ISSN 1682-7511

GACETA OFICIAL

DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

EDICIÓN ORDINARIA LA HABANA, VIERNES 13 DE SEPTIEMBRE DE 2024 AÑO CXXII

Sitio Web: http://www.gacetaoficial.gob.cu/—Calle Zanja No. 352 esquina a Escobar, Centro Habana

Teléfonos: 7878-4435 y 7870-0576

Número 89 Página 1519

SUMARIO

CONSEJO DE ESTADO

GOC-2024-527-O89

JUAN ESTEBAN LAZO HERNÁNDEZ, Presidente de la Asamblea Nacional del Poder Popular.

HAGO SABER: Que el Consejo de Estado ha considerado lo siguiente:

POR CUANTO: La Constitución de la República de Cuba y la legislación vigente en materia de telecomunicaciones, datos personales, protección al consumidor, entre otras que se han regulado de interés para la población y el país, dispone los fundamentos generales que permiten establecer la protección criptográfica de los contenidos informativos, la correspondencia, los datos personales que procesan las personas jurídicas y naturales, y de las trazas que emiten los medios, aplicaciones, servicios e infraestructuras técnicas de las gestiones informativas, las comunicaciones y los controles automáticos.

POR CUANTO: Los servicios de protección criptográfica salvaguardan la confidencialidad, integridad, autenticación, valor probatorio y no repudio de la información y las transacciones que producen, conservan y transmiten las personas naturales y jurídicas en sus actividades legítimas, así como los datos que emanan de los medios, aplicaciones, servicios e infraestructuras técnicas que se emplean, frente a las acciones delictivas e intrusivas que atenten contra los intereses del Estado y los de las citadas personas.

POR CUANTO: La utilización confiable y ordenada de la protección criptográfica constituye una prioridad para la seguridad del país, y la protección de los derechos y garantías de los ciudadanos a tono con el proceso de informatización de la sociedad cubana, lo que hace necesario adecuar los sistemas de trabajo con los dispositivos, servicios, recursos humanos y materiales que la garantizan, y al mismo tiempo asegurar su permanente desarrollo y sostenimiento con calidad, independencia, disciplina y soberanía tecnológica.

POR CUANTO: El Decreto-Ley 199 "Sobre la Seguridad y Protección de la Información Oficial", de 25 de noviembre de 1999, limita el marco jurídico del desarrollo, aplicación y empleo de la protección criptográfica al ámbito del citado tipo de información, lo que en el contexto actual requiere de una ampliación en beneficio de la transformación digital de la sociedad.

POR TANTO: El Consejo de Estado, en el ejercicio de la atribución que le está conferida, en el Artículo 122, inciso c), de la Constitución de la República de Cuba, acuerda dictar el siguiente:

DECRETO-LEY 79
SOBRE EL DESARROLLO, LA APLICACIÓN Y USO DE LOS DISPOSITIVOS DE PROTECCIÓN CRIPTOGRÁFICA Y SERVICIOS EN LA ESFERA DE LA CRIPTOGRAFÍA EN LA REPÚBLICA DE CUBA

CAPÍTULO I
GENERALIDADES

Artículo 1. El presente Decreto-Ley tiene por objeto ordenar el desarrollo científico y técnico, la aplicación y el uso de los dispositivos de protección criptográfica, en lo adelante, criptodispositivos; la organización y funcionamiento de los servicios en la esfera de la criptografía, en lo sucesivo, servicios criptográficos; y el funcionamiento del sistema de trabajo nacional para asegurar integralmente la calidad de los citados productos y servicios, en lo adelante, Sistema de Aseguramiento Integral.

Artículo 2.1. El Ministerio del Interior es el organismo de la Administración Central del Estado encargado de proponer y, una vez aprobada, implementar la política del Estado y el Gobierno en materia de criptografía para su desarrollo científico, tecnológico e industrial, la aplicación práctica y el uso de los criptodispositivos; la organización y funcionamiento de los servicios criptográficos y el sistema que lo asegura en el territorio nacional, las representaciones de Cuba en el exterior, el ciberespacio con dominio cibernético cubano, y la interrelación del país con el mundo.

2. En función del cumplimiento de lo previsto en el apartado anterior, se auxilia del Órgano Especializado en materia de criptografía del Ministerio del Interior, en lo adelante Órgano Especializado, para dirigir:

a) La actividad reguladora, la fiscalización e inspección estatal, la validación y certificación de la calidad de los criptodispositivos y demás elementos que conforman la protección criptográfica; así como de la emisión de permisos para la prestación de los servicios en el ámbito de la criptografía, que se describen en el presente Decreto-Ley;
b) el Sistema de Aseguramiento Integral, cuya composición se describe en el presente Decreto-Ley;
c) el Servicio Central de Cifras;
d) las actividades para impedir, descubrir, neutralizar, eliminar y enfrentar las acciones ilícitas en la esfera de la criptografía, que afectan la defensa y seguridad nacional,

y la de terceros países desde el territorio nacional, la tranquilidad ciudadana y la confianza de las personas naturales en el uso de los servicios criptográficos; y

e) los asuntos relacionados con el establecimiento de vínculos de cooperación, colaboración, comercio y servicios con sujetos homólogos extranjeros y el intercambio con los organismos internacionales en materia de criptografía.

Artículo 3. Los jefes de las unidades organizativas que se encargan de la dirección de los sistemas de Seguridad y Protección en los órganos, organismos y entidades del Estado, las organizaciones políticas, sociales y de masas, y del sistema empresarial, garantizan en sus ámbitos de competencia, las condiciones técnicas y de seguridad en locales y medios generales que se utilizan para la protección criptográfica, así como la capacitación y el completamiento de los recursos humanos que se designan con el fin de su atención técnica y funcional, en correspondencia con los dictámenes y propuestas emitidas por el Órgano Especializado.

CAPÍTULO II

DE LOS CRIPTODISPOSITIVOS Y LOS SERVICIOS CRIPTOGRÁFICOS

SECCIÓN PRIMERA

Disposiciones generales

Artículo 4.1. Se define como criptodispositivo, al medio o bien social o individual, conformado por componentes mecánicos, electrónicos y de software o combinados, que ejecuta operaciones para la transformación de una información inteligible en un dato cifrado, o viceversa, y que incluye como un sub componente distintivo a los criptomateriales, que se constituyen como el conjunto de piezas de información crítica, y se construyen a partir de una secuencia de números, letras o alfanuméricas con características específicas que controla la operación y la seguridad de un criptodispositivo y del proceso de cifre y descifre; comúnmente denominadas llaves criptográficas.

2. Los servicios criptográficos son las prestaciones que se conforman con los medios, normas, procedimientos, planes, cartas tecnológicas, medidas de control y seguridad, y el personal especializado que se autoriza para la realización de actividades de la esfera de la criptografía que se describen en el presente Decreto-Ley.

Artículo 5. El Estado promueve la explotación en el país de los criptodispositivos provenientes de la industria cubana, y ejerce la soberanía sobre la actividad de administración del ciclo de vida de los criptomateriales, tanto en el territorio nacional como en sus representaciones estatales, de colaboración y comerciales cubanas en el exterior, de acuerdo con las medidas que dicta al efecto el Ministerio del Interior, quien además examina y aprueba el suministro por fuentes extranjeras de tecnologías criptográficas y criptomateriales, en los casos específicos que lo requieran los sistemas a proteger.

Artículo 6. Todos los criptodispositivos y servicios de protección criptográfica que operan en el territorio nacional y en las representaciones estatales, de colaboración y comerciales cubanas en el exterior, se certifican y acreditan, por el Órgano Especializado, conforme a las distintas categorizaciones de los sistemas y procesos a proteger, según la legislación vigente y el presente Decreto-Ley.

Artículo 7.1. El tratamiento de los servicios en la esfera de la criptografía se estructura a partir de la atención diferenciada a:

a) La salvaguarda de la información clasificada y limitada que gestionan las personas naturales y jurídicas en sus funciones políticas, estatales, administrativas, guber-

namentales, económicas y sociales a todos los niveles organizativos del país, así como de los datos que emanan de las operaciones técnicas de los medios, aplicaciones, redes, servicios e infraestructuras de procesamiento, almacenamiento y transmisión para la gestión del citado tipo de información y de los procesos automáticos críticos para la vitalidad y seguridad nacional.

Los criptodispositivos que se emplean a tales fines y su documentación tecnológica, se tratan como material clasificado, y se construyen, suministran, operan, custodian y resguardan con medidas que contrarrestan las amenazas y riesgos de agresión para la defensa y seguridad nacional.

Estos servicios criptográficos se proporcionan por prestadores con especialización técnica de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, así como por otros que aprueba el Ministerio del Interior para casos específicos.

b) La salvaguarda de la información no clasificada que gestionan las personas naturales y jurídicas en sus actividades y trámites electrónicos legales hasta nivel de población, y de los datos que emanan de las operaciones técnicas de los medios, aplicaciones, redes, servicios e infraestructuras de procesamiento, almacenamiento y transmisión para la gestión del citado tipo de información.

Los criptodispositivos que se emplean a tales fines y su documentación tecnológica, se tratan como materiales no clasificados y se construyen, operan, suministran, custodian, y resguardan aplicando medidas que contrarrestan las amenazas y riesgos de agresión con técnicas accesibles al público y factibles para cometer acciones delictivas.

c) La exportación, importación, producción nacional y comercio en la red minorista del país de criptodispositivos para la protección de la información no clasificada, así como las actividades académicas en la esfera de la criptografía, que se realiza por el Ministerio del Interior, en coordinación con los ministerios del Comercio Exterior y la Inversión Extranjera, Comercio Interior, Comunicaciones, Ciencia, Tecnología y Medio Ambiente, Educación Superior e Industrias, según corresponda.

2. Los servicios y asuntos que se describen en los incisos b) y c) del apartado anterior se aseguran por prestadores, los que deben contar con la acreditación correspondiente y cumplen las normas técnicas cubanas establecidas al efecto.

Artículo 8. Los servicios de Telecomunicaciones y de las Tecnologías de la Información y la Comunicación, en lo adelante Telecomunicaciones/TIC, que para su operación necesiten la aplicación de criptodispositivos, requieren del dictamen previo del Órgano Especializado; para ello los ministerios de Comunicaciones y del Interior, coordinan las acciones que correspondan.

Artículo 9. Los titulares de los órganos, organismos y entidades del Estado, las organizaciones políticas, sociales y de masas, y del sistema empresarial, establecen la obligatoriedad para el empleo de protección criptográfica en los sistemas técnicos de gestión informativa o de transacciones de datos, en sus respectivos ámbitos de competencia.

Artículo 10.1. Los proveedores de servicios criptográficos aseguran su actividad y la oferta de garantías de seguridad a los clientes, con sus recursos y finanzas.

2. Los gastos para la implementación de los servicios de protección criptográfica que requieren las personas naturales y jurídicas para su actividad, se planifican y ejecutan desde sus presupuestos.

Artículo 11. Las personas naturales o jurídicas que incumplan lo establecido en las leyes y las normas técnicas cubanas para la transmisión de señales electrónicas que se realice con protección criptográfica, por cualquier vía, forma o medio, se les puede cancelar o

suspender dicha transmisión cuando afecte el derecho de los demás, la seguridad colectiva, el bienestar general o el respeto al orden público, así como que incumpla la Constitución y las leyes.

Artículo 12.1. Los usuarios de servicios criptográficos al detectar que se haya vulnerado la seguridad de un criptodispositivo que emplee para fines legítimos y que se encuentre nominado en las listas oficiales de calidad de los productos de esta naturaleza, están obligados a notificar el incidente al proveedor del servicio y al Órgano Especializado, a los efectos procedentes.

2. Si como resultado de las investigaciones realizadas no se determina responsabilidad del usuario en el incidente, este puede interponer la reclamación pertinente al proveedor del servicio, de acuerdo con lo establecido en la legislación vigente.

3. El proveedor del servicio está obligado a restablecer la protección criptográfica en función de restaurar el estándar de seguridad vulnerado.

Artículo 13. Las conductas violatorias del régimen de seguridad establecido para el desarrollo, producción, aplicación y el uso de los criptodispositivos, en que puedan incurrir las personas naturales o jurídicas que brinden o reciban servicios criptográficos, quedan sujetas a la aplicación de medidas administrativas, laborales o penales, si son declarados responsables de estas, según corresponda.

SECCIÓN SEGUNDA

Sobre los criptodispositivos, su fabricación y suministro

Artículo 14. Los criptodispositivos se implementan para garantizar la confidencialidad, privacidad, autenticación, integridad, control de acceso y no repudio de transacciones o eventos informativos de datos, voz, imagen y documentación que producen las personas naturales y jurídicas en sus actividades, así como de los datos, metadatos y trazas que emiten los medios, aplicaciones, servicios e infraestructuras técnicas que los gestionan durante su procesamiento, conservación y transmisión.

Artículo 15. El Órgano Especializado emite las normas técnicas y procedimientos pertinentes para la clasificación técnica de los criptodispositivos, en virtud de la facilitación y seguridad en su desarrollo, asimilación, innovación, producción y empleo en el país.

Artículo 16. Los prestadores de servicios autorizados para el abastecimiento, asistencia y actualización técnica de los criptodispositivos que emplea el país, adoptan las medidas pertinentes y comprobables que aseguren la invulnerabilidad y confianza en los diversos canales de la cadena de suministros que se utilicen, frente al probable carácter de las acciones agresivas de terceros.

Artículo 17.1. El encadenamiento productivo para la creación, producción y suministros de criptodispositivos a los fines del consumo nacional y la exportación, se realiza entre prestadores de servicios autorizados por el Órgano Especializado.

2. El Órgano Especializado, examina y aprueba las propuestas de encadenamientos productivos señaladas en el apartado anterior.

3. Excepcionalmente, el ministro del Interior aprueba suministradores y fabricantes no previstos en el encadenamiento productivo que por necesidades del país se requieran.

Artículo 18.1. El Órgano Especializado valida, clasifica y aprueba, para su distribución, los resultados científicos y tecnológicos con el fin de convertir en técnica aplicable, los métodos y funciones matemáticas a los efectos de realizar operaciones criptográficas, en virtud de su entrega a un proceso de fabricación de criptodispositivos.

2. En este proceso es obligatorio el cumplimiento de la legislación vigente en materia de propiedad intelectual e industrial.

Artículo 19. Los fabricantes, importadores y operadores nacionales de medios, aplicaciones, servicios e infraestructuras de las Telecomunicaciones/TIC y de la automatización, están obligados a incluir en sus productos y servicios, los criptodispositivos que aparecen en las listas de aprobación que emite el Órgano Especializado.

Artículo 20. Los procedimientos para la realización de las actividades descritas en los artículos 17,18 y19 del presente Decreto-Ley, se establecen por el Ministerio del Interior, en coordinación con los organismos competentes.

SECCIÓN TERCERA

Sobre la organización de los servicios criptográficos

Artículo 21. Los servicios criptográficos se organizan e implementan para funcionar ininterrumpidamente en cualquier circunstancia que enfrente el país, y se clasifican en:

1. Servicio Central de Cifras, se ejecuta por personal especializado del Ministerio del Interior, para la dirección, elaboración, ejecución de proyectos, diseños, producción y suministros de criptodispositivos y criptomateriales asociados; la realización de operaciones de cifre y descifre de la información; la asistencia técnica a los citados medios y la capacitación de sus usuarios, en virtud de la protección de los sistemas informativos y sus tecnologías de gestión, en interés de la seguridad nacional.
2. Servicios de la Industria de Medios Criptográficos, se ejecutan para proyectar, diseñar, ensayar y producir criptodispositivos y criptomateriales; capacitar al cliente y entregarle la documentación sobre el manejo y las garantías de dichos medios, también pueden abarcar el suministro y asistencia técnica a los puntos finales que operan la protección informativa.
3. Servicios de Operaciones y Administración Criptográfica, se ejecutan para el cifre y descifre informativo, la asistencia técnica, la defensa colateral, administración, guarda y custodia de los criptodispositivos y criptomateriales en operación, en vinculación con los propietarios de la información a proteger, las actividades automáticas o los operadores.
4. Servicios de la Infraestructura Nacional de Llave Pública, se ejecutan para el registro, expedición, validación ante el público, renovación y revocación de certificados digitales de llave pública y sus criptomateriales.
5. Servicios de Cadena de Bloques, se prestan para la emisión de un registro único sobre un dato o activo digital existente, que se conforma con la toma de muestras en cadena seriada que acuñan de forma independiente con métodos de firma digital, los entes integrantes del servicio.
6. Servicios de Confianza Digital basados en Certificados Digitales de Llave Pública, que se constituyen para las prestaciones intermediarías de protección de activos, bienes o hechos digitales como terceras partes confiables.
7. Servicios Académicos, se ejecutan para la impartición de docencia teórica y práctica, para la actualización de conocimientos, el ejercicio de consultorías científico técnica, y el suministro de literatura y publicaciones no clasificadas y limitadas sobre la ciencia de la criptografía.

Artículo 22. Los certificados digitales de llave pública, registros y sellos electrónicos que emiten los prestadores de servicios de la Infraestructura Nacional de Llave Pública, de Cadena de Bloques y de Confianza Digital, y las firmas digitales que dichos prestadores plasman sobre los citados objetos por ellos producidos, tienen valor para las gestiones informatizadas nacionales e internacionales.

Artículo 23.1. Todos los prestadores de servicios criptográficos radican en el territorio nacional o en el ciberespacio con dominio cibernético cubano, y están en la obligación de

publicar sus declaraciones de políticas de seguridad y prácticas para el servicio ante sus clientes.

2. Los casos de prestadores de servicios criptográficos que radican en el exterior o con dominio cibernético fuera de Cuba, se aprueban por el Ministro del Interior, en consulta con los organismos de la Administración Central del Estado o entidad, en correspondencia con el nivel de actividad que se protege.

Artículo 24.1. Los diferentes tipos de servicios criptográficos establecidos en el presente Decreto-Ley, se estructuran y funcionan sobre la base de:

a) Los documentos normativos de la criptografía para aplicar la protección de la información y los datos de todo tipo y formato que aseguran el cumplimiento de lo que establecen las disposiciones jurídicas, normas técnicas y procedimientos vigentes al respecto;
b) el funcionamiento de los medios, aplicaciones, servicios e infraestructuras técnicas de la información, la comunicación y la automatización, la ciberseguridad y el mantenimiento del ambiente de control interno en la entidad o espacio de aplicación; y
c) los resultados de la compatibilización de los proyectos e inversiones del desarrollo socioeconómico con los intereses de la defensa y la seguridad nacional.

2. El Órgano Especializado realiza de forma permanente la labor de asesoramiento en interés de alcanzar la calidad en la protección criptográfica, a través de los funcionarios encargados de los asuntos de la criptografía de las unidades organizativas que se encargan de la dirección de los sistemas de Seguridad y Protección en los órganos, organismos y entidades del Estado, las organizaciones políticas, sociales y de masas, y del sistema empresarial.

Artículo 25.1. Los prestadores de los servicios que se relacionan en el Artículo 21, numerales del 3 al 6, del presente Decreto-Ley, adoptan las medidas que garanticen el empleo de los criptodispositivos y otros medios conexos que ofertan, solo a los fines de protección para lo cual se designan.

2. Además, están obligados a establecer:

a) La segmentación de roles en sus funcionarios;
b) los sistemas de trazas;
c) las alertas de eventos anómalos y los planes de manejo de riesgos;
d) la conservación de los datos e información resultante de su actividad;
e) la capacitación de los beneficiaros de sus productos y servicios; y
f) la adopción de medidas de seguridad en el resguardo de copias de contraseñas y criptomateriales en los casos necesarios, según la categorización de los sistemas a proteger y las normas vigentes.

SECCIÓN CUARTA
Del Servicio Central de Cifras

Artículo 26. El Servicio Central de Cifras del Ministerio del Interior, se encarga de:

1. Garantizar la prestación de los servicios criptográficos de acuerdo con el Artículo 7, apartado 1, inciso a) del presente Decreto-Ley, que requieren la dirección de los órganos, organismos y entidades del Estado, las organizaciones políticas y de masas, y del sistema empresarial; así como para el intercambio de información cablegráfica y de otros formatos de estos con las sedes diplomáticas y representaciones cubanas en el exterior.
2. Actuar como centro coordinador y supervisor de las operaciones tecnológicas, técnicas y de seguridad para la aplicación de la criptografía; y como gestor de la producción de los criptomateriales necesarios en la protección de los sistemas es-

tablecidos en el Artículo 7, apartado 1, del presente Decreto-Ley y otros que se decidan por el Ministerio del Interior.

3. Funcionar como autoridad raíz de la Infraestructura Nacional de Llave Pública, dirigir técnicamente sus operaciones y organizar las formas de conectar la cadena de comprobación automática o no, por los propietarios de certificados digitales de llave pública, la confianza en los prestadores de servicios que los emiten, en correspondencia con los requisitos nacionales y las buenas prácticas internacionales.
4. Asegurar la cobertura de protección criptográfica que demanda el Sistema Seguro de Comunicaciones de la Dirección del país, en coordinación con los servicios que al respecto disponen los ministerios de Comunicaciones y de las Fuerzas Armadas Revolucionarias.

Artículo 27. El ministro del Interior, en coordinación con los titulares de los ministerios de Relaciones Exteriores, y del Comercio Exterior y la Inversión Extranjera, propone al Presidente de la República, a los efectos de su aprobación, la organización de las actividades, aseguramientos y medidas de seguridad del Servicio Central de Cifras en la protección del intercambio de información cablegráfica, con las representaciones estatales de Cuba en el exterior.

SECCIÓN QUINTA

De los servicios de la industria de medios criptográficos

Artículo 28.1. Los prestadores de servicios de la industria de medios criptográficos, en lo adelante prestador industrial criptográfico, especializan su actividad de acuerdo con lo que establece el Artículo 7 del presente Decreto-Ley.

2. Cuando las prioridades del desarrollo socioeconómico, la preparación para la defensa y la seguridad del país, requieren que un prestador industrial criptográfico, preste sus servicios en varias estructuras, es indispensable presentar al Órgano Especializado para su aprobación lo siguiente:

a) Esquemas y evidencias de segmentación de roles;
b) métodos criptográficos en la garantía de la preservación de los secretos tecnológicos de la protección de los sistemas críticos nacionales; y
c) documentos de niveles superiores que demandan estas acciones.

Artículo 29. La producción de criptomateriales de forma independiente para los criptodispositivos y servicios que lo requieran, se ejecuta con:

a) Sistemas y medios sin capacidad física de conexión a redes de comunicaciones;
b) la aplicación de altas medidas técnicas y organizativas de defensa contra irradiaciones eléctricas, electromagnéticas, acústicas, ópticas, termales e informáticas;
c) el empaquetamiento de los portadores para la entrega a los clientes;
d) controles de acceso a locales y para la guarda y custodia de almacenamiento, instrumentos y medios productivos y de trazas de eventos; y
e) programas para la modelación matemática de verificación de la calidad criptológica de los productos, de acuerdo con las normas vigentes.

Artículo 30. Los prestadores industriales criptográficos confeccionan expedientes sobre los procesos del servicio que brindan, los cuales se preservan y destruyen de acuerdo con los procedimientos que establece el reglamento del presente Decreto-Ley.

SECCIÓN SEXTA

De los servicios de operaciones y administración criptográfica

Artículo 31.1. Los servicios de operaciones y administración criptográfica son aquellos que se realizan fundamentalmente por prestadores de servicios de los propios entes

a proteger, con personal seleccionado por sus jefes, teniendo en cuenta la complejidad de los niveles de acceso y coordinación con la gestión documental, la informatización y ciberseguridad local que requieren los procesos de trabajo, el procesamiento y disponibilidad de la información y la actividad de protección criptográfica.

2. El servicio y el personal designado en el apartado anterior, se atiende metodológicamente por la estructura o cargo de Seguridad y Protección de la entidad y garantiza, en coordinación con los demás entes organizativos y técnicos implicados, la elaboración de las arquitecturas de protección criptográfica y planes de cobertura de estos servicios en su ámbito de responsabilidad.

Artículo 32. El jefe de una entidad puede contratar este servicio, o parte de él, a un prestador nacional externo autorizado, cuando las condiciones lo ameriten; además asegura que en el contrato se especifiquen los roles, responsabilidades y garantías en la confiabilidad de la protección a brindar, teniendo en cuenta lo dispuesto el Artículo 7 del presente Decreto-Ley.

SECCIÓN SÉPTIMA

De los servicios de la Infraestructura Nacional de Llave Pública, de Cadenas de Bloques y de Confianza Digital, basados en Certificados Digitales de Llave Pública y los de Firma Digital Criptográfica

Artículo 33. La Infraestructura Nacional de Llave Pública, es la plataforma técnica y organizativa que enlaza a los proveedores de servicios autorizados para:

a) El registro, emisión, validación, renovación y revocación de certificados digitales de llave pública que las personas naturales y jurídicas solicitan, poseen, utilizan o consultan como activo de identificación electrónica;
b) la creación y comprobación de firmas de objetos digitales; y
c) el cifrado de canales de comunicaciones.

Artículo 34.1. Los servicios de Cadena de Bloques, son las plataformas técnicas criptográficas que permiten a los usuarios participantes, alcanzar un consenso sobre la integridad de los datos que se someten a la protección de dicha cadena.

2. La cadena de bloques se conforma con prestadores de servicios independientes, los cuales construyen y firman criptográficamente eslabones de huellas digitales sobre la información que reciben de un prestador similar hasta llegar al final de la cadena.

3. Su seguridad radica en la participación de múltiples entes de servicio con actuación neutral respecto a sus vecinos.

Artículo 35. Los servicios de Confianza Digital basados en Certificados Digitales de Llave Pública, se ofertan en función de:

a) La custodia de mecanismos centralizados de creación de firmas digitales de ficheros;
b) la emisión de sellos electrónicos para persona jurídica;
c) el resguardo de documentos con protección;
d) los sistemas de sellado de tiempo de activos y hechos digitales para mostrar el valor probatorio de su existencia en el futuro;
e) la autenticación de sitios web; y
f) correos, entregas de objetos y mensajería corta certificada.

Artículo 36.1. El Certificado Digital de Llave Pública es el fichero electrónico sin duplicado, que se emite y entrega a los solicitantes o representantes de estos, por el sistema de prestación de servicios de la infraestructura, con período finito de validez que fija el emisor, según las normas técnicas establecidas.

2. Este permite corroborar ante terceros que una llave criptográfica pública es propiedad de una persona natural o jurídica, o de un medio técnico, proporcionando las garantías de

identificación y autenticación para efectuar operaciones criptográficas y servicios de confianza en el ciberespacio y las telecomunicaciones entre partes legítimas.

3. El propietario de la llave pública, dispone de otra bien conservada, que tiene carácter privado y se utiliza para descifrar transacciones y efectuar la firma criptográfica de ficheros digitales.

4. La conservación de los documentos electrónicos de valor histórico con la firma digital de sus autores, se realiza conforme a lo establecido en el Sistema de Gestión Documental y Archivos de la República de Cuba y se asegura que el Certificado Digital de Llave Pública correspondiente a las citadas firmas, disponga de la validez extendida durante el ciclo de vida de tales documentos, independientemente de que la persona natural o jurídica que lo haya firmado modifique su estatus como autoridad firmante, o si la persona natural ha fallecido.

Artículo 37. Las personas naturales y jurídicas, así como los prestadores de servicios que se relacionan en los artículos 33, 34 y 35 del presente Decreto-Ley, están obligados a utilizar los Certificados Digitales de Llave Pública, y criptodispositivos asociados, a los fines de la protección criptográfica para los cuales se emiten.

Artículo 38. El Órgano Especializado dicta las normas técnicas y procedimientos pertinentes para el funcionamiento, seguridad integral y plazos de vigencia de las operaciones de la prestación de servicios, enunciadas en los artículos 33, 34 y 35 del presente Decreto-Ley, así como el formato, clasificación, vigencia y manejo de los Certificados Digitales de Llave Pública, criptodispositivos y criptomateriales utilizados en estos.

Artículo 39. El empleo del certificado digital de Llave Pública y de los medios de creación de la firma digital, que se incluyan en el documento oficial de identidad del ciudadano en el país, están sujetos a las regulaciones específicas del sistema de Identidad Nacional, y a lo establecido en el presente Decreto-Ley.

Artículo 40. Cuando por intereses nacionales sea conveniente que el Certificado Digital de Llave Pública de un prestador de servicios criptográficos, se firme por un proveedor foráneo, que no radica en Cuba, se requiere la aprobación del ministro del Interior, previa consulta con los organismos de la Administración Central del Estado que correspondan.

Artículo 41. Los órganos, organismos y entidades del Estado, las organizaciones políticas, sociales y de masas, y del sistema empresarial que se relacionan con organismos y organizaciones multilaterales de la Organización de las Naciones Unidas, y otros organismos e instituciones internacionales de carácter regional o sectoriales que disponen de infraestructuras de llave pública para la interacción con sus afiliados, pueden suscribirse a esos servicios, lo cual se notifica por sus jefes al Órgano Especializado, quien brinda la asesoría y orientaciones pertinentes.

Artículo 42. A los efectos de esta norma jurídica, se identifica como firma digital criptográfica, al dato numérico que se adhiere a un fichero electrónico, obtenido mediante un procedimiento matemático que ejecuta una aplicación computacional específica que hace un resumen del contenido del fichero y lo cifra con la llave criptográfica privada y secreta del firmante, quedando con autenticación de autoría y marca de integridad del contenido ante destinatarios o terceros, quienes la comprueban mediante un procedimiento matemático similar que opera con la llave criptográfica pública contenida en el certificado digital del firmante.

Artículo 43. La firma digital criptográfica avanzada y reconocida, se expresa cuando se demuestra que la creación de la firma digital se realiza con una llave criptográfica pri-

vada, cuyo acceso siempre se encuentra bajo la custodia y posesión exclusiva del autor de la citada firma y lo vincula de manera única a la misma, y su llave criptográfica pública, para comprobar por terceros la validez de la firma, está contenida en un certificado digital de llave pública que emite un proveedor de servicios con autorización a los fines de operar en la Infraestructura.

SECCIÓN OCTAVA
De los servicios académicos

Artículo 44. Los servicios académicos se brindan por las instituciones de educación superior, centros científicos, industriales y de prestación de servicios, autorizados para realizar las actividades que se establecen en el Artículo 21, numeral 7, del presente Decreto-Ley, y tienen entre sus objetivos construir, producir, generalizar, actualizar y fortalecer la base de conocimientos y las capacidades humanas de la ciencia y la tecnología criptográfica cubana, en correspondencia con las necesidades del país.

Artículo 45. El Ministerio del Interior, en coordinación con los ministerios de Comunicaciones, de Ciencia, Tecnología y Medio Ambiente, de Educación, de Educación Superior, de las Fuerzas Armadas Revolucionarias, y de Industrias, según las prioridades de protección, las necesidades del desarrollo de los servicios, el incremento de la experticia, la competencia y renovación del capital humano en la esfera de la criptografía, emite los lineamientos y la cartera de temas en función de la materialización de los aspectos siguientes:

a) El establecimiento de proyectos nacionales o ramales de investigación científica e innovación tecnológica;
b) los planes de preparación, capacitación técnica y de actualización de los programas docentes; y
c) la obtención de grados y categorías científicas y pedagógicas de especialistas.

Artículo 46. El Ministerio del Interior, en coordinación con los organismos competentes y de acuerdo con la legislación vigente, dictamina sobre las propuestas de auspicio y realización en el país de eventos y lanzamiento de publicaciones científicas y tecnológicas en materia de la criptografía pública y universal, los objetivos a alcanzar e impacto en las prioridades del país, así como los temas a tratar y la participación de nacionales y extranjeros.

CAPÍTULO III
DE LA ORGANIZACIÓN Y FUNCIONAMIENTO DEL SISTEMA DE ASEGURAMIENTO INTEGRAL

SECCIÓN PRIMERA
Disposiciones generales

Artículo 47. El Sistema de Aseguramiento Integral se conforma por:

a) El Órgano Especializado, que asume la función de coordinador general;
b) los órganos colegiados, que son: el Grupo Técnico Asesor en Políticas Criptográficas y el Comité Técnico de Normalización de Criptografía;
c) las unidades organizativas que se encargan de la dirección de los sistemas de Seguridad y Protección en órganos, organismos y entidades del Estado, las organizaciones políticas y de masas, y del sistema empresarial;
d) los prestadores de servicio en la esfera de la criptografía, según los perfiles que establece el Artículo 21 del presente Decreto-Ley; y
e) los sujetos autorizados a importar, exportar y comercializar en el territorio nacional productos de la esfera de la criptografía.

Artículo 48. El Ministerio del Interior reglamenta el funcionamiento del Sistema de Aseguramiento Integral, y planifica las actividades de los órganos colegiados relacionados en el artículo anterior.

Artículo 49. El Grupo Técnico Asesor en Políticas Criptográficas, es el encargado de colegiar las propuestas de directrices técnicas a someter a la aprobación de las autoridades competentes para el diseño de criptodispositivos y su aplicación en el país; está integrado por representantes de los ministerios de las Fuerzas Armadas Revolucionarias, de Comunicaciones, del Interior, de Ciencia, Tecnología y Medio Ambiente, así como de Industrias.

Artículo 50.1. El Comité Técnico de Normalización de criptografía, realiza el análisis multilateral de los proyectos de Normas Técnicas Cubanas a poner en vigor de acuerdo con el Artículo 7, apartado 1, incisos b) y e) del presente Decreto-Ley, así como sus planes de implementación; está integrado por representantes de los ministerios del Interior, de Comunicaciones, de Justicia, de las Fuerzas Armadas Revolucionarias, de Ciencia, Tecnología y Medio Ambiente, de Industrias, de Finanzas y Precios, de Comercio Interior, del Comercio Exterior y la Inversión Extranjera, de Educación Superior, y de las oficinas nacionales de Estadística e Información, y de Normalización.

2. Incluye, además, una Sección Consultiva de Ciencia e Innovación Tecnológica de criptografía, que agrupa expertos con categoría científica y docente de las universidades, centros científicos y de la industria.

3. El Ministerio del Interior, en coordinación con los integrantes del Comité Técnico de Normalización de criptografía, determina la cantidad y los participantes en las diferentes sesiones consultivas, según los temas a discutir.

Artículo 51.1. Las dependencias que se encargan de la dirección de los sistemas de Seguridad y Protección, gestionan el completamiento de la protección criptográfica que requiere la organización a la que pertenecen para la gestión informativa interna y en virtud de su interrelación con el Estado y la sociedad, controlan su implementación y reciben el asesoramiento y la asistencia en capacitación por parte del Órgano Especializado.

2. Cuando no exista en una organización, estructura de Seguridad y Protección, el directivo general que atiende la actividad, asume las responsabilidades establecidas en el apartado anterior ante las autoridades competentes, apoyándose en los entes organizativos de las Telecomunicaciones/TIC de dicha organización.

SECCIÓN SEGUNDA
Sobre la Información Estadística-Analítica, de Alerta Temprana sobre amenazas y vulnerabilidades, y las publicaciones en el ámbito de la criptografía

Artículo 52. A los efectos del Servicio Criptográfico, la efectividad en la calidad de dichos servicios se evalúa a partir de:

a) El nivel de completamiento de la protección criptográfica que se planifica y aprueba poner en explotación en todos los sectores del país, su disposición operacional y empleo real que comprueba el Ministerio del Interior mediante los controles estatales que se establecen al efecto;
b) el nivel de seguridad y confianza técnica y estatal que se alcanza para los bienes bajo salvaguarda criptográfica, los incidentes de seguridad ocurridos en la protección criptográfica, sus causas, medidas de mitigación que se adoptan y sanciones a los incumplidores;

c) las capacidades existentes de prestadores de servicios criptográficos, el nivel de independencia y soberanía existente en los conocimientos, tecnologías, técnicas y criptodispositivos;
d) la idoneidad demostrada de los recursos humanos que se desempeñan en el sistema de aseguramiento integral; y
e) la contribución de la criptografía a la satisfacción de las prioridades del desarrollo socioeconómico, la preparación para la defensa y seguridad del país.

Artículo 53. El ministro del Interior presenta al Presidente de la República o al Primer Ministro, en los plazos que se le indique, según sea el caso, la información estadística analítica necesaria para la evaluación del comportamiento y efectividad de la actividad general en el ámbito de la criptografía, a partir de lo dispuesto en el artículo anterior, y otras particularidades que resulten pertinentes incluir.

Artículo 54. El Órgano Especializado emite:

a) Los requerimientos informativos a rendir en el Sistema Integral de Aseguramiento, así como los boletines de Alerta Temprana, ante amenazas y vulnerabilidades que pongan en peligro la protección criptográfica empleada, los bienes que se protegen o los proyectos de desarrollo y producción de nuevos criptodispositivos;
b) la lista de criptodispositivos, y de prestadores de servicios en la esfera de la criptografía autorizados para operar en el país, según la categorización de los sistemas a proteger y la clasificación de la tecnología y los medios criptográficos; y
c) la lista de criptodispositivos, y de prestadores de servicios en la esfera de la criptografía que se destinan a fondos exportables.

Artículo 55. El Ministerio del Interior establece las características de cada fase informativa y las especificaciones de las medidas a adoptar, según el caso.

SECCIÓN TERCERA

De la Metrología, Acreditación y Certificación en la esfera de la criptografía

Artículo 56.1. La actividad de Metrología, Acreditación y Certificación en el ámbito de la criptografía, se dirige por el Órgano Especializado y se desarrolla mediante la constitución de una red de laboratorios de pruebas evaluativas y tribunales de expertos, que se acredita por la Oficina Nacional de Normalización perteneciente Ministerio de Ciencia, Tecnología y Medio Ambiente.

2. Esta actividad forma parte del Sistema Nacional de Metrología encargado de evaluar, medir, acreditar y certificar cíclicamente la calidad del desarrollo, producción, aplicación y empleo de los criptodispositivos, medios colaterales y de los servicios en interés de la protección criptográfica.

3. La evaluación de la calidad y seguridad de los medios y servicios de protección criptográfica que corresponden al Artículo 7, apartado 1, inciso a) del presente Decreto-Ley, se realiza por laboratorios especializados de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, según corresponda.

Artículo 57. El Órgano Especializado establece:

a) Las guías, procedimientos, modelos teóricos y prácticos, y los tipos de medios e instrumentos a utilizar;
b) los documentos declaratorios de práctica de certificación;
c) los requisitos profesionales de los especialistas para el ejercicio de la evaluación en la red de laboratorios de pruebas;
d) el funcionamiento de los tribunales de expertos; y
e) los procesos de acreditación y certificación de la calidad.

Artículo 58.1. Los criptodispositivos, sean estos de fabricación nacional o importados, requieren disponer del documento y marca de certificación emitidos por el Órgano Especializado, y son accesibles a las autoridades competentes y a los beneficiarios, para poder funcionar en las prestaciones de protección en el país y en sus representaciones en el exterior.

2. Los criptodispositivos cubanos para su exportación, están obligados a cumplir los requisitos establecidos en el apartado anterior.

CAPÍTULO IV
DE LAS RELACIONES INTERNACIONALES EN LA ESFERA DE LA CRIPTOGRAFÍA

Artículo 59.1. Los organismos de la Administración Central del Estado, responsabilizados con la representación del Estado cubano ante las organizaciones y organismos internacionales, concilian con el Ministerio del Interior los argumentos a exponer en esos escenarios a nombre del país, en todo lo relativo con la criptografía, sus tecnologías y servicios de protección.

2. Son previamente colegiados y aprobados por el Ministerio del Interior, los intereses puntuales e informaciones que, en materia de criptografía, pretendan presentar ante las organizaciones y organismos internacionales, los órganos y organismos de la Administración Central del Estado.

Artículo 60.1. Corresponde al Ministerio del Interior establecer en el ámbito de la criptografía, las relaciones de cooperación internacional con sujetos homólogos de otros Estados.

2. Las empresas y prestadores cubanos de servicios criptográficos, para establecer relaciones de cooperación internacional en el ámbito de la criptografía, requieren del dictamen previo del Ministerio del Interior.

3. Las obligaciones derivadas de tratados internacionales en vigor para la República de Cuba en materia de criptografía, forman parte o se integran, según corresponda, al ordenamiento jurídico nacional, de acuerdo con lo establecido en la Constitución de la República de Cuba.

DISPOSICIÓN ESPECIAL

ÚNICA: El Ministerio del Interior, coordina con la Oficina Nacional de Estadística e Información, las informaciones específicas de la criptografía que requiere el Sistema de Información del Gobierno.

DISPOSICIONES FINALES

PRIMERA: El Consejo de Ministros, a propuesta del Ministerio del Interior, en un plazo de noventa días posteriores a la publicación del presente Decreto-Ley en la Gaceta Oficial de la República, dicta el Decreto que lo reglamenta.

SEGUNDA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior, para adecuar, en lo que resulte necesario, las disposiciones establecidas en este Decreto-Ley a las particularidades de las funciones, misiones y características de dichos organismos.

TERCERA: Los ministros del Interior, de Finanzas y Precios y de Ciencia, Tecnología y Medio Ambiente, dictan en un plazo de noventa días, contados a partir de la fecha de publicación del presente Decreto-Ley, las disposiciones complementarias que aseguren el cumplimiento de lo establecido en esta norma.

CUARTA: A las personas naturales y jurídicas que incurran en infracciones en materia de criptografía, se les aplica el régimen contravencional regulado en el Decreto complementario al presente Decreto-Ley.

QUINTA: El presente Decreto-Ley entra en vigor a los noventa días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en La Habana, a los 26 días del mes de octubre de 2023.

Juan Esteban Lazo Hernández

CONSEJO DE MINISTROS

GOC-2024-528-O89

MANUEL MARRERO CRUZ, Primer Ministro.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley 79 "Sobre el desarrollo, la aplicación y uso de los dispositivos de protección criptográfica y servicios en la esfera de la criptografía en la República de Cuba", de 26 de octubre de 2023, en su Disposición Final Primera establece que el Consejo de Ministros, a propuesta del Ministerio del Interior, dicta el Decreto que lo reglamenta.

POR CUANTO: Resulta necesaria la instrumentación y aplicación de acciones en función del desarrollo, aplicación y uso de los dispositivos de protección criptográfica y los servicios en la esfera de la criptografía en la República de Cuba, que obstaculicen e impidan el acceso a los datos, informaciones, infraestructuras y procesos críticos por personas no autorizadas, atemperadas con la actual y perspectiva evolución política, socioeconómica y tecnológica del país; modernizándolos, simplificándolos y poniéndolos a tono con la práctica internacionalmente reconocida en esta materia, así como establecer las contravenciones en la materia; la cuantía de las multas y demás sanciones a imponer por su comisión, las autoridades facultadas para imponerlas y resolver los recursos que contra estas se interpongan por los afectados, en correspondencia con la legislación vigente.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o), de la Constitución de la República de Cuba, dicta el siguiente:

DECRETO 106
REGLAMENTO DEL DECRETO-LEY 79 "SOBRE EL DESARROLLO, LA APLICACIÓN Y USO DE LOS DISPOSITIVOS DE PROTECCIÓN CRIPTOGRÁFICA Y SERVICIOS EN LA ESFERA DE LA CRIPTOGRAFÍA EN LA REPÚBLICA DE CUBA", DE 26 DE OCTUBRE DE 2023

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Este Reglamento tiene por objeto poner en vigor los procedimientos y especificaciones generales para la aplicación de lo dispuesto en el Decreto-Ley 79 "Sobre el desarrollo, la aplicación y uso de los dispositivos de protección criptográfica y servicios en la esfera de la criptografía en la República de Cuba", de 26 de octubre de 2023, en lo adelante Decreto-Ley, en lo referente a:

1. Implementar la protección criptográfica que demandan los diferentes sistemas de información, bases de datos, controles automáticos, las Telecomunicaciones, Tecnologías de la Información y la Comunicación, en lo adelante Telecomunicaciones/ TIC, y los servicios postales del país.
2. La calidad técnica y de seguridad criptológica y operacional del diseño, producción, suministro, instalación, mantenimiento, explotación y renovación periódica de los criptodispositivos, servicios de protección criptográficos y de otros productos que proporciona el Sistema de Aseguramiento Integral.
3. El funcionamiento de los servicios criptográficos, y del Sistema de Aseguramiento Integral que establece la legislación al respecto.
4. Establecer las contravenciones en materia del desarrollo, aplicación y uso de los dispositivos de protección criptográfica y los servicios en la esfera de la criptografía; la cuantía de las multas y demás sanciones a imponer por su comisión, así como las autoridades facultadas para imponerlas y resolver los recursos que contra estas se interpongan por los afectados.

Artículo 2. Están sujetos al cumplimiento de lo establecido en el presente Reglamento:

1. Las personas naturales y jurídicas en el territorio nacional y en las representaciones de Cuba en el exterior.
2. Los prestadores de servicios criptográficos en Cuba que radican en el exterior.
3. Las personas naturales y jurídicas extranjeras, en el marco de las relaciones internacionales con Cuba, que se establezcan por medio de convenios o contratos.

Artículo 3. La Dirección de Criptografía del Ministerio del Interior, en lo adelante Dirección de Criptografía, es el órgano especializado que se encarga, junto con las dependencias territoriales de esta especialidad en las jefaturas provinciales y del municipio especial Isla de la Juventud de ese organismo, de:

1. La conducción de los procesos y la ejecución de las actividades que aseguran la disponibilidad, el orden y la seguridad de la protección criptográfica y los servicios que al respecto demanda el país.
2. El cumplimiento de lo que se establece en el presente Reglamento y de la interrelación de esta rama con la Infraestructura Nacional de Calidad, según la legislación vigente.

Artículo 4. Se entiende por adversario, a todo ente organizativo o persona natural, nacional o extranjero que, con recursos técnicos, métodos de ataques y ubicación territorial, intente socavar, vulnerar, burlar y debilitar la protección criptográfica que se establece para la salvaguarda de documentos, datos, y los sistemas críticos con el propósito de acceder sin autorización legal a ellos y causar daños cualquiera sea su finalidad y magnitud.

Artículo 5. La seguridad criptológica y operacional se cataloga como el estado de confianza que depositan las personas naturales y jurídicas en la protección criptográfica que utilizan, a partir del conjunto de medidas científicas, técnicas, organizativas, procedimentales, de control integral y custodia física que se adoptan en el ciclo de vida de los criptodispositivos, y los servicios de protección criptográfica, en virtud de prevenir y contrarrestar las amenazas y riesgos de probables ataques de adversarios, a partir de las acciones siguientes:

1. Estudio de debilidades y vulnerabilidades en el orden matemático criptográfico, en lo adelante, criptoanálisis de los criptodispositivos, módulos criptográficos y sobre las operaciones de control, custodia y empleo del servicio de protección.
2. Obtención o deducción de datos no públicos sobre la arquitectura, tecnologías e ingeniería de los criptodispositivos, módulos criptográficos y procesos sensibles de la prestación de los servicios.

3. Estudio de la capacidad de los posibles adversarios para la obtención de datos criptográficos sensibles que puedan fugarse de los criptodispositivos y módulos criptográficos durante su funcionamiento, a través de canales técnicos colaterales de índole acústica, mecánica, eléctrica, electromagnética, óptica, informática, térmica y electrónica.

Artículo 6. La protección criptográfica se aplica para cumplir los requisitos de seguridad que establecen las autoridades competentes y las normas del país, en materia de gestión informativa, manejo de datos y de la correspondencia, en cualquier formato, ámbito y tipo de tecnología, con el objetivo de garantizar:

1. La confidencialidad e integridad de las informaciones y datos que procesan, almacenan y transmiten hacia los destinos legítimos las personas naturales, y de aquellos que producen los medios técnicos para su archivado y conservación; telemetría, control automático, canales y pasarelas de pago, así como para establecer las rutas de las telecomunicaciones entre pares y multipuntos.
2. La autenticación de autores de ficheros electrónicos, y el control de acceso y autorización a personas, programas informáticos u objetos de automatización para la ejecución de operaciones técnicas en los sistemas de información e infraestructuras, plataformas, servicios y aplicaciones de Telecomunicaciones/TIC, procesos automáticos y de telemetría.
3. La facilitación de la identidad electrónica de las personas naturales, jurídicas y de objetos en el ciberespacio y la transformación digital de la sociedad.
4. El no repudio por las partes participantes en las transacciones hechas a través de las Telecomunicaciones/TIC.

Artículo 7. Las especificaciones técnicas y de seguridad criptológica y operacional de la protección criptográfica de la información, se establecen teniendo en cuenta el plazo que se exige para su implementación y los entornos de la gestión informativa a salvaguardar siguientes:

1. Procesamiento criptográfico de la información con criptodispositivos aislados y sin conexión a redes de telecomunicaciones.
2. Procesamiento criptográfico de la información con criptodispositivos ubicados en redes de Telecomunicaciones/TIC sin conexión a sistemas públicos nacionales e internacionales.
3. Procesamiento criptográfico de la información con criptodispositivos ubicados en redes de Telecomunicaciones/TIC con conexión a sistemas públicos nacionales e internacionales.

CAPÍTULO II
DE LOS CRIPTODISPOSITIVOS, LOS SERVICIOS CRIPTOGRÁFICOS Y OTROS PRODUCTOS QUE PROPORCIONA EL SISTEMA DE ASEGURAMIENTO INTEGRAL

SECCIÓN PRIMERA
De la composición y la calidad

Artículo 8. Los criptodispositivos se conforman como un componente integrado o en módulos independientes interconectados, que ejecutan:

1. Las operaciones matemáticas que se implementan a través de artículos manuscritos, mecánicos, electrónicos o informáticos, en lo adelante algoritmos criptográficos, para el cifre y descifre de datos; la generación, conservación y destrucción de criptomateriales; y el intercambio protegido de llaves criptográficas empleadas en el

establecimiento de comunicaciones cifradas de acuerdo con los protocolos que se fijan al respecto.

2. Las técnicas de blindaje y neutralización que se adicionan para defender al citado criptodispositivo de ataques adversarios por canales técnicos colaterales no criptográficos.

Artículo 9. El ciclo de vida de los criptodispositivos, la protección criptográfica que se implanta y de otros productos que proporciona el Sistema de Aseguramiento Integral que demanda el país, se integra por las fases siguientes:

1. La elaboración de los proyectos que definen los objetivos, arquitectura, especificaciones organizativas, científicas, didácticas y técnicas de los criptodispositivos, los servicios criptográficos y demás productos que proporciona el Sistema de Aseguramiento Integral para satisfacer la demanda general o particular que se identifica en materia de criptografía.
2. El proceso de adquisición de los algoritmos criptográficos y las tecnologías y técnicas para su implementación práctica.
3. El diseño de los criptodispositivos y otros productos de la esfera de la criptografía, su fabricación a partir de las capacidades del Sistema de Aseguramiento Integral; o la asimilación total, parcial o bajo innovación de códigos libres o abiertos; la transferencia de tecnologías y técnicas según acuerdos entre personas jurídicas con acreditación, la importación en diferentes variantes comerciales de productos de estos tipos, o las soluciones híbridas.
4. La ejecución de pruebas de campo y ensayos para verificar la calidad de los criptodispositivos y de otros productos de la esfera de la criptografía, así como de la capacitación de los potenciales usuarios y del personal para la asistencia técnica pos suministro.
5. La ejecución de la cadena de suministro de los citados medios desde la fábrica o lugar de importación, hasta los destinos finales de empleo.
6. La instalación masiva y puesta en marcha de los criptodispositivos y otros productos de la esfera de la criptografía, en los destinos finales de empleo para la conformación de la protección criptográfica, los laboratorios de evaluación de la calidad, centros docentes y de entrenamientos, y demás aplicaciones que correspondan.
7. El empleo de los bienes que se señalan en el inciso anterior.
8. La administración y el mantenimiento técnico de la protección criptográfica que se implanta, los medios de evaluación de la calidad, los que se utilizan en centros docentes y demás aplicaciones específicas.
9. La actualización, renovación o desactivación de los criptodispositivos, protección criptográfica en explotación y de otros productos de la esfera de la criptografía, de acuerdo a los cambios científicos, tecnológicos, procedimentales y de operaciones que se producen frente a nuevos requisitos de funcionabilidad o riesgos de seguridad que potencial o realmente se descubren y puedan introducirse.

Artículo 10.1. Antes de aprobarse el suministro y uso de cualquier criptodispositivo en las actividades que ofrecen servicios legales a personas naturales y jurídicas del país o externas, este se somete a examen evaluativo de los laboratorios de la infraestructura nacional de calidad especializada en materia de criptografía, en lo adelante Infraestructura de Calidad Criptográfica.

2. Dicho examen evaluativo se realiza, además, en cada fase de su ciclo de vida, de acuerdo con los protocolos que establece la Dirección de Criptografía.

Artículo 11. En virtud de certificar la garantía de seguridad criptológica y operacional que ofrecen los criptodispositivos y módulos criptográficos, frente a las capacidades de ataques que se conocen, se establecen para los criptodispositivos los niveles de seguridad siguientes:

1. Nivel de Seguridad número 1: El criptodispositivo ejecuta las funciones de protección que se documentan por el suministrador y su diseño es efectivo para contrarrestar el éxito de ataques a los textos cifrados y a los módulos que lo componen, por adversarios que disponen de poco tiempo de acción, y emplean herramientas disponibles pública y libremente, que requieren de bajos conocimientos técnicos en su aplicación.
2. Nivel de Seguridad número 2: El criptodispositivo ejecuta las funciones de protección que se documenta por el suministrador y su diseño es efectivo para contrarrestar el éxito de ataques de duración media sobre los textos cifrados y a los módulos que lo componen, por adversarios que disponen de un tiempo mediano de acción, y que emplean, además de las herramientas que se indican en el Nivel de Seguridad número 1, de otras comerciales, que requieren de conocimientos técnicos medios en su aplicación.
3. Nivel de Seguridad número 3: El criptodispositivo ejecuta las funciones de protección que se documenta por el suministrador y su diseño es efectivo para contrarrestar el éxito de ataques de duración considerable sobre los textos cifrados, los procesos de cifre y descifre, y los módulos que lo componen, por adversarios que disponen de un tiempo apreciable de acción, y que emplean, además de las herramientas que se indican en el Nivel de Seguridad número 2, otras comerciales o de laboratorios especializados, que requieren de elevados conocimientos técnicos y de ingeniería en su aplicación.
4. Nivel de Seguridad número 4: El criptodispositivo ejecuta las funciones de protección que se documenta por el suministrador y su diseño es efectivo para contrarrestar el éxito de ataques sofisticados de larga duración sobre los textos cifrados, los procesos de cifre y descifre, y a los módulos que lo componen, por organizaciones adversarias calificadas y dedicadas a estas actividades que disponen de tiempo permanente, y emplean, además de las herramientas que se indican en el Nivel de Seguridad número 3, otras muy especializadas, que requieren altos conocimientos técnicos y de ingeniería en su aplicación.

Artículo 12.1. El dictamen que se emite para la aprobación de la puesta en marcha de un servicio de protección criptográfica, se basa en:

a) El nivel de seguridad que ofrecen las certificaciones de los criptodispositivos a emplear;
b) la calidad del personal que se acredita para operar y ejecutar su asistencia técnica en la explotación; y
c) el conjunto de medidas adicionales tecnológicas, procedimentales para el manejo, control, medición del funcionamiento y guarda y custodia de los citados medios, que se implantan en los locales y entornos de operaciones de los mismos, de acuerdo con la categorización de la seguridad del objetivo a proteger.

2. A los efectos de la emisión del dictamen para la aprobación de la puesta en marcha de un servicio de protección criptográfica, el propietario o titular del objetivo a proteger está en la obligación de presentar, a la autoridad emisora, la declaración jurada sobre la categorización de la seguridad de dicho objetivo.

3. La calidad de los criptodispositivos y los servicios asociados a la salvaguarda de la información clasificada y limitada, así como de los datos que producen las operaciones técnicas de los medios, aplicaciones, redes, servicios e infraestructuras de Telecomunicaciones/TIC y procesos automáticos de los sistemas críticos para la vitalidad, defensa y seguridad nacional, se evalúa anualmente, además de la monitorización permanente del comportamiento de los criptodispositivos y los servicios asociados, de acuerdo con los procedimientos básicos siguientes:

a) El examen por la Dirección de Criptografía sobre la actualización de los conocimientos y habilidades en materia criptológica de los especialistas de los prestadores de servicios que atienden dichos sistemas;
b) la comprobación por los laboratorios de evaluación de la fortaleza de los datos y accesos criptográficamente protegidos, que pueden ser visualizados por los atacantes previstos en tales sistemas; y
c) la comprobación de la actualización y conformidad de la declaración jurada de los directivos de los prestadores de servicios criptográficos, sobre las medidas técnicas y organizativas implantadas en el ámbito interno de la protección.

Artículo 13. La soberanía en la administración del ciclo de vida de los criptomateriales consiste en:

1. La capacidad de los proveedores de servicios de protección criptográfica para organizar e implementar la generación, traslado, empleo, conservación, mejoramiento de los parámetros de seguridad, desactivación y destrucción de las llaves criptográficas que garantizan la ejecución del cifrado y descifrado de datos, sin la solicitud de licencias o permisos a suministradores extranjeros.
2. El dominio por los prestadores de servicios de protección criptográfica y las autoridades competentes, de la tecnología y métodos de comprobación medibles de la calidad y seguridad criptológica y operacional del ciclo de vida de los criptomateriales, cuyos resultados se registran en expedientes al efecto, con las medidas de preservación, custodia y control pertinentes.

Artículo 14. La Dirección de Criptografía, con vistas a garantizar la efectividad del cumplimiento de las normas de protección criptográfica, establece las coordinaciones y el intercambio de información con:

1. Las autoridades competentes del Ministerio de Comunicaciones sobre los procesos legales de autorización de operación de redes de Telecomunicaciones/TIC con la incorporación de criptodispositivos para el cifrado de canales de transmisión, y en virtud de la interacción de la industria del software con los servicios criptográficos para la producción de medios informáticos con la inclusión de criptodispositivos.
2. Las autoridades competentes del Ministerio de Industrias en función de la interacción de la industria electrónica con los servicios criptográficos para la producción de medios electrónicos con la inclusión de criptodispositivos.
3. Las autoridades del Ministerio de Finanzas y Precios para aportar los elementos técnicos, funcionales y de calidad que se requieren por el citado ministerio en función de establecer los precios y tarifas de los criptodispositivos y de los servicios criptográficos.

SECCIÓN SEGUNDA
De los documentos normativos

Artículo 15. Todos los procesos y planes para la obtención, puesta en funcionamiento y operación de criptodispositivos y sobre la ejecución de las actividades en los servicios

criptográficos, se rigen por documentos normativos de diferentes categorías, los que se elaboran y ponen en vigor en consonancia con los procedimientos de la Infraestructura Nacional de Calidad y las particularidades que al respecto establece el Ministerio del Interior, con la finalidad de:

1. La seguridad, competencia y despliegue oportuno de la protección que se implementa y los servicios que se ofrecen.
2. La disciplina tecnológica y operacional al respecto.
3. Evitar obstáculos innecesarios a los servicios primarios que se prestan en los ámbitos protegidos y en las cadenas de suministros de los criptodispositivos.

Artículo 16. Se rigen por documentos normativos de carácter obligatorio, los criptodispositivos y los servicios asociados que aseguran la protección en:

1. La gestión de la información clasificada y limitada de la administración operacional de los sistemas técnicos que se utilizan al efecto.
2. El intercambio automático de datos que producen en sus operaciones los equipos, aplicaciones, redes, servicios e infraestructuras técnicas que aseguran el funcionamiento de los sistemas críticos para la vitalidad y seguridad nacional, así como en el control de acceso a su administración por los operarios.
3. Los canales y pasarelas electrónicas de pago.
4. Los casos en que los criptodispositivos y sus servicios constituyen una condición primaria y necesaria para garantizar la debida protección.
5. Los sistemas para el cumplimiento de los derechos legales de las personas naturales y jurídicas en las transacciones y correspondencias electrónicas.
6. Las plataformas de información pública a ofrecer hacia los ámbitos nacional e internacional, a cargo de las autoridades estatales, administrativas y de gobierno.
7. Los productos de las Telecomunicaciones/TIC que se ofertan al público en las redes del comercio interior.

Artículo 17. La Dirección de Criptografía, en coordinación con la Oficina Nacional de Normalización y otras autoridades afines que se requieran:

1. Emite las instrucciones para la elaboración y empleo de las diferentes categorías de documentos normativos de acuerdo con los procedimientos de la Infraestructura Nacional de Calidad.
2. Organiza, convoca y dirige los eventos y procesos con directivos, expertos y especialistas del Sistema de Aseguramiento Integral para definir las necesidades de elaboración de nuevos documentos normativos y la actualización de los vigentes.
3. Establece la clasificación de confidencialidad y formas pertinentes de diseminación de los documentos normativos, especificaciones técnicas y de buenas prácticas, necesarios y suficientes para:
   a) La instalación, operación, mantenimiento, control o reparación de los criptodispositivos; y
   b) la exportación de estos tipos de productos y servicios, según su impacto en la seguridad de las personas, el Estado, la propiedad intelectual, y del propio resguardo de la protección criptográfica.
4. Propone la elaboración o revisión de las normas cubanas en materia de criptografía para su integración al Programa Nacional de Normalización, de acuerdo con los plazos fijados al efecto por la citada Oficina Nacional.
5. Orienta a los órganos, organismos, entidades del Estado, al sistema empresarial y a las organizaciones políticas, sociales y de masas, respecto a la equiparación de las normas cubanas con las que emiten las organizaciones internacionales, a los efectos

de establecer en convenios y contratos con entes extranjeros, los intercambios protegidos a través de las Telecomunicaciones/TIC globales.

6. Diseña e implementa, según las necesidades del país, las acciones de superación técnica y profesional en materia de normalización y calidad en la esfera de la criptografía.

Artículo 18. Los servicios criptográficos y otros que utilicen la protección criptográfica como parte de la garantía de las prestaciones que ofrecen, están en la obligación de refrendar en los contratos o documentación equivalente, los requerimientos normativos que se establecen para la citada protección y actividades relacionadas, así como las obligaciones de cada parte para garantizar la seguridad criptológica y operacional de las mismas.

SECCIÓN TERCERA
Del Control, la Metrología, Acreditación y Certificación de la conformidad de la Calidad en la esfera de la Criptografía

Artículo 19.1. Los procesos que desarrolla la Infraestructura de Calidad Criptográfica establecen un nivel de confianza para los criptodispositivos y servicios de protección asociados, atendiendo al grado en que satisfacen la funcionalidad de seguridad que se espera de ellos y los resultados de las pruebas evaluativas que les aplican sobre la conformidad con las normas al efecto.

2. La citada Infraestructura, se dirige por la Dirección de Criptografía y funciona bajo el principio de la integración y correlación con el sistema de control a la seguridad y protección de objetivos y la Infraestructura Nacional de Calidad.

Artículo 20. La Dirección de Criptografía en función del Control, la Metrología, Acreditación y Certificación de la Conformidad de la Calidad en la esfera de la criptografía:

1. Mantiene el intercambio informativo y la coordinación necesaria con la Oficina Nacional de Normalización, para asegurar el cumplimiento de la legislación vigente en materia de la calidad de las producciones y los servicios criptográficos a emplear en Cuba y los que se prestan en el marco de las relaciones internacionales del país.
2. Aprueba la puesta en funcionamiento de los laboratorios de evaluación de la calidad de los criptodispositivos, que incluye:
   a) La preparación y acreditación del personal especializado que los conforman;
   b) la ejecución del proceso de consulta, previo a la aprobación, con las autoridades competentes que se requieran sobre la reputación de los citados laboratorios; y
   c) la coordinación de sus planes de evaluación.
3. Certifica y actualiza en los plazos que establece la Infraestructura Nacional de Calidad y de acuerdo con la evolución de las tecnologías criptográficas y de los riesgos de seguridad criptológica:
   a) Las guías, procedimientos, modelos teóricos y prácticos;
   b) las métricas, los instrumentos y herramientas de medición a emplear, para la realización de las pruebas de la conformidad; y
   c) los conocimientos del personal especialista de los laboratorios.
4. Actualiza y compatibiliza con las directrices de la Oficina Nacional de Normalización, los documentos declaratorios de prácticas de certificación de la red de laboratorios de evaluación de la calidad de los servicios criptográficos.
5. Conduce el proceso y aprueba la composición de los tribunales de expertos, y organiza la preparación y actualización de los conocimientos de sus integrantes.

6. Comprueba que los suministradores de criptodispositivos con aprobación, muestren en sus catálogos las características principales y la información sobre el nivel de seguridad vigente que certifica al respecto la Infraestructura de Calidad Criptográfica, que requieren los consumidores para la confianza en su explotación nacional o para la exportación de productos y servicios.
7. Organiza y pone en práctica, en coordinación con la Oficina Nacional de Normalización, los ministerios de Educación y Educación Superior, así como con el Sistema de Aseguramiento Integral y otras autoridades que se requieran, el programa de preparación, capacitación y actualización de conocimientos de los especialistas de criptografía, como condición necesaria para el ejercicio de las actividades de los servicios criptográficos, y de las funciones en la Infraestructura de Calidad Criptográfica.
8. Emite el acta de acreditación de las personas naturales que se especializan en las tecnologías y la aplicación de técnicas criptográficas, para ejecutar las tareas específicas en la prestación de los servicios criptográficos, una vez concluido el proceso de preparación y capacitación, examen de conocimientos y dictamen de los tribunales de expertos.
9. Ejecuta las acciones que le corresponden como centro de observación metrológica y de pronóstico nacional y conduce la participación de los actores del Sistema de Aseguramiento Integral para:
   a) La prevención de amenazas a la calidad de la protección criptográfica; y
   b) las nuevas aplicaciones de la criptografía en aras de mitigar riesgos de ataques a los sistemas de información y a los medios técnicos que garantizan su gestión, mediante la realización de ensayos, prospección científica y tecnológica, a partir del análisis de información procedente de fuentes informativas públicas con crédito.
10. Emite los boletines informativos de alerta temprana sobre las amenazas y sus mitigaciones, así como recibe y atiende los reportes y quejas sobre incidentes de seguridad y anomalías en la protección criptográfica en explotación.
11. Propone al Ministro del Interior, las políticas y planes de aseguramiento, relativos a la interrelación de los laboratorios de evaluación con homólogos extranjeros, de acuerdo con los requerimientos del comercio exterior, el desarrollo de las exportaciones y las relaciones internacionales de Cuba, y coordina su implementación en los casos que se aprueben.
12. Controla y verifica la conformidad del cumplimiento de las normas de instalación, administración, disponibilidad, seguridad y operación de los servicios de protección criptográfica, para lo que utiliza los procederes de comprobación con herramientas técnicas y los métodos administrativos correspondientes, en los eventos de control estatal a la seguridad y protección de objetivos y en la inspección estatal especializada.

Artículo 21.1. Los laboratorios de evaluación de la calidad, en base a los métodos, instrumentos y herramientas de medición que disponen con acreditación de la Dirección de Criptografía, realizan las pruebas y califican los niveles de seguridad que alcanzan los criptodispositivos bajo examen en los aspectos siguientes:

a) Los módulos criptográficos que lo conforman;
b) las interfaces o enlaces entre los módulos criptográficos y con otros componentes con los que tienen que interconectarse;
c) los roles, servicios y autenticaciones que incorpora el criptodispositivo para sus operaciones, tanto para el funcionamiento de sus módulos o la interacción de estos

con otros componentes técnicos no criptográficos, sea por accionamiento de operadores humanos o automáticos;

d) las medidas de integridad que se aplican para garantizar la seguridad de la interacción entre los módulos criptográficos con el firmware, los softwares básicos y el hardware donde operan;

e) el ambiente operacional en que funcionan los parámetros criptográficos que pueden comprometer la confiabilidad del criptodispositivo y sus módulos;

f) las medidas de seguridad física, que incluye las acciones de protección en la fase productiva, el empaquetamiento del producto terminado, y las técnicas de detección y defensa frente a ataques invasivos de apertura del equipamiento que conforma al criptodispositivo, así como para contrarrestar la inyección intencional de fallas;

g) las medidas de seguridad frente al criptoanálisis;

h) la administración de los parámetros de seguridad del funcionamiento del criptodispositivo y sus módulos;

i) la implementación de autocontroles de seguridad que realiza automáticamente el criptodispositivo;

j) las medidas de aseguramiento del ciclo de vida del producto, que incluye la administración de sus configuraciones, los modos de distribución para el suministro, la operatoria y guías de la administración operacional y del manejo por los usuarios;

k) las contramedidas frente a ataques de canal técnico colateral; y

l) la demostración del cumplimiento de obligaciones y recomendaciones que se derivan de la aplicación de las leyes y del proceso de compatibilización de la inversión y el diseño con los intereses de la defensa, la seguridad y el orden interior.

2. Los renglones de comprobación de la calidad que se describen en el numeral anterior, se aplican para el análisis de un módulo criptográfico a introducir en programas computacionales, medios electrónicos o de otra magnitud física cuya función principal no es criptográfica.

Artículo 22. Los criptodispositivos o equipamientos destinados a la generación de números aleatorios para la producción independiente de criptomateriales, tienen que cumplir las reglas siguientes:

1. Refrendar la verificación de la calidad con evidencias de observación física, medición de parámetros electrónicos e informáticos, según corresponda, así como de las resultantes de la aplicación sobre los criptomateriales producidos de modelos matemáticos de probabilidades y estadísticas con acreditación al efecto.
2. Funcionar sin capacidad física alguna de conexión a redes de Telecomunicaciones/TIC, tanto del equipo generador de números aleatorios, como el medio para implementar los resultados del primero como llaves criptográficas prácticas.
3. El equipo generador de números aleatorios y el medio para implementar los resultados, se construyen con altas medidas de apantallamiento y filtraje eléctrico, electromagnético, acústico, óptico y térmico; sistemas de detección y barreras contra accesos físicos y lógicos hacia su interior, así como el borrado seguro de huellas digitales comprometedoras, y la conexión que se establece entre ambos no debe ser superior a un metro de distancia.
4. Aplicar sellaje de alta seguridad sobre el empaquetamiento del producto a entregar al cliente.
5. Tener los medios en locales con medidas técnicas y organizativas de protección física.

Artículo 23. El jefe de la Dirección de Criptografía emite como regla cada cinco años, el documento normativo que pone en vigor las especificaciones de las pruebas a realizar por los laboratorios de evaluación, según las áreas de exámenes que se definen en el pre-

sente Reglamento, y para las evidencias a presentar por los desarrolladores de los prestadores de servicios criptográficos industriales sobre la calidad y fortaleza de sus productos.

Artículo 24. Los tiempos máximos de duración del proceso de pruebas, que realizan los laboratorios de evaluación para dictaminar sobre la conformidad de los productos que presentan los desarrolladores de los servicios industriales criptográficos, son los siguientes:

1. Nivel de Seguridad número 1, hasta tres meses.
2. Nivel de Seguridad número 2, hasta seis meses.
3. Nivel de Seguridad número 3, hasta nueve meses.
4. Nivel de Seguridad número 4, hasta doce meses.

Artículo 25. La Dirección de Criptografía determina el tiempo por el que los laboratorios de evaluación conservan los resultados de las pruebas y calificaciones, como evidencias legales que demuestran el nivel de seguridad que disponían los criptodispositivos en el momento de ser aprobados para su empleo por el país.

Artículo 26. La certificación del nivel de calidad de los criptodispositivos se revalida cada cinco años, salvo que surjan modificaciones en su arquitectura tecnológica o nuevos mecanismos de ataques, que potencialmente afecten la seguridad calificada, lo cual requiere de una nueva evaluación para mantener su empleo en los servicios de protección.

Artículo 27. Se crean dos tribunales de expertos por la Dirección de Criptografía; uno para atender los asuntos que se relacionan con la aplicación de la criptografía en interés de objetivos de la defensa y seguridad nacional, y otro para el resto de las tecnologías, las técnicas y los servicios.

Artículo 28. Los tribunales se conforman con expertos que se escogen del Sistema de Aseguramiento Integral, en una cantidad de miembros impar, no superior a cinco y se renuevan cada dos años, para evaluar y dictaminar:

1. Los estudios de factibilidad y los proyectos de creación, innovación o asimilación tecnológica de algoritmos criptográficos.
2. Los diseños en fase de concepción de nuevos criptodispositivos.
3. La calificación de los conocimientos y destrezas del personal a acreditar para operar en la prestación técnica de los servicios criptográficos.

Artículo 29. Los miembros de los tribunales tienen que poseer experticia en materia de criptografía teórica y de aplicación práctica, categorización científica o tecnológica; y durante su permanencia en estos tribunales, no se recomienda que participen en trabajos de desarrollo de productos y servicios criptográficos, en virtud de garantizar su neutralidad e imparcialidad.

SECCIÓN CUARTA

De la planificación en la esfera de la criptografía

Artículo 30. Los planes a corto, mediano y largo plazos para alcanzar la satisfacción de la demanda nacional en materia de servicios criptográficos, se elaboran de acuerdo con la base legal y las prioridades de la economía, la sociedad, la defensa y la seguridad del país, teniendo en cuenta:

1. La evolución de la ciencia, la innovación tecnológica, la industria, la técnica, la metrología de la calidad, los instrumentos jurídicos normativos, económicos, operacionales y de comercio en materia de criptografía a escala nacional e internacional.
2. La organización, niveles técnicos y de empleo de los sistemas, equipos, programas y redes de gestión informativa, de datos, procesos automáticos y de telecomunicaciones del país.

3. El desarrollo de las amenazas y riesgos que se reconocen por autoridades nacionales e internacionales sobre la criptografía aplicada, así como sobre la información, las infraestructuras, plataformas, servicios y aplicaciones que se utilizan para su gestión, mitigables o anuladas con el empleo o el perfeccionamiento de la protección criptográfica.
4. La evolución de los medios de defensa técnica colateral de los propios servicios criptográficos para mitigar ataques contra la protección.
5. Las capacidades científicas, técnicas y organizativas disponibles en el Sistema de Aseguramiento Integral.

Artículo 31. A los efectos de facilitar la elaboración de los citados planes, la Dirección de Criptografía establece y disemina, por las vías pertinentes, las listas de:

1. Los criptodispositivos, módulos criptográficos y protocolos de comunicaciones cifradas que se aprueban para su empleo en la protección de la información del país, en correspondencia con la categorización de seguridad de los diferentes sistemas de trabajo y de la técnica que utilizan en la gestión informativa y de datos, así como los que se destinan a los fondos exportables y las relaciones internacionales públicas.
2. Los prestadores de servicios criptográficos y los laboratorios de evaluación de la calidad con acreditación en el Sistema de Aseguramiento Integral.
3. Los mecanismos y dominios comunes de ataques a los sistemas de la información, de controles automáticos de procesos industriales y de las Telecomunicaciones/TIC, que reconocen las autoridades nacionales competentes, y pueden ser evitados o mitigados en su totalidad o en parte con el empleo de la protección criptográfica.
4. Los plazos de obsolescencia de los criptodispositivos, en interés de la creación y puesta en funcionamiento de nuevos medios y para la organización de los tránsitos tecnológicos que correspondan.
5. Los lineamientos y prioridades integrales de actualidad en materia de protección criptográfica y para los servicios criptográficos.

Artículo 32. Son sujetos de elaboración de planes para la satisfacción de la demanda en materia de criptografía:

1. Los proveedores de servicios criptográficos.
2. Los proveedores de servicios de las Telecomunicaciones/TIC y la automatización, que aplican la protección criptográfica como parte de la calidad de sus prestaciones y por requerimientos legales, así como los suministradores de fondos exportables y de importación de productos que incluyen criptodispositivos.
3. Los órganos, organismos y entidades del Estado, el sistema empresarial y las organizaciones políticas, sociales y de masas, usufructuarios de la protección criptográfica, tanto para la salvaguarda de sus actividades, como en función de la que deben proporcionar en la interacción como servidores públicos.

Artículo 33. Los planes para alcanzar la satisfacción de la demanda de servicios criptográficos se establecen para:

1. El diseño, fabricación, suministro, adquisición e implementación práctica de criptodispositivos, protocolos de comunicaciones cifradas y para la habilitación de herramientas de análisis de la calidad de los citados medios y protocolos.
2. El completamiento o renovación de la protección criptográfica en los distintos ámbitos de manejo de datos, informaciones, señales técnicas, controles de acceso, identificación electrónica de personas y de sistemas de autorización para ejecutar operaciones con seguridad.

3. La formación, preparación, superación y capacitación de las personas naturales que se responsabilizan con el trabajo de especialistas en esta rama y con el empleo de la protección criptográfica.
4. Las investigaciones científicas y procesos de innovación tecnológica para perfeccionar las cualidades de seguridad de la protección criptográfica; las publicaciones científicas aplicadas de carácter público; la realización de eventos de esta categoría y las exportaciones en la esfera de la criptografía.

Artículo 34. Los planes que se establecen en esta sección, se firman y actualizan anualmente por los titulares de los sujetos declarados en el Artículo 32:

1. Los resultados de los estudios de factibilidad económica, organizativa y de capacidades humanas para su realización.
2. El análisis de riesgos y equilibrio entre las medidas técnicas, funcionales y organizativas para garantizar la seguridad y calidad necesarias de la protección a establecer y los servicios propios a ofertar.
3. Las inversiones a ejecutar.
4. Las nuevas implementaciones de protección criptográfica a desplegar en el período que se planifica.
5. El mejoramiento de los sistemas existentes.

Artículo 35. Los proyectos de planes se envían, por las direcciones de los sistemas de seguridad y protección, directores de los prestadores de servicios, o responsables de las actividades de esta rama en los sujetos, a la Dirección de Criptografía, la cual:

1. Los examina y coordina el proceso de consulta con las autoridades rectoras competentes, según el tema.
2. Presenta la propuesta de los dictámenes técnicos correspondientes al Ministro del Interior para su aprobación total o con las salvedades o recomendaciones pertinentes.
3. Realiza la actividad de asesoramiento para la elaboración de los planes que se señalan.

Artículo 36. Una vez aprobados por el ministro del Interior, los dictámenes de las propuestas de planes, son enviados a las entidades para su aprobación definitiva por sus titulares.

Artículo 37. En los controles estatales a los sistemas de seguridad y protección, y otros eventos de fiscalización que se realizan, la Dirección de Criptografía verifica que los planes para la satisfacción de la demanda en materia criptográfica, se encuentren con el debido respaldo económico y financiero a cargo del sujeto bajo control.

SECCIÓN QUINTA

Generalidades sobre los servicios criptográficos

Artículo 38. Los prestadores de servicios criptográficos en virtud de la creación, producción, suministro de criptodispositivos, la implementación de la debida protección y su asistencia técnica en el ámbito nacional y para la exportación, presentan a la Dirección de Criptografía, para su aprobación, con dos meses de antelación antes del inicio del ciclo de vida de los productos que se señalan, los requerimientos de encadenamiento productivo con entidades no pertenecientes al Sistema de Aseguramiento Integral.

Artículo 39.1. Los prestadores de servicios criptográficos conservan los expedientes sobre los procesos de la prestación que brindan durante el ciclo de vida del producto o actividad que lo genera, a los efectos de poder realizar análisis y controles preventivos y correctivos con el fin de mantener o mejorar los parámetros de calidad funcional y de seguridad, según corresponda, así como para establecer la memoria histórica pertinente en el Sistema de Aseguramiento Integral.

2. Las solicitudes de destrucción parcial o total de los expedientes, una vez concluido el ciclo de vida del producto o la actividad en cuestión, se presentan a la Dirección de Criptografía, con la fundamentación de la propuesta y la declaración jurada del no aprovechamiento de la documentación para la innovación tecnológica, la preparación y capacitación de especialistas, la memoria histórica de la criptografía, y a los efectos del sistema de control interno y otros fines de la economía, la seguridad, el orden interior, el cumplimiento de la ley y sobre reclamaciones de usuarios no atendidas.

Artículo 40.1. El proceso de validación, clasificación y aprobación de los algoritmos criptográficos que se presenten a la Dirección de Criptografía por personas naturales y jurídicas, como candidatos a convertirse en normativa ramal para su empleo en la confección de criptodispositivos por la industria, se someten al escrutinio y examen del Sistema de Aseguramiento Integral, incluida la Infraestructura de Calidad Criptográfica.

2. En el proceso de validación, clasificación y aprobación de los algoritmos criptográficos, se cumplen las medidas que garanticen la protección de las propiedades intelectual e industrial que corresponda.

3. El período para la culminación del proceso de validación, clasificación y aprobación de los algoritmos criptográficos es a lo sumo de tres años, desde su presentación.

4. La presentación de un algoritmo criptográfico al proceso que se señala, se realiza en forma de pseudocódigo, diagramas de flujo de su operatoria y en el lenguaje de programación específico que se propone o en algún objeto capaz de llevar a cabo sus instrucciones, con la fundamentación científica y tecnológica conceptual de la fortaleza de seguridad criptológica y operacional.

Artículo 41. Los servicios de la industria de criptodispositivos, académicos y de confianza digital, además de recibir de la Dirección de Criptografía las acreditaciones y permisos específicos de la rama para el desarrollo de sus prestaciones, tienen que disponer como condición necesaria, los documentos de validación de calidad que se normalizan nacional y obligatoriamente para los procesos industriales, docentes, de la ciencia y la innovación tecnológica, de negocios, y de los servicios que emiten las autoridades competentes al efecto.

SECCIÓN SEXTA

Sobre el Servicio Central de Cifras y la Infraestructura Nacional de Llave Pública

Artículo 42.1. La Dirección de Criptografía dirige el Servicio Central de Cifras y somete a la aprobación del ministro del Interior, la arquitectura, medidas de incremento, mantenimiento y perfeccionamiento de la seguridad criptológica y operacional de los diferentes servicios que lo conforman, así como las propuestas de presupuestos a solicitar a las autoridades competentes y usuarios al efecto; y tiene las funciones principales siguientes:

a) Ejecutar los programas de capacitación de administradores, operarios técnicos y de usuarios del Servicio, así como controlar la calidad de dicha capacitación e idoneidad del personal especialista de las diferentes prestaciones que brinda el citado Servicio, y practicar o proponer según corresponda, las medidas necesarias para su perfeccionamiento;
b) ejecutar las pruebas integrales de autocontrol sobre la calidad de funcionamiento y el mantenimiento de los niveles de seguridad de los citados servicios;
c) mantener actualizado el registro de usuarios del Servicio;

d) actuar como centro coordinador y supervisor de las operaciones tecnológicas, técnicas y de seguridad de las redes y aplicaciones criptográficas que soporta el Servicio Central;
e) prevenir y solucionar averías, y detectar intentos de ataques, así como en ese caso verificar y comprobar la efectividad de las contramedidas técnicas, físicas y organizativas instaladas;
f) recibir de los prestadores de servicios criptográficos con acreditación, en el primer trimestre de cada año, las demandas temporales de producción y para el próximo año de criptomateriales para sectores especiales; y
g) determinar las formas de ejecutar dicha producción segura en el Sistema de Aseguramiento Integral y los aseguramientos materiales o financieros que deben correr a cargo de los demandantes.

2. En el funcionamiento como Autoridad Raíz de la Infraestructura Nacional de Llave Pública, el Servicio Central de Cifras realiza las actividades siguientes:

a) Asesorar a los sujetos candidatos a funcionar como prestadores de servicios en la citada Infraestructura Nacional, o de aquellos vigentes que requieren perfeccionamiento, en la elaboración de los proyectos de declaraciones de política y de prácticas de certificación;
b) firmar digitalmente el certificado digital de la persona jurídica con acreditación para operar como prestador de servicios en la Infraestructura Nacional de Llave Pública;
c) establecer para los diversos entornos y circunstancias de empleo de los certificados digitales, los protocolos y técnicas de verificación en línea, de la validez de los certificados digitales de llave pública de los prestadores de servicios de la citada Infraestructura, en vista de facilitar con la seguridad y confianza que se requiere, el comercio y los servicios electrónicos nacionales e internacionales;
d) participar en los eventos de controles de la calidad del funcionamiento y seguridad de la Infraestructura Nacional de Llave Pública; y
e) promover y conducir la investigación científica y la innovación tecnológica para el perfeccionamiento de la Infraestructura Nacional de Llave Pública, con la participación de los factores del Sistema de Aseguramiento Integral.

Artículo 43. La Infraestructura Nacional de Llave Pública es la plataforma técnica y organizativa de protección informativa fundamental que contribuye a la efectividad de la transformación digital de la sociedad cubana y de la interrelación del país con el mundo a través de las Telecomunicaciones/TIC.

Artículo 44.1. El formato de certificado digital que se emplea en la Infraestructura Nacional de Llave Pública es el que instituya la Dirección de Criptografía, a partir del establecido como estándar global por la Unión Internacional de Telecomunicaciones.

2. En relación con el Servicio Central de Cifras y la Infraestructura Nacional de Llave Pública, la Dirección de Criptografía:

a) Informa al público la versión vigente del formato de certificado digital de Llave Pública a emplear en el país, y las especificaciones técnicas de los campos obligatorios y opcionales que se deben rellenar con los datos necesarios y suficientes para su funcionamiento confiable; y
b) emite los procedimientos técnicos y organizativos específicos que resulten necesarios, o propone la puesta en vigor de una norma de rango superior cuando corresponda, en el interés de mejorar y actualizar las prácticas del funcionamiento, la seguridad integral, interoperabilidad y efectividad de los servicios de la Infraestructura Nacional de Llave Pública, de Cadenas de Bloques y de Confianza Digital basados en el uso de los certificados digitales de Llave Pública.

Artículo 45. Los certificados digitales de Llave Pública se clasifican en las categorías siguientes:

1. Categoría 1: Certificados Digitales de Llave Pública para firma digital de mensajería y documentos electrónicos, CD Pfirma.
2. Categoría 2: Certificados Digitales de Llave Pública para firmar códigos computacionales por los fabricantes y suministradores de aplicaciones y componentes informáticos, CD PCOD.
3. Categoría 3: Certificados Digitales de Llave Pública para la autenticación de identidad de personas, servidores y equipos de cómputo en red y cifrado de canales de comunicaciones de los servicios de red web, CD SSL.

Artículo 46. Los certificados digitales son únicos y universales, se emiten y entregan a los solicitantes o a sus representantes legales por los prestadores de servicios con autorización de la Dirección de Criptografía para operar en la Infraestructura Nacional de Llave Pública, previa declaración aprobatoria de un sujeto administrativo que se acredita como una autoridad de registro, el que atestigua con evidencias, que dicho solicitante es quien dice ser.

Artículo 47. En el caso de los certificados digitales para la firma digital de documentos electrónicos y de códigos informáticos, puestos en vigor por la Infraestructura Nacional de Llave Pública, se establecen los principios generales siguientes:

1. La Llave criptográfica privada única, la genera y custodia el propietario solicitante del certificado digital, a partir de la norma técnica vigente para la creación de la firma digital.
2. Cuando la Llave criptográfica privada, a solicitud del propietario solicitante del certificado digital, o por razones técnicas o de seguridad, se genere por el prestador del servicios de emisión de certificados digitales, su producción se realiza obligatoriamente de forma compartida por tres funcionarios de dicho prestador, y se entrega al propietario en un dispositivo informático o electrónico bajo protección criptográfica y control de acceso a ella por medio de una contraseña o número de identificación personal, código PIN.
3. En el proceso de producción en el prestador de servicios, una vez obtenida la llave criptográfica privada, se procede, de forma automática y con registro, al borrado seguro de las huellas digitales del evento.
4. Cuando el citado medio no se entrega directamente al propietario, el traslado de la llave criptográfica privada, desde la ubicación del prestador de servicio hasta el destino geográfico del propietario, viaja con el código PIN que asigna el prestador de servicios, en sobre sellado y lacrado, a través de correo postal seguro.
5. Una vez que el propietario tiene en su poder la llave criptográfica privada, puede cambiar el código PIN del dispositivo protegido donde la aloja definitivamente, por otro código que conoce solamente él.
6. El prestador de servicios no guarda copia de la llave criptográfica privada del propietario, con el objetivo de asegurar la posesión exclusiva de esta por dicho propietario, en la garantía de la no existencia de dudas en la unicidad total del ejercicio de firma digital de documento o fichero electrónico, y el no repudio en esta acción personal e intransferible, de forma tal que no se pueda involucrar al citado prestador en hechos de falsificación o suplantación de la firma digital.
7. La copia de la llave criptográfica privada para el ejercicio de la firma digital, puede conservarse, mediante contratos, en otro prestador de servicios de confianza digital, cuyo negocio o designación tiene la acreditación en el Sistema de Aseguramiento

Integral y dispone de la organización, procedimientos y medios específicos para la custodia de documentos y otros valores electrónicos.

SECCIÓN SÉPTIMA

Sobre los servicios mediante cadenas de bloques

Artículo 48. La aprobación del establecimiento de servicios de protección criptográfica mediante el empleo de infraestructuras de cadenas de bloques en las redes Telecomunicaciones/TIC de Cuba, se basa en los requisitos siguientes:

1. Los prestadores de servicios de este tipo a acreditar, además de cumplir las normativas que se establecen en el proceso de acreditación en la Infraestructura de Calidad Criptográfica, presentan a la Dirección de Criptografía las obligaciones que demandan las autoridades de relación con la utilización de los citados servicios, sobre el tipo de permiso de acceso a los datos de control que ofrece la cadena de bloques.
2. Los criptodispositivos y algoritmos criptográficos que se utilizan para la seguridad de los registros de contabilidad distribuida y la formación de las cadenas de bloques, son aprobados por la Dirección de Criptografía.
3. La arquitectura de la cadena de bloques, proporciona y facilita la inspección y auditoría de las autoridades competentes.

SECCIÓN OCTAVA

Sobre los prestadores de servicios criptográficos

Artículo 49.1. El aspirante a prestador de servicios criptográficos realiza la solicitud oficial a la Dirección de Criptografía, la cual debe contener:

a) Datos identificativos y de contacto de la entidad solicitante;
b) fundamentación sobre la necesidad y alcance de la prestación del servicio;
c) estudio de factibilidad para su puesta en explotación y sostenibilidad, elaborado sobre la base de la evaluación de la existencia de condiciones tangibles para cumplir con las obligaciones y facultades establecidas en la operación del prestador de servicio propuesto; y
d) documentación probatoria de que es una persona jurídica constituida según la legislación vigente en la República de Cuba, con domicilio en la misma y que su objeto social esté en correspondencia con la prestación de los servicios que solicita y posee la acreditación o licencia del órgano competente.

2. Los sujetos que radican en el exterior o que poseen dominio cibernético fuera de Cuba, tienen que presentar, además, la aprobación de los organismos de la Administración Central del Estado competentes, para prestar servicios en el país.

Artículo 50. El proceso de aprobación por el ministro del Interior, se extiende por un período no mayor a noventa días hábiles, desde la fecha de presentación de la solicitud por los interesados, a través de la Dirección de Criptografía, la que emite la certificación de la decisión correspondiente.

Artículo 51.1. Todo prestador de servicios criptográficos está en la obligación de cumplir los requerimientos generales siguientes:

a) Tener definida e implementada con evidencias, la segmentación de roles de sus funcionarios; así como las medidas de seguridad que se establecen en el presente Reglamento;
b) tener habilitado el código de ética de los funcionarios, los que están en el deber de guardar el secreto profesional respecto a los datos confidenciales de carácter personal de los clientes;

c) disponer de una página web oficial y publicar sus declaraciones de políticas de seguridad y prácticas para el servicio que presta; vías de comunicación con sus usuarios y público en general; materiales informativos; y los precios de comercialización, cuando corresponda;
d) tener aprobados, por la Dirección de Criptografía, los medios y sistemas de protección criptográfica, que se requieran para la prestación de los servicios;
e) mantener actualizados los análisis y evaluación de riesgos y amenazas y los planes de reducción de desastres;
f) tener actualizados y validados los resultados de auditorías, inspecciones y otros procedimientos de control interno, que demuestren la existencia de un ambiente confiable en su entorno de funcionamiento, en correspondencia con lo establecido en la legislación vigente, teniendo en orden y acreditado por los órganos competentes, los mecanismos de solvencia económica para asegurar la prestación del servicio en general;
g) tener en funcionamiento permanente, todas las medidas de seguridad física y lógicas, así como las trazas auditables de los eventos para el aseguramiento de los servicios que presta y otros datos y medios requeridos por los clientes;
h) disponer de sistemas técnicos y organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios y locales de trabajo especializados, y la aplicación racional de métodos de defensa criptológica frente a intercepciones de sus comunicaciones e intromisiones informáticas o eléctricas en el equipamiento que se utiliza para prestar el servicio;
i) tener implementadas medidas para evitar y extinguir incendios, inundaciones, excesos de humedad y otros desastres naturales y tecnológicos, así como para la salva y restauración segura de la información de interés;
j) obtener, en los casos de prestadores comerciales de estos servicios, respaldo financiero mediante pólizas de seguro del tipo que corresponda, relacionados con los daños que un incidente cause a la actividad de los mismos;
k) asumir toda la responsabilidad frente a los clientes, en cuanto a la calidad del servicio que presta, con independencia de que parte de los procesos técnicos que lo aseguran se acuerden o contraten a una entidad externa al servicio criptográfico;
l) conservar en expedientes toda la información relevante sobre los procesos, sistemas de trazas, y cualquier dato o información resultante de su actividad, por el período de tiempo que establezca la Dirección de Criptografía, acorde a la actividad que realiza;
m) informar con antelación a sus clientes de cualquier cambio, modificación o suspensión de los servicios que presta;
n) atender y dar respuestas a las peticiones, quejas y reclamos hechos por los clientes;
ñ) tener aprobados previamente, por los máximos responsables de la entidad de su jurisdicción en correspondencia con los procedimientos estatales vigentes, a los funcionarios que laboran en las entidades prestadoras de servicios criptográficos, los cuales tendrán acreditados por la Dirección de Criptografía, los conocimientos y habilidades en materia criptológica; y
o) establecer con sus clientes, en los contratos y otros tipos de documentos, las obligaciones y derechos que contraen ambas partes en relación a los servicios y los tiempos de respuesta del prestador para dar solución a interrupciones técnicas, entrega de productos y demás prestaciones en la esfera de la criptografía.

2. Además de los anteriores, los prestadores tienen que cumplir los requerimientos particulares, que establece el Ministerio del Interior, de acuerdo con el tipo de servicio criptográfico a prestar.

Artículo 52. La Dirección de Criptografía establece los procedimientos, guías y requisitos específicos a evaluar para comprobar el cumplimiento de los requerimientos establecidos en el artículo precedente, por los prestadores de servicios criptográficos.

CAPÍTULO III
SOBRE EL FUNCIONAMIENTO DEL SISTEMA DE ASEGURAMIENTO INTEGRAL

SECCIÓN PRIMERA
Generalidades

Artículo 53. El Sistema de Aseguramiento Integral provee, como regla general, para el consumo nacional o la exportación de bienes y servicios:

1. Criptodispositivos integrales para la realización de la protección criptográfica.
2. Módulos criptográficos a ser incluidos como componentes adicionales en medios de propósito general para el procesamiento informativo, controles automáticos y las telecomunicaciones.
3. Tecnologías, técnicas, herramientas y equipos especiales para la medición y verificación de los parámetros de calidad de criptodispositivos y módulos criptográficos.
4. Materiales didácticos y divulgativos, de carácter científico, técnico, directivo y operacional, para las actividades de formación, superación, capacitación y entrenamiento de prestadores de servicios criptográficos y de otros que incorporen criptodispositivos a los servicios que ofertan, usuarios de la protección, funcionarios que actúan en el sistema de control interno, la investigación de incidentes y la verificación de la calidad en el ámbito de la criptografía y público en general, según corresponda.

Artículo 54.1. La Dirección de Criptografía, en relación con el Sistema de Aseguramiento Integral:

a) Aprueba la puesta en funcionamiento de las producciones del Sistema de Aseguramiento Integral que se señalan en el artículo precedente, destinadas a la protección de la información clasificada y limitada, las infraestructuras críticas, la dirección y gestión informativa de actividades desde los niveles centrales de los órganos, organismos, entidades del Estado, el sistema empresarial, las organizaciones políticas, sociales y de masas, las sedes diplomáticas, misiones y representaciones comerciales y empresariales cubanas en el exterior, la defensa y seguridad nacional; y
b) en coordinación con las autoridades competentes, establece las medidas que garanticen el cumplimiento de las normas nacionales de seguridad de la información en el ámbito tecnológico, técnico, operacional y comercial de los procesos de la producción, composición y distribución de los productos en la esfera de la criptografía, así como para la debida protección de las propiedades intelectual e industrial.

2. Las dependencias de criptografía en las jefaturas provinciales y del municipio especial Isla de la Juventud del Ministerio del Interior, aprueban la puesta en funcionamiento de las producciones del Sistema de Aseguramiento Integral desarrolladas en su localidad, destinadas a su utilización en la demarcación de sus competencias.

SECCIÓN SEGUNDA

De los órganos de colegio

Artículo 55. La Dirección de Criptografía actúa como coordinadora general del Sistema de Aseguramiento Integral y ejecuta las actividades directivas correspondientes, en aras de garantizar su funcionamiento permanente y eficaz.

Artículo 56.1. El Grupo Técnico Asesor en Políticas Criptográficas, órgano colegiado del citado Sistema de Aseguramiento Integral, realiza sus actividades de asesoramiento colectivo de forma presencial en espacios físicos o a través de los servicios de video o audioconferencias que proporciona el Sistema Seguro de Comunicaciones de la Dirección del País, convocado por la Dirección de Criptografía para la consulta de cuestiones estratégicas nacionales.

2. Para el tratamiento a cuestiones de envergadura menos estratégica y que requieren respuesta con inmediatez el Grupo Técnico Asesor en Políticas Criptográficas realiza el proceso de consulta mediante la circulación de documentos, por vías electrónicas cifradas o por correos personales según corresponda, dando a conocer a sus miembros los resultados de la consulta, así como de los acuerdos adoptados para todos los casos.

3. los miembros del Grupo Técnico Asesor en Políticas Criptográficas proponen temas a debatir y colegiar, para lo cual presentan a la Dirección de Criptografía sus propuestas con un mes de antelación a la fecha de convocatoria de la reunión del Grupo.

Artículo 57.1. El Comité Técnico de Normalización, órgano colegiado del citado Sistema de Aseguramiento Integral, se convoca de forma presencial por la Dirección de Criptografía, con el objetivo de analizar y recomendar sobre:

a) Los proyectos de documentos normativos existentes y evaluación de soluciones a prioridades del país en materia de calidad de los servicios criptográficos;
b) las propuestas de aspectos a incluir en el Programa Nacional de Normalización;
c) los temas a debatir en la Sección Consultiva de Ciencia e Innovación Tecnológica;
d) las políticas de precios, tarifas y seguros en los servicios de protección criptográfica; y
e) otros aspectos a establecer en la Infraestructura Nacional de Calidad en las áreas de su competencia.

2. Para el tratamiento a cuestiones de envergadura menos estratégica y que requieren respuesta con inmediatez, el Comité Técnico de Normalización realiza el proceso de consulta mediante la circulación de documentos, por vías electrónicas cifradas o por correos personales según corresponda, dando a conocer a sus miembros los resultados de la consulta, así como de los acuerdos de dicho Comité para todos los casos.

3. Los miembros del Comité Técnico de Normalización proponen temas a debatir y colegiar en el colectivo del mismo, para lo cual presentan a la Dirección de Criptografía sus propuestas con un mes de antelación a la fecha de convocatoria de la reunión del Comité.

4. En el primer trimestre de cada año, el Comité Técnico de Normalización analiza el comportamiento de la Sección Consultiva de Ciencia e Innovación Tecnológica, y propone al ministro del Interior, a través de la Dirección de Criptografía, las recomendaciones, los eventos a realizar por ésta y los cambios a introducir, según los aspectos que requieren de su concurso; la Dirección de Criptografía informa a los miembros del Comité sobre las decisiones al respecto.

Artículo 58.1. La Sección Consultiva de Ciencia e Innovación Tecnológica sesiona previo a las reuniones del Comité Técnico de Normalización, con el objetivo de realizar las recomendaciones pertinentes desde el ángulo de la ciencia y la tecnología para mejorar la calidad de la protección criptográfica del país, las que deben refrendarse mediante documentos normativos correspondientes.

2. La Sección Consultiva de Ciencia e Innovación Tecnológica se conforma con hasta ocho miembros permanentes y siete eventuales, estos últimos se seleccionan de acuerdo con los temas a debatir.

3. La Sección Consultiva de Ciencia e Innovación Tecnológica se constituye por expertos con categorización científica, tecnóloga y docente en materias afines a la criptografía, los cuales son propuestos, al Ministerio del Interior en el último trimestre del año corriente, por las máximas instancias de las universidades, centros científicos e industriales, con prioridad en aquellos que se califican como de alta tecnología y de otras entidades estatales afines, para su concesión, ratificación o renovación.

4. La Sección Consultiva de Ciencia e Innovación Tecnológica, se constituye además como un grupo auxiliar de la Dirección de Criptografía para la conducción de los procesos de obtención y aprobación de los algoritmos criptográficos a utilizar en los criptodispositivos que se emplean por el país en los sistemas de información pública y no clasificada, así como en interés de los fondos exportables.

Artículo 59.1. Como regla, la Dirección de Criptografía realiza anualmente con los directivos o representantes específicos de las partes que componen el Sistema de Aseguramiento Integral las acciones siguientes:

a) El balance de las actividades realizadas por el citado Sistema;
b) la evaluación de su efectividad; y
c) los posibles retos a enfrentar y acciones a ejecutar en el año y períodos subsiguientes, según la planificación del Gobierno.

2. En similar orden, organiza y desarrolla:

a) Los seminarios de preparación especializada de los miembros del Grupo Técnico Asesor en Políticas Criptográficas, del Comité Técnico de Normalización y los miembros permanentes de la Sección Consultiva de Ciencia e Innovación Tecnológica con vistas a la adquisición de los conocimientos integrales necesarios para el mejor ejercicio de sus funciones, e incluye la emisión de documentos didácticos en formato tradicional o digital, según las disponibilidades de recursos; y
b) la capacitación, contando con la colaboración de los entes pertinentes del Sistema de Aseguramiento Integral, de los funcionarios que atienden los asuntos de la protección criptográfica desde el sistema de seguridad y protección, en los órganos, organismos y entidades del Estado, el sistema empresarial y las organizaciones políticas, sociales y de masas, en temas de la criptografía afines a su radio de acción.

SECCIÓN TERCERA

Del Sistema de Información, Análisis y Prospectiva

Artículo 60. Las dependencias que se encargan de conducir los sistemas de Seguridad y Protección en los órganos, organismos y entidades del Estado, el sistema empresarial y las organizaciones políticas, sociales y de masas, así como los prestadores de servicios criptográficos, elaboran anualmente y presentan a la Dirección de Criptografía el informe contentivo de:

1. El cumplimiento de los planes.

2. El desenvolvimiento integral de la actividad.
3. El completamiento de la cobertura de protección criptográfica y la efectividad de su seguridad.
4. La prestación de los servicios al respecto.

Artículo 61. En relación con el Sistema de Información, Análisis y Prospectiva, la Dirección de Criptografía desarrolla las acciones siguientes:

1. Emite las precisiones sobre los requisitos informativos a evaluar, en correspondencia con lo que establece el citado Decreto-Ley 79 y las prioridades del país al respecto.
2. Elabora y propone al ministro del Interior, tomando como base los informes recibidos de los integrantes del Sistema de Aseguramiento Integral, la información estadística, analítica y prospectiva a presentar al Presidente de la República, en cuanto al comportamiento y efectividad de los servicios criptográficos y de la actividad general en el ámbito de la criptografía.
3. Mantiene el intercambio sistemático con la Oficina Nacional de Estadística e Información y se encarga de ejecutar los procedimientos pertinentes para garantizar la introducción de las informaciones específicas en materia criptográfica que requiere el Sistema de Información de Gobierno.
4. Emite cuando las circunstancias lo requieran, los boletines y notas informativas de Alerta Temprana, ante el surgimiento de amenazas, debilidades y vulnerabilidades que pongan en peligro la protección criptográfica que se emplea por el país, los bienes que se protegen o los proyectos de desarrollo y producción de nuevos criptodispositivos, así como las indicaciones con vistas a organizar y ampliar las medidas que se adoptan por los usuarios y proveedores de servicios criptográficos para cada una de las fases que se establecen en el presente Reglamento.

Artículo 62.1. La información de Alerta Temprana de Riesgos en el ámbito de la protección criptográfica, tiene como objetivo principal, prever la adopción de medidas para evitar o mitigar con métodos criptográficos, la realización de ataques con características técnicas públicamente conocidas, que pueden ser ejecutados sobre los sistemas informativos del país y su base tecnológica de gestión, incluida la propia protección criptográfica.

2. A los efectos de la emisión de las notas informativas y boletines de Alerta Temprana, se establecen tres fases de información:

a) Fase Informativa: Cuando se comprueba que las amenazas se encuentran en un plano teórico y de pruebas de concepto a nivel de laboratorio, que requieren para su realización de personal con muy alta especialización, herramientas y tácticas de agresión sofisticadas, violación de varias barreras de control presentes en los sistemas bajo probable riesgo, y que en el momento de la información, su probabilidad potencial de realización sea baja.

   Se emite por la Dirección de Criptografía para el conocimiento de los sujetos que conforman el Sistema de Aseguramiento Integral y los proveedores de servicios de las Telecomunicaciones/TIC.

b) Fase de Alerta: Cuando se comprueba que las amenazas se encuentran en pruebas de laboratorios, que pueden evolucionar hacia herramientas y tácticas de agresión prácticas en un periodo de tiempo no mayor a los dieciocho meses, aunque en el momento del análisis, se requiera para su realización de personal medianamente

calificado, violación de varias barreras de control presentes en los sistemas bajo probable riesgo y que en el momento de la alerta, su probabilidad real de realización sea media.

Se emite por la Dirección de Criptografía con la aprobación previa del ministro del Interior, para el conocimiento de los sujetos que conforman el Sistema de Aseguramiento Integral, de los proveedores de servicios de las Telecomunicaciones/TIC, las máximas direcciones de los órganos, organismos y entidades del Estado, el sistema empresarial y las organizaciones políticas, sociales y de masas.

c) Fase de Alarma: Cuando se comprueba que las amenazas y vulnerabilidades, pueden derivar en un ataque efectivo contra los sistemas informativos y su base tecnológica de gestión, se realiza con herramientas de agresión públicamente accesibles, fáciles de manipular anónimamente por personal no profesional, desde el exterior o interior del ente potencialmente víctima, y cuyo riesgo es severo por los daños que pudiese causar a la información propia y reputación de dicho ente o del país, así como a la base tecnológica de gestión informativa.

Se emite por el ministro del Interior a propuesta de la Dirección de Criptografía, para el conocimiento y efecto de los sujetos que conforman el Sistema de Aseguramiento Integral, los proveedores de servicios de las Telecomunicaciones/TIC, las máximas direcciones de los órganos, organismos y entidades del Estado, el sistema empresarial y las organizaciones políticas, sociales y de masas.

CAPÍTULO IV
DE LAS RELACIONES INTERNACIONALES EN LA ESFERA DE LA CRIPTOGRAFÍA

Artículo 63.1. La Dirección de Criptografía elabora la estrategia para las relaciones internacionales en la esfera de la criptografía con impacto en el desarrollo y la calidad de la base industrial nacional de esta especialidad, la cual se presenta por el ministro del Interior a la aprobación de los órganos superiores de dirección del país, según corresponda.

2. El proceso de elaboración de la citada estrategia, se desarrolla en consulta con el Grupo Técnico Asesor en Políticas Criptográficas, y según corresponda, con otras autoridades competentes de los ministerios de Comunicaciones, Ciencia, Tecnología y Medio Ambiente, Comercio Exterior y la Inversión Extranjera, Industrias, Relaciones Exteriores, las Fuerzas Armadas Revolucionarias y del Interior.

Artículo 64. Las personas naturales y jurídicas cubanas para establecer relaciones de cooperación, colaboración y de negocios, en materia de criptografía, con similares extranjeras, están obligadas a realizar el proceso de compatibilización con los intereses de la defensa, la seguridad y el orden interior, desde la etapa de concepción de estas, con el objetivo de garantizar la seguridad criptológica del país.

Artículo 65.1. El empleo en el territorio nacional de criptodispositivos procedentes de fuentes extranjeras, en los diferentes tipos y entornos de servicios, requieren del dictamen y las instrucciones específicas de la Dirección de Criptografía sobre el proceso de producción y administración de los criptomateriales a emplear.

2. El uso de estos criptodispositivos se realiza bajo contratos o acuerdos de garantías de seguridad con el suministrador.

CAPÍTULO V
DEL TRATAMIENTO A LOS INCIDENTES QUE ATENTAN CONTRA LA SEGURIDAD CRIPTOLÓGICA Y OPERACIONAL DE LOS CRIPTODISPOSITIVOS Y SERVICIOS CRIPTOGRÁFICOS Y SU REPUTACIÓN

SECCIÓN PRIMERA
Generalidades

Artículo 66.1. Se reconoce como incidente que atenta contra la seguridad criptológica y operacional de los criptodispositivos y servicios criptográficos, o contra la reputación de tales servicios, en lo adelante incidente, cuando se confirma o sospecha la ocurrencia de:

a) Actividad enemiga, delictiva o nociva;
b) una o varias de las conductas contraventoras descritas en el Capítulo VI del presente Reglamento; e
c) incumplimientos de las especificaciones técnicas, organizativas y procedimentales para el buen funcionamiento y salvaguarda de los criptodispositivos y servicios criptográficos, que comprometan, debiliten y vulneren la fortaleza defensiva de tales medios y prestaciones y que posibilite la ejecución de ataques previsibles, o pongan en duda su confiabilidad y calidad de cara a sus usuarios.

2. Un incidente puede ocurrir tanto en los objetivos protegidos criptográficamente, como en los sistemas de trabajo internos de un prestador de servicios criptográficos u otro prestador que utiliza criptodispositivos que se integran en los productos o servicios que oferta al público.
3. Las infracciones o incumplimientos de las especificaciones técnicas, organizativas o procedimentales en materia criptográfica que conllevan a la ocurrencia de un incidente, pueden categorizarse de leves, graves o muy graves en correspondencia con:
   a) La categorización que establece la legislación en materia de protección de la información y los datos, las Telecomunicaciones/TIC, la ciberseguridad, los controles automáticos para la seguridad del objetivo y actividades bajo salvaguarda, así como de los procesos productivos encaminados a la fabricación y suministro de diversos tipos de criptodispositivos integrales, módulos criptográficos u otros recursos y materiales en la esfera de la criptografía;
   b) la afectación que puede producir el incidente en servicios criptográficos de otros sistemas y actividades fuera del ámbito de ocurrencia del hecho, a la propiedad intelectual e industrial, y al patrimonio tecnológico nacional en materia de la criptografía; y
   c) el daño que se comprueba causa el incidente al objeto con protección criptográfica, así como a los procesos de producción y suministros de criptodispositivos integrales, módulos criptográficos u otros recursos y materiales de la esfera de la criptografía.

Artículo 67. Al ocurrir un incidente, se deben seguir los pasos siguientes:

1. La búsqueda de indicios o pruebas de la ocurrencia del incidente.
2. La emisión del reporte, por parte de quien detecta, hacia las autoridades competentes, que se encargan de encaminar y realizar la investigación sobre el incidente.
3. La ejecución de la investigación de rigor y análisis de los resultados para descartar: la actividad delictiva, la comisión de una o varias de las conductas contraventoras descritas en el Capítulo VI del presente Reglamento, o el incumplimiento de las especificaciones técnicas, organizativas y procedimentales; así como determinar los responsables, las causas y condiciones que favorecieron su ocurrencia y la magnitud del daño que ocasionó.

Estas investigaciones se realizan por expertos investigadores de la Infraestructura de Calidad Criptográfica, con acreditación de la Dirección de Criptografía o de las dependencias de esta especialidad en las jefaturas provinciales y del municipio especial Isla de la Juventud del Ministerio del Interior, en un término de treinta días hábiles.

4. La emisión del dictamen evaluativo del incidente por los expertos investigadores, para las autoridades competentes.

Artículo 68. El dictamen que emiten los expertos investigadores consta de los elementos siguientes:

1. La categorización del incidente.
2. La identificación de los responsables y sus conocimientos técnicos.
3. El nivel de daño o riesgos que genera en los sistemas que se protegen, u otros externos.
4. Las medidas técnicas, organizativas, procedimentales y financieras que deben adoptarse para eliminar las vulnerabilidades, en función de restablecer la confiabilidad del servicio criptográfico afectado y el plazo que se requiere, según la categorización de la seguridad del objetivo y actividades bajo protección.
5. La propuesta de medidas a adoptar a partir del tipo de incidente detectado.
6. Las recomendaciones sobre las medidas administrativas de índole laboral que pueden adoptarse por las autoridades competentes.

Artículo 69. La comprobación posterior sobre el cumplimiento de las medidas de saneamiento y restablecimiento de la confianza y las capacidades de seguridad criptológica y operacional de los criptodispositivos, servicios criptográficos y procesos afectados por un incidente, se incorpora en las agendas de inspección y demás actividades de control que efectúan las autoridades competentes.

Artículo 70. Cuando en el proceso investigativo de un incidente, existan evidencias para presumir que se trata de un hecho delictivo, los expertos investigadores a cargo, están en la obligación de formular la denuncia correspondiente, según lo dispuesto en la legislación penal vigente.

Artículo 71. Los gastos en que se incurra como consecuencia del saneamiento y restablecimiento de la confianza y las capacidades de seguridad criptológica y operacional de los criptodispositivos, servicios criptográficos y procesos afectados por un incidente, se exigen a los responsables según lo dispuesto en la legislación vigente.

Artículo 72. Los incidentes son detectados por:

1. Las personas naturales en el ejercicio de la gestión de su información o datos personales.
2. Los funcionarios y empleados en los órganos, organismos y entidades del Estado, el sistema empresarial, las organizaciones políticas, sociales y de masas, las sedes diplomáticas, misiones y representaciones comerciales y empresariales cubanas en el exterior, prestadores de servicios criptográficos y demás prestadores de servicios al público desde los sistemas empresariales.
3. Los centros de control técnico nacional, territorial o ramal de la Infraestructura de Calidad Criptográfica, del ciberespacio, los controles automáticos y las Telecomunicaciones/TIC.
4. Los funcionarios del Sistema de Aseguramiento Integral que se acreditan para realizar actividades de control en la Infraestructura de Calidad Criptográfica, sobre los servicios criptográficos en las áreas de su competencia.

Artículo 73. Los jefes de la Dirección de Criptografía y de las dependencias de esta especialidad en las jefaturas provinciales y del municipio especial Isla de la Juventud del Ministerio del Interior, establecen las vías, horarios y formas para la recepción de reportes sobre incidentes y su tratamiento por los centros que se destinan al efecto.

SECCIÓN SEGUNDA

Incidentes en materia de criptografía que se detectan en el ámbito de las personas jurídicas

Artículo 74.1. El funcionario o empleado de una entidad o de un prestador de servicios criptográficos, que detecte o tenga conocimiento de un incidente, lo informa de manera inmediata al jefe de la entidad donde se produce, y al de la estructura del Sistema de Seguridad y Protección, o al funcionario encargado de su atención.

2. El jefe de la entidad o el de la estructura de Seguridad y Protección en un plazo no superior a las 24 horas, informa sobre la ocurrencia del incidente a la Dirección de Criptografía o a las dependencias de esta especialidad en la jefatura provincial o del municipio especial Isla de la Juventud del Ministerio del Interior según corresponda, y solicita la presencia de los expertos investigadores.

3. Los expertos investigadores a cargo, una vez concluido el proceso investigativo, entregan el dictamen resultante al jefe de la entidad o del prestador de servicios criptográficos cuando corresponda, así como al jefe de la estructura de Seguridad y Protección o al funcionario encargado de esta actividad, y remiten una copia a la Dirección de Criptografía, o a la dependencia de esta especialidad en la jefatura provincial o del municipio especial Isla de la Juventud del Ministerio del Interior, según sea el caso.

4. El jefe del Sistema de Seguridad y Protección o el funcionario a cargo de esta actividad en la entidad de ocurrencia del incidente, una vez conocido el dictamen, organiza el análisis y propone al dirigente máximo:

a) Las medidas que correspondan implementar, en función del restablecimiento de las capacidades de seguridad criptológica y operacional afectadas o en riesgo;
b) las medidas administrativas a aplicar a los infractores internos, o la demanda al prestador de servicio criptográfico cuando dicho incidente sea de su responsabilidad; y
c) la información a rendir a la Dirección de Criptografía o a la instancia de esta especialidad en la jefatura provincial o el municipio especial Isla de la Juventud del Ministerio del Interior según corresponda, sobre el resultado del análisis y las medidas implementadas.

Artículo 75. Si la información sobre la detección de un incidente que atenta contra la seguridad criptológica y operacional de los sistemas a su cargo, procede de un centro de control técnico nacional, territorial o ramal de la Infraestructura de Calidad Criptográfica, del ciberespacio, los controles automáticos y las Telecomunicaciones/TIC, tanto el centro que detecta como la entidad donde se produce el incidente, están en la obligación de informar a la Dirección de Criptografía o la dependencia de esta especialidad en la jefatura provincial o del municipio especial Isla de la Juventud del Ministerio del Interior, según el territorio donde esté enclavada la entidad.

Artículo 76.1. La Dirección de Criptografía o las dependencias de esta especialidad en las jefaturas provinciales o del municipio especial Isla de la Juventud del Ministerio del Interior, según corresponda, notifica a la entidad responsable o donde se produce el incidente, el acta de conformidad del Ministerio del Interior al respecto, en un término no mayor a los treinta días hábiles a partir de la fecha en que se recibe la información.

2. En el acta de conformidad se recogen, entre otros aspectos, las rectificaciones o recomendaciones que resulten necesarias, de acuerdo con la gravedad del hecho y sus consecuencias.

SECCIÓN TERCERA

Incidentes en materia de criptografía que se detectan en el ámbito de las personas naturales

Artículo 77.1. Los prestadores de servicios criptográficos y de otros servicios que utilizan módulos criptográficos formando parte de sus productos básicos, que ofertan a las personas naturales para la salvaguarda de sus datos y correspondencia privada, están en la obligación de mostrar en sus medios de publicidad, las formas y vías, presenciales y por línea, que permitan canalizar por el público sus reportes de incidentes.

2. Cuando una persona natural en el uso de criptodispositivos o módulos criptográficos con certificación de la Dirección de Criptografía para la salvaguarda de sus datos privados y correspondencia particular, detecta la presencia de un incidente, reporta al prestador de servicio que corresponda, y solicita a este último los datos de identificación del reporte.

3. El prestador de servicios que recibe el reporte, atiende el incidente con expertos e investigadores propios, e informa de inmediato al centro destinado al efecto por la Dirección de Criptografía o sus dependencias en las jefaturas provinciales y del municipio especial Isla de la Juventud del Ministerio del Interior, según la geolocalización de la ocurrencia del incidente.

4. El prestador, una vez concluidas las investigaciones, procede a implementar las medidas que permitan eliminar las causas y condiciones que propiciaron el incidente, y el restablecimiento de la confianza en los servicios que presta, e informa sobre la aplicación de las mismas a la Dirección de Criptografía o sus dependencias en las jefaturas provinciales y del municipio especial Isla de la Juventud del Ministerio del Interior según corresponda y a la persona que realizó el reporte del incidente.

CAPITULO VI

DE LAS CONDUCTAS CONTRAVENTORAS

SECCIÓN PRIMERA

De las contravenciones

Artículo 78. Se consideran contravenciones en materia de desarrollo, aplicación y uso de los dispositivos de protección criptográfica, y servicios en la esfera de la criptografía, las siguientes:

1. Realizar actividades técnicas de búsqueda de vulnerabilidades en la protección criptográfica que se emplea en Cuba y sus representaciones en el exterior sin la acreditación de la Dirección de Criptografía, así como realizar dichas actividades desde el territorio nacional sobre entes de terceros países que operan en redes globales de comunicaciones.
2. Publicar tecnologías o vulnerabilidades asociadas a criptodispositivos de producción nacional o de importación que se utilizan para la protección de los sistemas de información y de las Telecomunicaciones/TIC que se establecen por las autoridades competentes del país, sin la autorización de la Dirección de Criptografía.
3. Importar, comercializar o poner en explotación criptodispositivos para ejercer la protección criptográfica en los ámbitos que establece el Artículo 6 del Decreto-Ley, o exportar estos productos, sin autorización de la Dirección de Criptografía.

4. Realizar cambios en la funcionabilidad criptográfica de uno o varios criptodispositivos aprobados para su explotación en una entidad; o brindar servicios criptográficos a terceros por un prestador del Sistema de Aseguramiento Integral, sin autorización de la Dirección de Criptografía.
5. Desactivar criptodispositivos o servicios criptográficos puestos en explotación para la protección en una entidad o de la prestación de servicios a terceros, sin la aprobación del jefe máximo de la entidad, o el conocimiento de los beneficiarios de dicho servicio, y sin la autorización previa de la Dirección de Criptografía.
6. Incumplir, por el prestador de servicios criptográficos, la ejecución, en los plazos establecidos en los boletines de alerta temprana, de los cambios de configuraciones a los criptodispositivos para contrarrestar las amenazas identificadas.
7. Incumplir las medidas de seguridad para la guarda, custodia y defensa de criptodispositivos o criptomateriales asignados al funcionario de una entidad o prestador de servicios.
8. Negarse un prestador de servicios criptográficos a brindar, a los beneficiados de la protección, los datos de carácter no clasificados sobre la calidad y fortaleza del producto o prestación que se proporciona, o las reglas para su uso.
9. Brindar, por un funcionario de la prestación de los servicios, a terceros no autorizados, los datos personales de clientes de los citados servicios, sin el consentimiento de estos, salvo en los casos previstos en ley.
10. Colocar o permitir que se coloque en sus medios publicitarios e informativos, tecnologías, técnicas y aplicaciones criptográficas de cualquier origen que no han sido objeto de aprobación, para su empleo por alguna persona natural o jurídica con acceso a los citados medios.

SECCIÓN SEGUNDA
De las sanciones a aplicar ante las contravenciones

Artículo 79.1. A la persona natural que incurra en las contravenciones previstas en los numerales 1, 2, 3, 4, 5, 6 y 10 del artículo anterior se le impone una multa de seis mil pesos cubanos; en el caso de ser una persona jurídica esta asciende a doce mil pesos cubanos.

2. A la persona natural que incurra en las contravenciones previstas en los numerales 7, 8 y 9, del artículo anterior, se le impone una multa de tres mil pesos cubanos; y de ser una persona jurídica de seis mil pesos cubanos.

3. A los responsables de incurrir en las contravenciones previstas en los numerales 1, 3, 4 y 10 del artículo anterior, además de la multa, se les puede aplicar el decomiso, que constituye la confiscación de los equipos y medios utilizados en los hechos.

4. Cuando quien incurra en cualquiera de las contravenciones previstas sea un prestador de servicios en la esfera de la criptografía, se le puede aplicar además la sanción accesoria de suspensión temporal o definitiva de la autorización para el ejercicio de esta actividad.

Artículo 80. Las sanciones que impone la autoridad con facultades para exigir responsabilidad a quien incurra en contravenciones en materia de criptografía, en correspondencia con la gravedad de los daños que se ocasionan, se aplican en un plazo de hasta 10 días hábiles a partir que se identifique al o los responsables.

SECCIÓN TERCERA
De las autoridades facultadas para imponer las sanciones

Artículo 81. La autoridad facultada para imponer las sanciones a quien incurra en contravenciones en materia de criptografía establecidas en el presente Reglamento, es el

jefe de los funcionarios del Ministerio del Interior que ejercen la actividad de inspección en esta materia.

Artículo 82.1. Ante contravenciones en las que resulte necesaria la ocupación de los equipos y medios utilizados en los hechos que puedan resultar aplicable la sanción de decomiso, los funcionarios que ejercen la actividad de inspección en materia de criptografía, son los responsables de su conservación, guarda y custodia, previa elaboración del correspondiente expediente.

2. El expediente debe contener el documento que acredite la infracción cometida, descripción de la infracción, responsable, así como la resolución correspondiente y el acta de ocupación en la que se detalle las características del medio, su estado, marca, modelo, año de fabricación, número de serie y todos aquellos datos que permitan su identificación e individualización.

SECCIÓN CUARTA

De las recursos y autoridades facultadas para resolverlos

Artículo 83. Las personas naturales y jurídicas a las que se les imponga las sanciones previstas en el Artículo 79, pueden interponer recurso de reforma ante la autoridad prevista en el Artículo 81, en el plazo de diez días hábiles contados a partir de la fecha de su notificación; el que lo resuelve en el término de hasta treinta días naturales posteriores a la fecha en que se recibe la reclamación, y se le notifica al interesado en los cinco días siguientes.

Artículo 84. La persona inconforme con lo resuelto, puede interponer recurso de alzada ante el jefe inmediato de quien resolvió el recurso de reforma, en el plazo de diez días hábiles contados a partir de la fecha de notificación de la resolución; el que lo resuelve en el término de hasta cuarenta y cinco días naturales posteriores a la fecha en que se recibe el recurso, y se le notifica al interesado en los cinco días siguientes.

Artículo 85. Contra la resolución que resuelve el recurso de alzada no procede ningún otro recurso en la vía administrativa y queda expedita la vía judicial, de acuerdo con lo dispuesto en la legislación vigente.

Artículo 86. Los recursos de reforma y alzada se presentan por escrito con los datos siguientes:

1. Generales y dirección del reclamante.
2. Número de serie del talón de la multa impuesta; número y fecha de la Resolución por la cual se dispuso el decomiso o suspensión temporal o definitiva de la autorización para prestar servicios en la esfera de la criptografía.
3. Síntesis de los hechos.
4. Fundamentos en que se basa la reclamación.

DISPOSICIONES ESPECIALES

PRIMERA: El ministro del Interior, cuando proceda el decomiso de los equipos y medios utilizados en los hechos previstos como contravención, es la autoridad facultada para dar el destino socioeconómico más útil al país de los bienes decomisados, una vez hecha firme la resolución que lo dispuso.

SEGUNDA: El ministro del Interior, a propuesta de la Dirección de Criptografía y previa consulta de las autoridades que corresponda, somete a la aprobación del Presidente de la República las regulaciones que puedan resultar necesarias para asegurar la protección criptográfica del intercambio de información de los órganos estatales, organismos de la Administración Central del Estado, entidades del Estado, el sistema empresarial y las or-

ganizaciones políticas, sociales y de masas, con las sedes diplomáticas, representaciones comerciales y empresariales cubanas en el exterior.

DISPOSICIONES FINALES

PRIMERA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior adecuan la aplicación de las disposiciones establecidas en el presente Decreto, para ajustarlos a las características internas de ambos organismos.

SEGUNDA: Los servicios criptográficos que prestan entidades del Ministerio de la Fuerzas Armadas Revolucionarias y el Ministerio del Interior a personas naturales o jurídicas no pertenecientes a estos organismos, se ejecutan de acuerdo con lo establecido en el presente Decreto y demás disposiciones emitidas por el Ministerio del Interior, que garanticen la mejor aplicación y cumplimiento de lo dispuesto.

TERCERA: Derogar, de la Resolución 2 del ministro del Interior "Que pone en vigor los reglamentos para la criptografía y el servicio cifrado en el territorio nacional y para el servicio central cifrado en el exterior", de 2 de julio de 2002, el Anexo 1 "Reglamento para la criptografía y el servicio cifrado en el territorio nacional"; y la Resolución 2 del ministro del Interior "Que establece la infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial de la República de Cuba y aprueba el Reglamento para su funcionamiento", de 1ro. de septiembre de 2016.

CUARTA: El presente Decreto entra en vigor a los noventa días naturales siguientes a su publicación en la Gaceta Oficial de la República de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 24 días del mes de julio de 2024, "Año 66 de la Revolución".

Manuel Marrero Cruz