INTERIOR

RESOLUCION No. 2
DEL MINISTRO DEL INTERIOR

QUE PONE EN VIGOR LOS REGLAMENTOS PARA LA CRIPTOGRAFIA Y EL SERVICIO CIFRADO EN EL TERRITORIO NACIONAL Y PARA EL SERVICIO CENTRAL CIFRADO EN EL EXTERIOR

POR CUANTO: El Consejo de Estado ha aprobado el Decreto-Ley No. 199 del 25 de noviembre de 1999, "Sobre la Seguridad y Protección de la Información Oficial", mediante el cual se establece y regula la Criptografía y el Servicio Cifrado en el país**.**

POR CUANTO: La Criptografía y el Servicio Cifrado requieren de un conjunto de regulaciones, medidas organizativas y técnicas, y de medios para la protección criptográfica de la información oficial clasificada que se trasmite y almacena por las tecnologías de información de los órganos, organismos, entidades y sus dependencias o de cualquier otra persona jurídica con domicilio o establecimiento en el territorio nacional.

POR CUANTO: Es necesario fortalecer el desarrollo e incrementar el empleo de los Sistemas de Protección Criptográficos y el Servicio Cifrado en el país y en especial su uso por los dirigentes y funcionarios que cumplen misión en el exterior.

POR CUANTO: El precitado Decreto-Ley No. 199, en su Disposición Final Segunda, faculta al Ministerio del Interior para emitir el Reglamento y demás disposiciones complementarias que resulten necesarias para su mejor cumplimiento.

POR TANTO: En uso de las facultades que me están conferidas;

R e s u e l v o :

PRIMERO: Poner en vigor los Reglamentos para la Criptografía y el Servicio Cifrado en el Territorio Nacional y para el Servicio Central Cifrado en el Exterior, recogidos en anexos 1 y 2 a la presente Resolución.

SEGUNDO: El Viceministro del Interior emitirá las disposiciones complementarias que resulten necesarias para el cumplimiento de los reglamentos puestos en vigor en el apartado anterior.

TERCERO: Se excluye de lo que en la presente se establece, al Ministerio de las Fuerzas Armadas Revolucionarias, que se regirá por las regulaciones internas que al respecto establezca. En caso de requerirse utilizar el Servicio Central Cifrado y los Sistemas de Protección o producción Criptográfica, se cumplirá lo establecido en la presente Resolución.

CUARTO: Publíquese esta Resolución y el Reglamento para la Criptografía y el Servicio Cifrado en el Territorio Nacional, en la Gaceta Oficial de la República de Cuba.

QUINTO: Comuníquese el Reglamento para el Servicio Central Cifrado en el Exterior, al Consejo de Estado, Comité Ejecutivo del Consejo de Ministros, a la Asamblea Nacional del Poder Popular, a los Ministros de las Fuerzas Armadas Revolucionarias, Relaciones Exteriores, Comercio Exterior, Informática y las Comunicaciones, Inversión Extranjera, Ciencia, Tecnología y Medio Ambiente y al Presidente de la Banca Central.

Dada en la Ciudad de La Habana a los 2 días del mes de julio del 2002.

General de Cuerpo de Ejército
Abelardo Colomé Ibarra
Ministro del Interior

ANEXO 1

REGLAMENTO PARA LA CRIPTOGRAFIA Y EL SERVICIO CIFRADO EN EL TERRITORIO NACIONAL

CAPITULO I
GENERALIDADES

ARTICULO 1.-El presente Reglamento establece las normas, procedimientos y responsabilidades para el empleo de la Criptografía y el Servicio Cifrado en el territorio nacional, que deben aplicarse y cumplirse en los órganos, organismos, entidades y sus dependencias o por cualquier otra persona jurídica radicada en el territorio nacional y las personas naturales residentes en el país.

ARTICULO 2.-A los efectos del Decreto-Ley No.199 de 25 de noviembre de 1999 "Sobre la Seguridad y Protección de la Información Oficial", en lo adelante Decreto-Ley y el presente Reglamento se entenderá por:

Servicio Central Cifrado: Servicio Cifrado que brinda el Ministerio del Interior a los órganos, organismos y entidades del país y Misiones Estatales Cubanas en el exterior.

Servicio Cifrado de Uso Propio: Servicio cifrado que posee un órgano, organismo o entidad con un Sistema de Protección Criptográfica para la transmisión de la información oficial clasificada, autorizado por el Ministerio del Interior.

Sistema de Protección Criptográfica: Es el conjunto formado por el cifrador, los criptomateriales y los medios auxiliares que se emplean para el cifrado y descifrado de la información.

ARTICULO 3.-El acceso a las actividades de los Servicios Cifrados, sólo podrá autorizarse a personas naturales o jurídicas cubanas.

ARTICULO 4.-Toda persona natural o jurídica extranjera radicada en el país, para trasmitir información con protección criptográfica mediante sistemas de comunicaciones, requerirá de un permiso especial emitido por el Ministerio del Interior.

ARTICULO 5.-La Dirección de Informática, Comu-nicaciones y Cifras del Ministerio del Interior es el órgano encargado de garantizar el Servicio Central Cifrado para la información oficial del Partido Comunista de Cuba, el Consejo de Estado, el Consejo de Ministros, la Asamblea Nacional del Poder Popular y las Misiones Estatales Cubanas en el exterior.

ARTICULO 6.-En interés de la máxima compartimentación y seguridad de los Sistemas de Protección Criptográfica, la Dirección de Informática, Comunicaciones y Cifras del Ministerio del Interior centralizará la producción y el suministro de los criptomateriales, para el funcionamiento de todo Sistema de Protección Criptográfica.

ARTICULO 7.-El Ministerio de las Fuerzas Armadas Revolucionarias adecuará la aplicación de las disposiciones sobre Criptografía y Servicios Cifrados propios en correspondencia con sus necesidades.

CAPITULO II
DE LA CRIPTOGRAFIA Y LOS SISTEMAS DE PROTECCION CRIPTOGRAFICA

ARTICULO 8.-Las acciones dirigidas a la divulgación, promoción, intercambio o enseñanza de disciplinas criptográficas, podrán realizarse sólo con la aprobación del Ministerio del Interior.

ARTICULO 9.-La organización de eventos nacionales e internacionales por los órganos, organismos o entidades cubanas o extranjeras radicadas en el país, así como la participación y presentación de ponencias, sobre temas de disciplinas criptográficas en éstos, requerirá la autorización del Ministerio del Interior, para lo cual el responsable de la organización del evento y el personal que presenta ponencias, presentarán la solicitud:

1. Para la autorización del evento, como mínimo con 60 días de anticipación a su convocatoria.
2. Para la presentación de ponencias, como mínimo 45 días antes de presentar su solicitud de participación como ponente.
3. El personal extranjero con el fin de presentar ponencias, personalmente o mediante el órgano, organismo o entidad que lo representa, como mínimo 60 días de anticipación al evento.

ARTICULO 10.-Toda persona natural o jurídica que esté interesada en divulgar, promocionar o publicar información de, o sobre los Sistemas de Protección Criptográfica, deberá estar autorizada por el Ministerio del Interior.

ARTICULO 11.-Todo órgano, organismo o entidad, para desarrollar la investigación, diseño, producción o comercialización de un Sistema de Protección Criptográfica, deberá estar autorizado por el Ministerio del Interior y cumplir los requerimientos establecidos por éste.

ARTICULO 12.-Se prohíbe utilizar algoritmos criptográficos no desarrollados por el Ministerio del Interior u otra entidad autorizada por éste.

ARTICULO 13.-La importación y comercialización de un Sistema de Protección Criptográfica, se realizará sólo a través de las entidades autorizadas por el Ministerio del Interior, el cual dictaminará y lo aprobará previamente.

ARTICULO 14.-El máximo dirigente del órgano, organismo o entidad con interés de establecer relaciones de colaboración en el campo de la Criptografía con otros países u organizaciones no gubernamentales internacionales, se hará sólo con la autorización del Ministerio del Interior, el cual de autorizarlo, establecerá su participación y el sistema informativo y de control a cumplimentar.

CAPITULO III
DEL SERVICIO CENTRAL CIFRADO

ARTICULO 15.-La seguridad y fiabilidad del Servicio Cifrado se garantiza con:

1. la fortaleza de los Sistemas de Protección Criptográfica que se utilicen;
2. el estricto cumplimiento de las normas y procedimientos de cada sistema;
3. la confiabilidad del personal que trabaja en la investigación y construcción de los Sistemas de Protección Criptográfica y en el Servicio Cifrado; y
4. la aplicación de un riguroso régimen especial de compartimentación, protección y control permanente.

ARTICULO 16.-La designación de los usuarios del Servicio Central Cifrado es facultad del Jefe del órgano, organismo, o entidad; el que presentará a la Dirección de Informática, Comunicaciones y Cifras del Ministerio del Interior, la solicitud e informará todo movimiento de cargo que demande la actualización de la relación de usuarios.

ARTICULO 17.-Todo dirigente o funcionario en viaje de trabajo al exterior, está en la obligación de emplear el Servicio Central Cifrado en las Misiones Estatales Cubanas en el exterior para la tramitación de información clasificada, para lo que su órgano, organismo o entidad les dará la preparación correspondiente y lo dotarán con el documento que lo autoriza ante el Jefe de la Misión para hacer uso del Servicio Cifrado. Los Jefes de Misiones garantizarán las facilidades para que se cumpla lo anterior.

ARTICULO 18.-Todos los documentos tramitados como mensajes por medio del Servicio Central Cifrado serán clasificados como "SECRETO", independientemente de su contenido y mantendrán la categoría de "SECRETO DE ESTADO" aquellos mensajes que excepcionalmente se transmitan con este grado de clasificación.

ARTICULO 19.-Los usuarios del Servicio Central Cifrado son responsables de la información contenida en los mensajes que envíen o reciban y, a los efectos de su tramitación y control, le otorgarán el tratamiento establecido para la documentación oficial clasificada.

ARTICULO 20.-Todo usuario del Servicio Central Cifrado al elaborar un mensaje para ser cifrado o al recibirlo está obligado a cumplir con los procedimientos establecidos por la Dirección de Informática, Comunicaciones y Cifras.

CAPITULO IV
SERVICIO CIFRADO DE USO PROPIO

ARTICULO 21.-Para la utilización de un Servicio Cifrado de Uso Propio, los máximos dirigentes de los órganos, organismos y entidades solicitarán su aprobación al Ministerio del Interior.

ARTICULO 22.-Todo órgano, organismo o entidad estatal para ser autorizado a utilizar un Servicio Cifrado de Uso Propio, deberá cumplir los requerimientos técnicos y de seguridad establecidos por la Dirección de Informática, Comunicaciones y Cifras, en correspondencia al Sistema de Protección Criptográfica a emplear.

ARTICULO 23.-Los Jefes de órganos, organismos o entidades, aprobarán al personal para la operación del Servicio Cifrado de Uso Propio, garantizando su idoneidad, control y evaluación sistemática.

ARTICULO 24.-La Dirección de Informática, Comunicaciones y Cifras del Ministerio del Interior, será la encargada de dictaminar sobre las condiciones técnicas y de seguridad de los locales destinados al funcionamiento de los Sistemas de Protección Criptográficos, de acuerdo con los requisitos establecidos.

CAPITULO V
DEL CONTROL

ARTICULO 25.-La organización y realización de los controles sobre el cumplimiento del Decreto-Ley, en lo referido al Servicio Cifrado, el presente Reglamento y demás normas complementarias sobre la materia, es responsabilidad del Ministerio del Interior.

ARTICULO 26.-Los controles se efectúan periódicamente y según los intereses del Ministerio del Interior. Estos se programan y comunican oportunamente, no obstante pueden realizarse de forma sorpresiva o ante la detección de violaciones.

ARTICULO 27.-Los controles tienen los objetivos siguientes:

1. evaluar el nivel de conocimiento y la aplicación de la base legal del Servicio Cifrado y la Criptografía;
2. verificar el cumplimiento de las medidas de seguridad y protección de los Sistemas de Protección Criptográfica que se emplean; y
3. valorar el cumplimiento de las normas y procedimientos del Servicio Central Cifrado y de Uso Propio.

ARTICULO 28.-Los funcionarios designados para la realización de los controles tienen las facultades siguientes:

1. Establecer las violaciones y vulnerabilidades detectadas;
2. proponer sanciones administrativas;
3. hacer evaluaciones, recomendaciones y disponer acciones correctivas ante violaciones; y
4. proponer la suspensión de los servicios cuando la violación ponga en peligro la información y el sistema.