

El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático o los datos contenidos en él, de forma temporal o permanente, será sancionado por el órgano jurisdiccional competente con prisión de tres a cinco años y multa de entre 1.000.000 F. CFA. y 10.000.000 F. CFA.

Si la conducta anterior afectare a los sistemas informáticos del Estado, o aquellos destinados a la prestación de servicios de salud, comunicaciones, financieros, energía, suministro de agua, medios de transporte, puertos y aeropuertos, seguridad ciudadana, sistema de seguridad social, educación en cualquiera de sus subsistemas y defensa nacional u otros de servicio al público, la sanción de prisión será de cuatro a seis años y multa de entre 10.000.000 F. CFA. y 100.000.000 F. CFA.

**Artículo 29.- Alteración, daño a la integridad y disponibilidad de datos.**

El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado por el órgano jurisdiccional competente con prisión de cuatro a seis años y multa de entre 10.000.000 F.CFA y 100.000.000 F.CFA.

**Artículo 30.- Daños a sistemas informáticos.**

El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes físicos o lógicos que lo integran, será sancionado por el órgano jurisdiccional competente con prisión de tres a cinco años y multa de entre 10.000.000 F. CFA. y 100.000.000 F. CFA.

Si el delito previsto en el párrafo anterior se cometiere por imprudencia será sancionado con 2.500.000 F. CFA.

Si el delito previsto en el presente artículo recayera en contra de



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros, o que contengan datos personales, datos personales sensibles, información pública reservada, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de cuatro a seis años y multa de entre 10.000.000 F. CFA. Y 100.000.000 F. CFA.

Si la acción prevista en el párrafo anterior se cometiere por imprudencia será sancionado con 2.500.000 F. CFA.

**Artículo 31.- Posesión de equipos o prestación de servicios para vulnerar la seguridad informática.**

El que posea, produzca, facilite, adapte, importe, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado por el órgano jurisdiccional competente con prisión de cuatro a seis años y multa de entre 10.000.000 F. CFA. y 100.000.000 F. CFA.

**Artículo 32.- Fraude informático.**

El que por uso indebido de las Tecnologías de Información y Comunicación, valiéndose de cualquier manipulación de los sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado por el órgano jurisdiccional competente con prisión de tres a seis años y multa de entre 5.000.000 F. CFA. y 50.000.000 F. CFA.

**Artículo 33.- Espionaje informático.**

Quien indebidamente obtenga datos personales sensibles o información pública reservada, contenida en un sistema que utilice las Tecnologías de Información y Comunicación o en cualquiera de sus componentes, será



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

sancionado por el órgano jurisdiccional competente con prisión de cinco a ocho años y multa de entre 10.000.000 F. CFA. y 100.000.000 F. CFA.

Si algunas de las conductas descritas anteriormente se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas físicas o jurídicas como consecuencia de la revelación de la información pública clasificada como reservada de conformidad a la Ley vigente, la sanción será de seis a diez años de prisión y multa de entre 10.000.000 F. CFA. y 100.000.000 F. CFA.

**Artículo 34.- Violación de la seguridad del sistema informático.**

La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido, será sancionada por el órgano jurisdiccional competente con prisión de dos a cinco años y multa de entre 1.000.000 F. CFA. y 10.000.000 F. CFA.

Igual sanción se impondrá a quien induzca a un tercero para que de forma involuntaria realice la conducta descrita en el párrafo anterior.

**Artículo 35.- Hurto por medios informáticos.**

El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado por el órgano jurisdiccional competente con prisión de dos a cinco años, la restitución del importe hurtado y una multa igual al doble de lo hurtado.

**Artículo 36.- Manipulación de registros.**

Quien, abusando de sus funciones de administración de plataformas tecnológicas, públicas o privadas, deshabilite, altere, oculte, destruya, o inutilice en todo o en parte cualquier información, dato contenido en un registro de acceso o uso de los componentes de éstos, se le impondrá por el órgano jurisdiccional competente la pena de cinco a ocho años de prisión y multa de entre 10.000.000 F. CFA Y 100.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

**PRESIDENCIA**

Si las conductas descritas anteriormente favorecieren la comisión de otro delito por un tercero, la pena se agravará hasta en un tercio en su límite inferior o superior.

**Artículo 37.- Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares.**

El que intencionalmente y sin la debida autorización por cualquier medio cree, capture, grave, copie, altere, duplique, clone o elimine datos informáticos y electrónicos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, se le impondrá por el órgano jurisdiccional competente la pena de cinco a ocho años de prisión y multa de entre 5.000.000 F.CFA y 100.000.000 F.CFA.

**Artículo 38.- Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares.**

El que, sin autorización, haciendo uso de las Tecnologías de la Información y la Comunicación, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, para la obtención de cualquier bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida obtenida, se le impondrá por el órgano jurisdiccional competente la pena de cinco a ocho años de prisión y multa de entre 5.000.000 F. CFA y 100.000.000 F. CFA.

**Artículo 39.- Provisión indebida de bienes o servicios.**

Quien a sabiendas que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado o alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico se le impondrá por el órgano jurisdiccional competente la pena de cinco a ocho años de prisión y multa de entre 10.000.000 F. CFA y 100.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

**Artículo 40.- Violación de la custodia judicial de datos.**

Quien a sabiendas que un sistema informático o cualquiera de sus componentes se encuentra bajo custodia judicial y haga uso de éstos, manipule sus registros o contenidos, violente los precintos o sellados, se le impondrá por el órgano jurisdiccional competente la pena de uno a cuatro años de prisión y multa de entre 10.000.000 F. CFA y 100.000.000 F. CFA.

Si la acción descrita en el párrafo anterior fuere realizada, facilitada o permitida por el encargado de la custodia judicial se le impondrá una pena de dos a cinco años de prisión y multa de entre 10.000.000 F. CFA y 100.000.000 F. CFA.

**Artículo 41.- Falta a la confidencialidad.**

Quien faltare a la confidencialidad sobre la información que conoció en ocasión de su participación en el proceso de investigación, recolección, interceptación o intervención de datos de un sistema informático o de sus componentes, se le impondrá por el órgano jurisdiccional competente la pena de cuatro a seis años y una multa de entre 500.000 F. CFA y 5.000.000 F. CFA.

**CAPÍTULO II**

**CIBERDELITOS**

**Artículo 42.- Suplantación y apropiación de identidad informática.**

El que suplantare o se apoderare de la identidad informática de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, se le impondrá por el órgano jurisdiccional competente la pena de tres a cinco años de prisión y multa de entre 1.000.000 F. CFA y 10.000.000 F. CFA.

Si con las conductas descritas en el párrafo anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros, se le impondrá de cinco a ocho años de prisión y una multa de entre 5.000.000 F. CFA y 50.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

**Artículo 43.- Divulgación no autorizada.**

El que sin autorización diere a conocer un código, contraseña o cualquier otro medio de acceso a un programa, información o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse a sí mismo, a un tercero o para cometer un delito, se le impondrá por el órgano jurisdiccional competente la pena de cinco a ocho años de prisión y una multa de entre 1.000.000 F. CFA y 10.000.000 F. CFA.

**Artículo 44.- Utilización de datos personales.**

El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, se le impondrá por el órgano jurisdiccional competente la pena de cuatro a seis años de prisión y una multa de entre 1.000.000 F. CFA y 10.000.000 F. CFA.

La sanción aumentará hasta en una tercera parte del límite superior de la pena prevista en el párrafo anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.

**Artículo 45.- Transferencia de información pública reservada.**

El que sin autorización o excediendo la que se le hubiere concedido, transfiera información Pública clasificada como reservada, de conformidad con la ley en la materia y que mediante el uso de esa información vulnere un sistema o datos informáticos o se pusiere en peligro la seguridad del Estado, apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, se le impondrá por el órgano jurisdiccional competente la pena de ocho a quince años de prisión y una multa de entre 50.000.000 F. CFA y 500.000.000 F. CFA.



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

**Artículo 46.-Revelación indebida de datos o información de carácter personal.**

El que, sin el consentimiento del titular de la información de carácter privado y personal, revele, difunda o ceda en todo o en parte, dicha información o datos, sean éstos en imágenes, vídeo, texto, audio u otros, obtenidos por medio de las Tecnologías de la Información y la Comunicación, se le impondrá por el órgano jurisdiccional competente la pena de tres a seis años de prisión y una multa de entre 1.000.000 F. CFA y 10.000.000 F. CFA.

Si alguna de las conductas descritas en el párrafo anterior, se hubiese realizado con ánimo de lucro, facilitare la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, se le impondrá la pena de cuatro a ocho años de prisión y multa de entre 5.000.000 F CFA y 50.000.00 F CFA.

Se impondrá el límite máximo de la pena del párrafo anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el presente artículo, recae sobre datos personales sensibles.

**Artículo 47.-Suplantación informática en actos de comercialización.**

Quien, mediante el uso de las Tecnologías de la Información y la Comunicación, venda o comercialice bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado, será sancionado por el órgano jurisdiccional competente la pena de tres a cinco años de prisión y una multa de entre 1.000.000 F. CFA y 10.000.000 F. CFA.

La conducta descrita en el párrafo anterior se agravará con pena de prisión de cuatro a seis años y una multa de entre 5.000.000 F. CFA y 20.000.000 F. CFA., cuando la venta o comercialización sea de medicamentos, suplementos o productos alimenticios, bebidas o cualquier producto de consumo humano.

**Artículo 48.- De las amenazas a través de las Tecnologías de la Información y la Comunicación.**

Quien amenace a otro a través del uso de las Tecnologías de la Información y la Comunicación con:



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

1) Causar a él, a su familia o a otras personas con las que esté relacionado, un mal que constituya delito y que por su naturaleza parezca verosímil, se le impondrá por el órgano jurisdiccional competente la pena de uno a tres años de prisión y una multa de entre 5.000.000 F. CFA. y 15.000.000 F. CFA.

2) Hacer imputaciones contra el honor, o el prestigio, violar o divulgar secretos, con perjuicio para él, su familia, otras personas con la que esté relacionado, o entidad que representa o en que tenga interés, se le impondrá por el órgano jurisdiccional competente la pena de dos a cuatro años de prisión y una multa de entre 5.000.000 F. CFA. y 15.000.000 F. CFA.

*a)* Si la amenaza se hiciera en nombre de entidades o grupos reales o supuestos, se impondrá pena de tres a cinco años de prisión.

*b)* Si la amenaza de un mal que constituya delito fuese dirigida a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, colectivo social o a cualquier otro grupo de personas y tuvieran la capacidad necesaria para conseguirlo, se le impondrá por el órgano jurisdiccional competente la pena de seis a diez años de prisión y una multa de entre 100.000.000 F. CFA. Y 500.000.000 F.CFA.

**Artículo 49.- Provocación, apología e inducción a la comisión de delitos a través de las Tecnologías de la Información y la Comunicación.**

Quien, haciendo uso de las Tecnologías de la Información y la Comunicación, incite, instigue, provoque o promueva la comisión de delitos, ensalce el crimen o enaltezca a su autor o partícipes o se lo adjudique, se le impondrá por el órgano jurisdiccional competente la pena de tres a cinco años de prisión y una multa de entre 10.000.000 F. CFA y 100.000.000 F. CFA.

**Artículo 50.- Propagación de noticias falsas a través de las Tecnologías de la Información y la Comunicación.**

1.- Quien, usando las Tecnologías de la Información y la Comunicación, publique o difunda información falsa y/o tergiversada, que produzca alarma, temor, zozobra en la población, o a un grupo o sector de ella a una persona o a



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

su familia, se le impondrá por el órgano jurisdiccional competente la pena de dos a cuatro años de prisión y una multa de entre 5.000.000 F. CFA y 50.000.000 F. CFA.

2.- Si la publicación o difusión de la información falsa y/o tergiversada, perjudica el honor, prestigio o reputación de una persona o a su familia, se le impondrá una pena de tres a seis años de prisión y multa de entre 5.000.000 F. CFA y 50.000.000 F. CFA.

3.- Si la publicación o difusión de la información falsa y/o tergiversada, incita al odio y a la violencia, pone en peligro la estabilidad económica, el orden público, la salud pública o la seguridad del Estado, se le impondrá por el órgano jurisdiccional competente la pena de diez a veinticinco años de prisión y multa de entre 100.000.000 F. CFA y 500.000.000 F. CFA.

**Artículo 51.- Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación.**

Quien, por medio del uso de las Tecnologías de la Información y la Comunicación, induzca, facilite, promueva, utilice, abuse o explote con fines sexuales o eróticos a niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado, se le impondrá por el órgano jurisdiccional competente la pena de cinco a diez años de prisión y una multa de entre 5.000.000 F. CFA y 50.000.000 F. CFA.

No se reconoce, en ninguno de los supuestos descritos en el párrafo anterior, valor al consentimiento de la víctima.

**Artículo 52.- Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación.**

1.- Toda persona mayor de 18 años que haga propuestas implícitas o explícitas a personas menores de 16 años o personas con discapacidad necesitada de especial protección para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

de la Información y la Comunicación para sí o para terceros, se le impondrá por el órgano jurisdiccional competente la pena de cinco a diez años de prisión y una multa de entre 5.000.000 F. CFA. y 50.000.000 F. CFA.

2.- Si algunas de las conductas descritas anteriormente, se cometiere con el fin de obtener beneficios pecuniarios para sí o para terceros, la pena será de cinco a quince años de prisión y una multa de entre 5.000.000 F. CFA. y 50.000.000 F. CFA.

**Artículo 53.- Acoso a través del uso de las Tecnologías de la Información y la Comunicación.**

1.- Quien atormente, hostigue, humille, insulte, denigre o manifieste otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física, por medio del uso de las Tecnologías de la Información y la Comunicación, se le impondrá por el órgano jurisdiccional competente la pena de dos a cuatro años de prisión y una multa de entre 2.000.000 F. CFA. y 25.000.000 F. CFA.

2.- Cuando la víctima sea niña, niño, adolescente o persona con discapacidad necesitada de especial protección, se le impondrá pena de cuatro a seis años de prisión y una multa de entre 5.000.000 F. CFA. y 50.000.000 F. CFA.

**Artículo 54.- Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación.**

1.- Incurrir el delito de acoso sexual con penas de uno a dos años de prisión y multa de 2.000.000 a 25.000.000 F. Cfas, la persona mayor de edad que solicitare favores de naturaleza sexual, usando medios de la tecnología de la información y de las comunicaciones, para sí o para un tercero, en el ámbito de una relación laboral, docente, de prestación de servicios o análoga, poniendo a la víctima en una situación objetiva y gravemente intimidatoria, hostil o humillante.

2.- El culpable de acoso sexual que hubiera cometido el hecho prevaliéndose de una situación de superioridad laboral, docente o jerárquica, o sobre persona sujeta a su guarda o custodia, o con el anuncio expreso o tácito de causar a la víctima un mal relacionado con las legítimas expectativas que aquella



REPUBLICA DE GUINEA ECUATORIAL

---

**PRESIDENCIA**

---

pueda tener en el ámbito de la indicada relación y, si el acto sexual solicitada se hubiere consumado, como si la amenaza hubiera llegado a realizarse, será castigado con penas de dos a cuatro años de prisión.

3.- Cuando la víctima sea menor de 16 años, con o sin su consentimiento o persona con discapacidad necesitada de especial protección se le impondrá pena de cuatro a seis años de prisión, y una multa de entre 5.000.000 F. CFA. y 50.000.000 F. CFA.

**Artículo 55.- Circunstancias agravantes comunes.**

Los delitos referidos a los Artículos 52 al 55 serán sancionados con la pena máxima correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las acciones descritas fuera realizado por:

1. Ascendientes, descendientes, hermanos, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad;
2. Autoridad, funcionario y empleado público;
3. La persona encargada de la tutela, curatela, protección o vigilancia de la víctima; y
4. Toda persona que, prevaliéndose de la superioridad originada por relaciones de confianza, educativa, de trabajo, credo/religioso o cualquier otra relación.

**Artículo 56.- Investigación, obtención y preservación de datos.**

En la investigación, obtención y preservación de los datos contenidos en un sistema de información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, se aplicará lo establecido en la presente Ley, sin perjuicio de las limitaciones establecidas en las demás Disposiciones reguladoras de Protección de datos personales y la conservación de datos en las comunicaciones electrónicas y redes de comunicación.



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

**Artículo 57.- Conservación de datos.**

La Policía Nacional o el Ministerio Fiscal, en el ámbito de su competencia, actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

**Artículo 58.- Medidas de aseguramiento.**

Sin perjuicio de cualesquiera otras medidas de aseguramiento que pudieran contribuir a la persecución efectiva de los delitos comprendidos dentro del ámbito de aplicación de esta Ley, los órganos competentes podrán solicitar las siguientes medidas específicas:

1. La incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos.
2. El sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos.
3. El requerimiento de preservación inmediata de datos que se hallen en poder de terceros.
4. La copia de datos.

**Artículo 59.- Solicitud de autorización judicial.**

En la etapa de investigación para la obtención y conservación de la información contenida en los sistemas informáticos o cualquiera de sus componentes, se requerirá autorización judicial, a petición debidamente fundamentada por la Policía Nacional o el Ministerio Fiscal. Una vez iniciado el proceso, cualquiera de las partes podrá solicitar la autorización al Juez competente.

Para tal efecto, el Juez podrá:



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

1. Ordenar a una persona física o jurídica la entrega inmediata de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;
2. Ordenar a una persona física o jurídica preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, conservar los datos de tráfico, conexión, acceso o cualquier otra información que se encuentre en su poder o bajo su control y que pueda ser de utilidad a la investigación, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada una sola vez por el mismo plazo;
3. Ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;
4. Ordenar a un proveedor de servicios suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control;
5. Secuestrar o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;
6. Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes;
7. Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes;
8. Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accedido para la investigación;
9. Ordenar a la persona que tenga conocimiento acerca del funcionamiento de un sistema de información o de cualquiera de sus componentes o de las medidas de protección de los datos en dicho sistema, a proveer la información necesaria para realizar las investigaciones correspondientes;



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

10. Ordenar la extracción, recolección o grabación de los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;

11. Ordenar al proveedor de servicios, recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;

12. Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, de conformidad con la legislación.

13. Ordenar cualquier otra medida aplicable a un sistema de información o sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos.

Si la autorización es decretada luego de celebrada la Audiencia Preliminar o la Inicial, según se trate, el defensor deberá ser notificado y tendrá derecho a estar presente en la práctica del acto.

En casos de urgencia para realizar el acto de investigación, se procederá de conformidad con la Ley.

**Artículo 60.- Competencia Objetiva.**

Los delitos previstos en la presente Ley serán de la competencia de los Juzgados de Instrucción y de los Órganos de enjuiciamiento penal previstos en la vigente Ley Orgánica de Poder Judicial.

**Artículo 61.- Responsabilidad del custodio judicial de sistemas informáticos.**

A quien se le haya confiado la preservación del sistema informático o de cualquiera de sus componentes, así como de su contenido, conservará la confidencialidad e integridad de los mismos, impidiendo que terceros, fuera de las autoridades competentes, tengan acceso y conocimiento de ellos.

Asimismo, la persona encargada de la custodia no podrá hacer uso del



REPUBLICA DE GUINEA ECUATORIAL

-----  
**PRESIDENCIA**  
-----

sistema de información o de cualquiera de sus componentes en custodia para fines distintos a los concernientes al proceso investigativo.

**Artículo 62.- Confidencialidad del proceso investigativo.**

Los que participen en el proceso de investigación, recolección, interceptación, intervención de datos de un sistema de información o de sus componentes, mantendrá la confidencialidad de toda la información que conociere sobre la ejecución de los actos realizados por parte de la autoridad competente.

**Artículo 63.- La extradición.**

Para efectos de extradición relacionada a la comisión de los delitos tipificados en la presente Ley, a falta de Tratados o Convenios Internacionales de los cuales la República de Guinea Ecuatorial sea Estado parte, las condiciones, el procedimiento y los efectos de la extradición estarán determinados por lo dispuesto en la legislación ecuatoguineana vigente en materia de extradición, lo cual se aplicará también a los aspectos que no hayan sido previstos por el Tratado o Convenio respectivo.

**Artículo 64.- De la asistencia judicial mutua.**

Las autoridades competentes de la República de Guinea Ecuatorial podrán prestar o solicitar cooperación internacional o asistencia judicial mutua, en las investigaciones y procesos relacionados con la aplicación de la presente Ley, de conformidad con los Convenios o Tratados Internacionales en los que la República de Guinea Ecuatorial sea Estado parte.

A falta de Acuerdo, Convenio o Tratado, podrá prestarse o solicitarse asistencia legal mutua en base al principio de reciprocidad.

**DISPOSICIÓN ADICIONAL**

Se faculta al Gobierno dictar cuantas disposiciones sean necesarias para el cumplimiento de lo dispuesto en la presente Ley.



REPUBLICA DE GUINEA ECUATORIAL

PRESIDENCIA

### DISPOSICIÓN DEROGATORIA

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta Ley.

### DISPOSICIÓN FINAL

La presente Ley entrará en vigor a los 90 días siguientes de su publicación en el Boletín Oficial del Estado o en los Medios de Comunicación Oficiales.

Así lo dispongo por la presente Ley, dada en Malabo, a veintitrés días del mes de diciembre del año dos mil veinticuatro.

**POR UNA GUINEA MEJOR,**



**OBIANG NGUEMA MBASOGO  
PRESIDENTE DE LA REPÚBLICA.**

Boletín Oficial del Estado.