HOJA DE REMISIÓN

CLASIFICACIÓN
ORDINARIO

A : LISTA DE DISTRIBUCIÓN

DE : SECRETARÍA DEL CONSEJO DE MINISTROS

ADJUNTO ENVIAMOS LOS SIGUIENTES DOCUMENTOS:

DECRETO NO. 360

CON EL OBJETIVO SIGUIENTE:

PARA SU INFORMACIÓN	X
PARA UNA PRÓXIMA REUNIÓN	
OTRO (VER MANDATOS)	

OBSERVACIONES:

Reg.: 827 - 0

FECHA		
D	M	A
6	6	19

EJECUTOR	APROBADO POR:
Jefa Grupo Asesoría Jurídica	José Amado Ricardo Guerra

HOJA DE REMISIÓN

CLASIFICACIÓN
ORDINARIO

A : DIRECCIÓN DE LEGISLACIÓN Y ASESORÍA

DE : SECRETARÍA DEL CONSEJO DE MINISTROS

ADJUNTO ENVIAMOS LOS SIGUIENTES DOCUMENTOS:

DECRETO NO. 360

CON EL OBJETIVO SIGUIENTE:

PARA SU PUBLICACIÓN [X]

OBSERVACIONES

Reg.: 8217 -0

FECHA		
D	M	A
6	6	19

EJECUTOR
Jefa Grupo Asesoría Jurídica

APROBADO POR:
José Amado Ricardo Guerra

HOJA DE DISTRIBUCIÓN DE DOCUMENTOS:	REGISTRO
DECRETO NO. 360	8217-D -O

	CONSEJO DE MINISTROS	
	COMITÉ EJECUTIVO	
	PRESIDENTE	
X	Miguel Díaz-Canel Bermúdez	
	PRIMER VICEPRESIDENTE	
X	Salvador Valdés Mesa	PVP CE
	VICEPRESIDENTES	
X	C. Rev. Ramiro Valdés Menéndez	BP y VPCE
X	Ricardo Cabrisas Ruiz	
X	Ulises Rosales del Toro	
X	Inés María Chapman Waugh	VP CE
X	Roberto Morales Ojeda	BP y VP CE
	SECRETARIO	
	Amado Ricardo Guerra	
	MINISTROS Y PRESIDENTES	
X	Rodrigo Malmierca Díaz	MINCEX
X	Irma Martínez Castrillón	BCC
X	Alejandro Gil Fernández	MEP
X	GCE Leopoldo Cintra Frías	MINFAR, MCE y BP
X	VA Julio C. Gandarilla Bermejo	MININT
X	José R. Saborido Loidi	MES
X	René Mesa Villafaña	MICONS
X	Margarita M. González Fernández	MTSS
X	Betsy Díaz Velázquez	MINCIN
X	Raúl García Barreiro	MINEM
X	Iris Quiñones Rojas	MINAL
X	Alfredo López Valdés	MINDUS
X	Gustavo Rodríguez Rollero	MINAG
X	José Angel Portal Miranda	MINSAP
X	Manuel Marrero Cruz	MINTUR
X	Meisi Bolaños Weis	MFP
X	Elba Rosa Pérez Montoya	CITMA
X	Alpidio Alonso Grau	MINCULT
X	Eduardo Rodríguez Dávila	MITRANS
X	Ena Elsa Velázquez Cobiella	MINED
X	Bruno E. Rodríguez Parrilla	MCE, BP y MINREX
X	José Luis Perdomo Di-Lella	MINCOM
X	Oscar Manuel Silveira Martínez	MINJUS
X	Antonio Eduardo Becali Garrido	INDER
X	Alfonso Noya Martínez	ICRT
X	Antonio Rodríguez Rodríguez	INRH
	Abel Prieto Jiménez	Asesor Pdte.CM
	CONSEJO DE ESTADO	
X	Homero Acosta Álvarez	Sec. CE
	Minerva Valdés Temprana	Jurídico
X	Gladys Bejerano Portela	CGR y VPCE
X	Yamila Peña Ojeda	FGR
X	Rubén Remigio Ferro	TSP
	José Miguel Miyar Barrueco	
	Ricardo Alarcón de Quesada	
	ANPP	
X	Esteban Lazo Hernández	Presid. y BP
	Ana María Mari Machado	Vicepres.
	Miriam Brito Sarroca	Secretaria

	OTRAS		
X	Julio Andrés García Pérez	AZCUBA	
X	Eduardo Martínez Díaz	BioCubaFarma	
X	Cor. Nelson Enrique Cordovés Reyes	AGR	
X	Samuel Rodiles Planas	IPF	
X	CA Luis Fernández Navarro	INRE	
X	Eusebio Leal Spengler	Hist LH	
X	Luis A. Rodríguez López-Callejas	GAE	
	Héctor Oroza Busutil	CIMEX	
	Otto Vaillant Frías	ESTI	
	Enith Alerm Prieto	Memorial JM	
	Yailin Orta Rivero	Dtor. Granma	
X	Ana Teresa Igarza Martínez	Of ZEDM	
	Ana Sánchez Collazo	C Est. Mart.	
X	Ramón Pardo Guerra	J´EMNDC	
	Caridad del R. Diego Bello	CC PCC Of. Asuntos Religiosos	
	Fabio Raimundo Torrado	CC PCC	
X	Marino Murillo Jorge	J¨ CPID	
	Leonardo Andollo Valdés	2 CPID	
	GD José J. Milián Pino	MININT	
	GCE Álvaro López Miera	BP y VMP J´EMG FAR	
	GCE Ramón Espinosa Martín	BP y VM FAR	
	GCE Joaquín Quintas Solá	VM FAR	
	Aymara Guzmán Carrazana	OPJM	
X	Miguel Mario Cabrera Castellanos	DC E y G	
X	Ulises Guilarte de Nacimiento	MCE BP CTC	
	Teresa Amarelle Boué	MCE, BP y FMC	
	José A. Carrillo Gómez	ACRC	
	Rafael Ramón Santiesteban Pozo	MCE ANAP	
	Susely Morfa González	MCE UJC	
	Carlos Rafael Miranda Martínez	MCE CDR	
	José R. Machado Ventura	2do Sec CC PCC	
	RESTO BURÓ POLÍTICO		
	Miriam Nicado García	UCI	
	SECRETARIADO CC PCC		
	Olga Lidia Tapia Iglesias		
	José R. Balaguer Cabrera		
	Omar Ruiz Martín		
	Jorge Cuevas Ramos		
	Abelardo Álvarez Gil		
	PRIMEROS SECRETARIOS PCC		
	Julio César Rodríguez Pimentel	Pinar del Río	
	Luis Antonio Torres Iribar	La Habana	
	Gladys Martínez Verdecia	Artemisa	
	Yanina de la Nuez Aclich	Mayabeque	
	Manuela Teresa Rojas Monzón	Matanzas	
	Julio Ramiro Lima Corzo	Villa Clara	
	Lidia Esther Bruner Nodarse	Cienfuegos	
	Deivy Pérez Martínez	Sancti Spíritus	
	Félix Duarte Ortega	Ciego de Ávila	
	Jorge Luis Tapia Fonseca	Camagüey	
	Ariel Santana Santiesteban	Las Tunas	
	Ernesto Santiesteban Velázquez	Holguín	
	Federico Hernández Hernández	Granma	
	Lázaro F. Expósito Canto	Santiago de Cuba	
	Rafael Pérez Fernández	Guantánamo	

	PRESIDENTES CAP	
X	Ernesto Barreto Castillo	Pinar del Río
X	Reinaldo García Zapata	La Habana
X	Tania León Silveira	Matanzas
X	Alberto López Díaz	Villa Clara
X	F. Mayerelis Pernia Cordero	Cienfuegos
X	Teresita Romero Rodríguez	Sancti Spíritus
X	Raúl Pérez Carmenate	Ciego de Ávila
X	Isabel González Cárdenas	Camagüey
X	Lilian González Rodríguez	Las Tunas
X	Julio César Estupiñan Rodríguez	Holguín
X	Manuel S. Sobrino Martínez	Granma
X	Beatriz Johnson Urrutia	Stgo Cuba VPCE
X	Nancy Acosta Hernández	Guantánamo
X	Arelys Casañola Quintana	I Juventud
	JEFES DE ADMINISTRACIÓN PROVINCIAL	
X	Teresa Martínez Mendaro	Artemisa
X	Julio César García García	Mayabeque
	PRESIDENTES APPP	
	Juan Domínguez Miranda	Artemisa
	Tamara Valido Benítez	Mayabeque
	SECRETARÍA CM	
	Marcia Fernández Andreu	¨Vicejefe
	Juan Carlos García Granda	Vicejefe y J¨¨UPSI
	Norberto Gibert Montano	¨Vicejefe y J¨Planif
	Juan L. Fernández Delgado	
	Caridad Rodríguez Álvarez	
	María de los A. Peñate	
X	Niurka Álvarez Vila	
	Emilia Herrera Mendoza	
X	Elisita Estremera Deniz	
X	Lázaro Chávez Novo	
	Eduardo Normand Cabrera	
X	Mercedes Linda Puentes Trillo	
X	María Eugenia Llanusa Ruiz	
	Elba Martínez Amador	
X	Iliana García Savigne	
	Yohanka Miranda Mariño	
X	Benigno Corrales Pérez	
X	Manuel T. Soengas Domínguez	
X	Graciel Rodríguez Rodríguez	
	Orlando Martínez Obeso	
	Norma Reyes Moreno	
X	Jorge F. Lefebre Nicolas	
X	Boris Jiménez Rojas	
	Juan Hernández Leal	
	Marilín Rodríguez Rodríguez	
	Sergio Ramón Ricaño Pérez	
	Darío Delgado Cura	Asesor CM
	Maimir Mesa Ramos	Asesor CM
	Miguel M. Cabrera Castellanos	Dir Cuadros
	Abraham Maciques Maciques	PALCO
X	Juana M. Pantoja Hernández	ONEI
	Eduardo Acén Comas	J´ Of. Viviendas CM
	OCIC Secretaría	

HECHO POR: GRUPO ASESORÍA JURÍDICA — FECHA:31.5.19

República de Cuba
Consejo de Ministros
Secretaría

El Secretario del Consejo de Ministros

CERTIFICA

Que el Consejo de Ministros, en el ejercicio de las atribuciones que le otorgan los incisos ñ) y o) del Artículo 137 de la Constitución de la República de Cuba, y de conformidad con el Artículo 30 del Decreto-Ley No. 272 "De la Organización y Funcionamiento del Consejo de Ministros", del 16 de julio de 2010, adoptó con fecha 31 de mayo de 2019, el Decreto No. 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional".

Y PARA PUBLICAR en la Gaceta Oficial de la República de Cuba y remitir copia a los miembros del Consejo de Ministros, extiendo y firmo la presente certificación, en el Palacio de la Revolución, a los 31 días del mes de mayo de 2019. "AÑO 61 DE LA REVOLUCIÓN".

José Amado Ricardo Guerra

PARA CONTROL ADMINISTRATIVO
Decreto No. 360
Seguridad TIC y Defensa del
Ciberespacio Nacional
/CMEB
RS: 8217-0

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente de los consejos de Estado y de Ministros de la República de Cuba.

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

POR CUANTO: El Decreto-Ley No. 370 "Sobre la Informatización de la Sociedad en Cuba", del 17 de diciembre del 2018, en su Disposición Final Primera establece que el Consejo de Ministros queda encargado de dictar las disposiciones complementarias sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

POR CUANTO: El referido Decreto-Ley No. 370, dispone las regulaciones generales aplicables a las Tecnologías de la Información y la Comunicación (TIC) y recoge los principios a seguir y las acciones y medidas para la determinación, desarrollo y mejoramiento de las condiciones de fiabilidad, estabilidad y seguridad de las TIC que respalden la informatización de la sociedad y la soberanía de la nación, la investigación, el desarrollo, la asimilación tecnológica y los soportes de soluciones para su seguridad de forma sostenible; acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias.

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 NO. 360

SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA DEL CIBERESPACIO NACIONAL

CAPÍTULO I
OBJETO, OBJETIVOS, DEFINICIONES Y ÁMBITO DE APLICACIÓN

Artículo 1. El Estado moviliza los recursos necesarios para lograr el empleo seguro y eficiente de las Tecnologías de la Información y la Comunicación en función de las necesidades que requiere el desarrollo del país; además, en su papel rector de la sociedad, dirige la implementación de la estrategia aprobada en materia de Seguridad de las Tecnologías de la Información y la Comunicación y controla su cumplimiento, así como promueve la investigación, el desarrollo, la aplicación, la innovación, la divulgación y la capacitación.

Artículo 2. El objeto del presente Decreto es establecer el marco legal que ordene el empleo seguro de las Tecnologías de la Información y la Comunicación, en lo adelante TIC, para la informatización de la sociedad, la defensa del Ciberespacio Nacional en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los tratados y demás instrumentos jurídicos internacionales de los que la República de Cuba es Estado parte.

Artículo 3. El objetivo general de este Decreto es establecer los niveles de seguridad en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de enfrentar estos últimos, y tiene los objetivos específicos siguientes:

a) Proteger el Ciberespacio Nacional y preservar la soberanía sobre su utilización;

b) establecer la seguridad de las TIC y de los servicios y aplicaciones que soportan; así como la de las Infraestructuras Críticas de las TIC con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.

Artículo 4. El Ciberespacio es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones, que interactúan entre sí y con las personas, y en el que la información se crea, procesa, almacena y transmite.

Artículo 5. La Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio.

En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia.

Artículo 6. La situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema se denomina amenaza.

Artículo 7. Se denomina ataque al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad.

Artículo 8. Se identifica como riesgo a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización.

Artículo 9. La vulnerabilidad se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema.

Artículo 10. El presente Decreto es de aplicación a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, el sistema empresarial y las unidades presupuestadas, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales.

Artículo 11. Constituyen premisas de la seguridad de las TIC para la informatización de la sociedad y la defensa del Ciberespacio Nacional las siguientes:

a) Elevar la Ciberseguridad frente a las amenazas, los ataques y riesgos a los que se exponen las TIC;

b) garantizar que todos los activos de las TIC sean gestionados de acuerdo con los estándares y buenas prácticas en seguridad;

c) aumentar el nivel de atención a la seguridad de las TIC y garantizar que el personal vinculado a estas domine sus deberes y responsabilidades;

d) establecer las bases de un modelo integral de gestión de la seguridad que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales;

e) garantizar el cumplimiento de la legislación vigente en materia de seguridad de las TIC;

f) elevar la seguridad de las TIC mediante el desarrollo de la industria nacional de programas y aplicaciones informáticas;

g) potenciar la preparación de los profesionales de las TIC, la preservación de estos y el desarrollo integral del capital humano asociado a la actividad;

h) concebir la seguridad en todas las etapas de desarrollo e implantación de las TIC;

i) garantizar la seguridad y resiliencia de las redes y los sistemas de información empleados en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular;

j) posibilitar la integración de la investigación, desarrollo e innovación con la producción y comercialización de productos, tecnologías y servicios de seguridad; y

k) promover la cooperación e intercambio internacional en función de la Ciberseguridad y la gobernanza de Internet.

Artículo 12. La Seguridad de las TIC es el conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC; el empleo del término seguridad informática, tiene igual significado.

CAPÍTULO II
SISTEMA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Sección Primera
Estrategia y Planificación

Artículo 13. El Sistema de Seguridad de las TIC es el conjunto de medios humanos, técnicos y administrativos que, de manera interrelacionada garantiza diferentes grados de seguridad informática, en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

Artículo 14. El Sistema de Seguridad de las TIC se constituye a partir de los sistemas de seguridad existentes en las instituciones del país que posean o utilicen las TIC, en interés propio o de terceros, e incluye:

a) Operadores de redes de telecomunicaciones, en lo adelante operadores;

b) proveedores de servicios públicos y privados de acceso a Internet;

c) productor de equipos;

d) proveedor de servicios de red;

e) proveedores de servicios de las TIC;

f) usuarios de las TIC; y

g) entidades encargadas de la dirección, el control y la supervisión de la seguridad de las TIC, así como de las actividades relacionadas con la vigilancia tecnológica, la alerta temprana y la gestión de incidentes.

Artículo 15. Los mecanismos de seguridad comprenden la implementación de hardware o software diseñados o construidos para prevenir, detectar o responder a incidentes de seguridad.

Artículo 16. Se considera un incidente de seguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan.

Artículo 17. Cada entidad que haga uso de las TIC diseña, implanta, gestiona y mantiene actualizado un Sistema de Seguridad, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos.

Artículo 18. A partir del Sistema de Seguridad diseñado, cada entidad elabora su Plan de Seguridad de las TIC.

Artículo 19. El diseño del Sistema de Seguridad de las TIC y la elaboración del Plan de Seguridad de cada entidad se realizan en correspondencia con las metodologías establecidas al respecto por el Ministerio de Comunicaciones.

Artículo 20. El Plan de Seguridad de las TIC de una organización es el documento que incluye, describe y aplica las políticas, medidas y procedimientos diseñados para esta a partir de los riesgos estimados, así como establece las responsabilidades de los diferentes actores que participan en su ejecución.

Artículo 21. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y en aquellas entidades en que la cantidad, diversidad e importancia de las TIC lo requieran, según el análisis que para ello se realice, disponen de los cargos de especialistas de seguridad de las TIC que garanticen la atención de esta actividad.

Artículo 22. Los usuarios de las TIC asumen, en primera instancia, la responsabilidad de las consecuencias que se deriven de su utilización impropia.

Sección Segunda
Organización institucional, competencias y atribuciones

Artículo 23. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, el sistema empresarial y demás entidades, de acuerdo con su misión y funciones específicas, desarrollan las acciones que se establecen mediante el presente Decreto, en el marco del proceso de Informatización de la Sociedad Cubana.

Artículo 24. El Ministerio de Comunicaciones controla a todos los niveles de dirección de los organismos de la Administración Central del Estado y de las demás personas jurídicas, el cumplimiento de las normas de seguridad de las TIC, excepto aquellos que se determinen por ese propio Ministerio.

Artículo 25. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, establece las normas de seguridad de las TIC y se responsabiliza por la ejecución de las acciones siguientes:

a) Desarrollar y modernizar la infraestructura vinculada a la seguridad de las TIC para incrementar la efectividad en la protección del Ciberespacio Nacional mediante un enfoque sistémico, conceptual y organizativo;

b) impulsar la cooperación internacional y coordinar la participación en eventos que permitan adoptar normas globales para el desarrollo de la Seguridad de las TIC, así como defender la posición del país en materia de Ciberseguridad;

c) suscribir convenios que contribuyan a desarrollar soluciones de seguridad, ampliar el acceso y la transferencia del país a nuevas tecnologías, preparar el capital humano y contribuir al enfrentamiento de las amenazas en el plano internacional;

d) establecer el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad y asegurar los procedimientos para su implementación en todos los niveles por parte de los órganos,

organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, así como realizar el enfrentamiento y neutralización de estos sucesos atendiendo a lo que a cada organismo le corresponde;

e) establecer un sistema de trabajo entre las entidades especializadas en seguridad de las TIC que garantice el cumplimiento de sus funciones en el intercambio seguro de información relativa a vulnerabilidades e incidentes de Ciberseguridad, la colaboración y la coordinación entre sí, con el empleo de servicios seguros de voz, videoconferencia y datos;

f) organizar y potenciar de modo sostenible la investigación, el desarrollo, la innovación y el soporte tecnológico, en función de los sistemas para la Seguridad de las TIC;

g) perfeccionar y potenciar la supervisión, certificación, homologación y acreditación de las soluciones, servicios y la infraestructura tecnológica vinculados a la seguridad de las TIC;

h) asimilar y recibir transferencia tecnológica de las infraestructuras técnicas y organizacionales, de hardware y software, en centros de investigación para la seguridad, parques científicos-tecnológicos, los sistemas operativos, los equipos de cómputo y los relacionados con la conectividad;

i) diseñar e implementar acciones de inspección, asistencia, consultoría y auditoría, de la seguridad de las TIC; así como para su control, en correspondencia con la categorización de los sistemas y actividades;

j) ejercer la fiscalización de la seguridad de las TIC;

k) fortalecer la estrategia de desarrollo del antivirus nacional;

l) garantizar el desarrollo de las actividades que los ministerios de las Fuerzas Armadas Revolucionarias y del Interior realizan para la supervisión y el control de los servicios de las TIC;

m) adquirir, asimilar y desarrollar equipamientos y soluciones para la supervisión y control de servicios y aplicaciones con impacto en la Seguridad Nacional;

n) instrumentar los mecanismos que organicen e incentiven la cooperación internacional en función del desarrollo de soluciones y tecnologías de seguridad en el territorio nacional;

o) garantizar el desarrollo de las actividades de supervisión y control de los servicios de las TIC;

p) perfeccionar de forma ordenada los sistemas y mecanismos de supervisión y control existentes sobre las TIC que utilizan el espectro radioeléctrico, así como garantizar la compatibilidad electromagnética y su uso seguro;

q) establecer los requerimientos básicos para las aplicaciones informáticas destinadas a la gestión de incidentes de Ciberseguridad;

r) organizar y controlar la protección de las principales redes informáticas y sistemas de trabajo que generan servicios de esta naturaleza, que constituyen Infraestructuras Críticas de las TIC, para dotarlas del nivel de seguridad en correspondencia con su categoría;

s) certificar la seguridad de las Infraestructuras Críticas de las TIC;

t) establecer e implementar el Sistema Nacional de Certificación de la Seguridad de las TIC y los laboratorios de certificación para evaluarla, en correspondencia con la categorización de los sistemas y actividades;

u) implementar y potenciar la Red de Gobierno con los requerimientos disponibles de máxima seguridad;

v) incrementar y fortalecer mecanismos de seguridad que permitan detectar y prevenir actividades nocivas en las redes informáticas de los operadores, así como en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y demás entidades;

w) desarrollar e implementar proyectos propios de soluciones integrales, telemática, protección técnica integral y canales colaterales, programas y aplicaciones informáticas básicas, protección de activos digitales, licenciamiento y las soluciones para la Seguridad y Defensa

Nacional y el Orden Interior, en correspondencia con la categorización de los sistemas y actividades;

x) desarrollar entrenamientos de Ciberseguridad en los ejercicios que se ejecuten para elevar la defensa del país en el Ciberespacio y comprobar la efectividad de los planes orientados a dar respuesta a incidentes de Seguridad de las TIC; e

y) incrementar la calidad de la gestión del capital humano especializado en la Seguridad de las TIC.

Artículo 26. El Ministerio de Comunicaciones, de conformidad con sus atribuciones y funciones específicas, es el responsable de las actividades siguientes:

a) Fortalecer la infraestructura de seguridad en las redes informáticas;

b) establecer y controlar la implementación de configuraciones básicas de seguridad orientadas al fortalecimiento de las aplicaciones y equipos que operan en el perímetro de las redes informáticas de las entidades;

c) adquirir y desarrollar equipamientos y programas informáticos especializados para el procesamiento y almacenamiento de las evidencias digitales relacionadas con incidentes de Ciberseguridad;

d) facilitar el hospedaje de los servicios de las entidades estatales y del sector no estatal en los centros de datos públicos para garantizar la racionalidad de las infraestructuras de seguridad y su despliegue y minimizar su diseminación;

e) perfeccionar el marco legal con la finalidad de sustentar la seguridad de las TIC en la informatización de la sociedad para establecer interoperabilidad, integridad, confidencialidad, disponibilidad y no repudio de la información;

f) establecer los mecanismos a emplear para la prevención y respuesta a incidentes de seguridad informática que involucren las TIC ubicadas en los hogares y las áreas públicas para el acceso al ciberespacio, por parte de las personas naturales y jurídicas; y

g) garantizar la recopilación de los incidentes de Ciberseguridad que se detecten.

Artículo 27. El Ministerio del Interior, de conjunto con el Ministerio de las Fuerzas Armadas Revolucionarias, de acuerdo con sus funciones específicas, es responsable de fortalecer los mecanismos de seguridad que permitan detectar y prevenir actividades enemigas y delictivas en las redes informáticas de los operadores, así como en las entidades.

Artículo 28. El Ministerio del Interior en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y de Comunicaciones, realiza las acciones siguientes:

a) Organizar actividades para fortalecer la recopilación y el análisis nacional sobre Seguridad de las TIC; y

b) establecer la gestión de identidad como parte indispensable del proceso de registro y validación, en correspondencia con la legislación vigente.

Artículo 29. El Ministerio de las Fuerzas Armadas Revolucionarias, en coordinación con los ministerios del Interior y de Comunicaciones, mantiene actualizado el Procedimiento para la Compatibilización con la Defensa de los servicios, tecnologías e inversiones vinculadas a las TIC.

Sección Tercera
Del empleo seguro de las Tecnologías de la Información y la Comunicación

Artículo 30. La seguridad de la información oficial se rige por la legislación vigente que regula lo relativo a su protección, en cualquier soporte en el que se encuentre.

Artículo 31. Los requerimientos de seguridad para la proyección, diseño e instalación de locales tecnológicos en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, se establecen según lo dispuesto en la legislación vigente.

Artículo 32. Los ministerios del Interior y de Justicia, de acuerdo con sus funciones, son los encargados de regular y controlar la protección de la información correspondiente a las personas naturales y jurídicas y la privacidad de los datos personales.

Artículo 33. La entidad que por sus funciones posea o controle datos de las personas naturales o jurídicas es responsable de la protección de la información personal y la privacidad de los documentos y únicamente facilita a las autoridades competentes la supervisión y acceso a estos datos personales, en correspondencia con la legislación vigente.

Artículo 34. El que haga uso, procese, trasmita y almacene información de personas naturales y jurídicas, lo realiza bajo los principios de legalidad, propiedad y necesidad e indica, de forma explícita, a estas personas los objetivos y el alcance, y han de tener su consentimiento cuando se requiera.

Artículo 35. Las reglas para la recopilación y el uso de la información tienen carácter público y se divulgan de forma oportuna y precisa para garantizar el conocimiento por las personas naturales y jurídicas.

Artículo 36. Se consideran bienes informáticos a los elementos que componen el sistema informático que son protegidos para evitar que sufran algún tipo de daño, como resultado de la materialización de una amenaza.

Artículo 37. Los bienes informáticos de una entidad son utilizados en las funciones propias del trabajo, así como en tareas autorizadas por la dirección de esta.

Artículo 38. Todos los bienes informáticos de una entidad se identifican y controlan, para lo cual se conforma y mantiene actualizado su estado físico, incluidos sus componentes y las especificaciones técnicas de aquellos que pudieran ser sustituidos.

Artículo 39. Es un deber y un derecho de la dirección de la entidad el control y supervisión del correcto empleo de las TIC por parte de los usuarios y su uso no autorizado es sancionable según la legislación vigente.

Artículo 40. Los jefes a cada nivel garantizan que el personal vinculado a las TIC esté capacitado para su utilización, que conozca los deberes y derechos en relación con el Sistema de Seguridad Informática, así como que exista constancia del conocimiento y compromiso que asume este personal de forma individual.

Artículo 41. El Ministerio de Comunicaciones otorga una licencia de operación a las entidades que pueden brindar servicios de seguridad de las TIC a terceros.

Artículo 42. El acceso del personal a las facilidades de procesamiento y a los servicios que brindan las tecnologías requiere de autorización expresa y de un control estricto de su uso por la dirección de cada entidad, las que establecen los requerimientos específicos para garantizar la seguridad, a partir de los riesgos que esto pueda introducir.

Artículo 43. La unidad organizativa que corresponda en cada entidad, de acuerdo con su estructura, exige a los usuarios de las TIC el cumplimiento de la información inmediata de cualquier incidente de seguridad, debilidad o amenaza a los sistemas y servicios con que opera.

Artículo 44. Se denomina Barrera de Protección al dispositivo físico o lógico utilizado para proteger un sistema informático o red de telecomunicaciones y obstaculizar el acceso a estos o entre sus componentes, ya sea de forma directa o remota.

Artículo 45. La dirección de cada entidad determina aquellos equipamientos de las TIC que por las funciones a las que se destinan, la información que contengan y las condiciones de los locales en que se encuentran ubicados, requieren la aplicación específica de medidas especiales de protección física y asegura una barrera de protección a estos medios que impida su empleo en la comisión de hechos intencionales que violen lo establecido o en actividades delictivas.

Artículo 46. El Ministerio de Comunicaciones ejecuta periódicamente las acciones de control a la seguridad de las TIC siguientes:

a) Realizar diagnósticos integrales en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, tanto tecnológicos como organizativos, que permitan evaluar el estado de la seguridad de las TIC e implementar acciones correctivas para su solución;

b) evaluar sistemáticamente las condiciones de seguridad de las aplicaciones informáticas, tanto en su codificación y despliegue como en la ejecución y trazabilidad de las operaciones realizadas; y

c) diseñar y establecer los mecanismos de comprobación de la Seguridad de las TIC que se utilizan por las personas naturales y jurídicas para acceder al ciberespacio.

Artículo 47. En cada entidad se implementan los controles y procedimientos que los protegen contra programas malignos, con el fin de mitigar sus efectos nocivos e impedir su generalización; para la protección contra virus informático se utilizan los programas antivirus de producción nacional y otros autorizados para su uso en el país, con un soporte establecido que permita su actualización.

Artículo 48. El Virus Informático es el programa capaz de reproducirse a sí mismo sin que el usuario esté consciente de ello; se adiciona a programas de aplicación, así como a componentes ejecutables del sistema, de forma tal que pueda tomar el control de este durante la ejecución del programa infectado.

Artículo 49. Queda prohibido el envío de mensajes masivos que:

a) Sean no deseados (Spam); que se entiende por toda información de voz o datos transmitida o enviada de forma masiva, indiscriminada y repetitivamente por medio de las redes de telecomunicaciones, sin el previo consentimiento de sus destinatarios.

b) no contenga, sea falso u oculto el asunto y la dirección o ubicación física o electrónica, número telefónico, identidad u otro medio de identificación del emisor e impidan a los destinatarios o receptores notificar su voluntad de no recibir más mensajes o no incluyan mecanismos que permitan al receptor manifestar su voluntad de no recibirlos;

c) afecten el uso seguro y la calidad de las redes de telecomunicaciones de Cuba o de otros países o de los servicios que se prestan a través de estas; y

d) posean un contenido que transgreda lo establecido en la legislación vigente cubana o los tratados, convenios o cualquier otro instrumento jurídico de carácter internacional de los que la República de Cuba es Estado parte.

Artículo 50. Los mensajes que contengan las características referidas en el Artículo anterior se consideran mensajes masivos dañinos.

Artículo 51. Corresponde a los operadores y proveedores:

a) Bloquear el envío, recepción o transmisión de los mensajes masivos dañinos que se cursan por sus redes y utilizan sus servicios;

b) suspender temporalmente por hasta un mes las comunicaciones entre sus redes y las que se establecen con las redes de operadores o proveedores extranjeros que no adopten las medidas necesarias para impedir el tráfico de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, dar cuenta al Ministerio de Comunicaciones; y

c) suspender temporalmente por hasta un mes el servicio prestado a los usuarios responsables del envío de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, da cuenta al Ministerio de Comunicaciones, a los órganos del Ministerio del Interior o de la Fiscalía General de la República.

Artículo 52.- En los contratos suscritos por los operadores y proveedores entre sí y con sus usuarios, se incluye una cláusula sobre la responsabilidad derivada del envío de mensajes masivos dañinos a través de las redes de telecomunicaciones con utilización de las TIC o de los equipos terminales de telecomunicaciones que son objeto de control por el Ministerio de Comunicaciones y, ante su incumplimiento, se le aplican las medidas previstas en la legislación vigente.

Artículo 53. Es responsable del envío de mensajes masivos dañinos toda persona natural o jurídica que:

a) directamente los envíe;

b) los genere a través de los equipos de telecomunicaciones de otras personas;

c) los transporte o intermedie en su difusión o trasmisión o haya incidido en su contenido, si mediante sus medios técnicos lo hubiese conocido y no evita su transportación, difusión, trasmisión, envío y reenvío; y

d) cree, venda, preste, intercambie o realice cualquier tipo de recolección o transferencia de listas de direcciones de correo electrónico, números telefónicos u otro medio de identificación del emisor que haya sido realizada sin la autorización o consentimiento de su titular o del operador o proveedor de los servicios y sean conformadas para el envío de mensajes masivos dañinos.

Sección Cuarta
De la Seguridad de las Operaciones

Artículo 54. La seguridad de las operaciones realizadas sobre las TIC es garantizada por la protección desplegada de seguridad de la red por niveles para evitar interferencias, daños o accesos no autorizados, fugas de datos, robos o falsificación.

Artículo 55. Se denomina traza al registro cronológico de las acciones que se realizan en un sistema, el acceso a este y los procesos y ficheros que han intervenido.

Artículo 56. Los proveedores de servicio de acceso a Internet, para garantizar la seguridad de sus operaciones, cumplen con los deberes siguientes:

a) elaborar procedimientos de operación y gestión de seguridad internos;

b) determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan;

c) adoptar medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;

d) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos;

e) establecer el registro y la trazabilidad de las operaciones realizadas, así como el control de los eventos e incidentes, en correspondencia con las regulaciones vigentes;

f) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles y el cifrado; y

g) establecer la obligatoriedad de las personas naturales y jurídicas de preservar las trazas de los servicios utilizados para acceder al ciberespacio.

Artículo 57. Los responsables de la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad, cumplen con la legislación vigente relativa a los requerimientos de la Seguridad y Defensa Nacional; los requisitos establecidos en las normas nacionales son evaluados por la entidad autorizada por el Ministerio de Comunicaciones a través de la implementación de las medidas siguientes:

a) Establecer un catálogo de equipos y servicios especializados de seguridad considerados como críticos; y

b) promover el reconocimiento recíproco, entre las entidades especializadas en seguridad de las TIC, de certificaciones de seguridad y los resultados de controles, inspecciones y auditorías, para evitar la duplicación de esfuerzos.

Artículo 58. Al determinar las responsabilidades asignadas al personal que labora en las áreas relacionadas con la seguridad informática, se tiene en cuenta el principio de separación de funciones y se especifican las tareas que no pueden ser ejecutadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada, o uso inadecuado de los sistemas de las TIC.

Artículo 59. El jefe de la entidad es el responsable de la introducción de los servicios de las TIC, actualizaciones y nuevas versiones, en correspondencia con el sistema de seguridad establecido y los resultados de las pruebas realizadas, para determinar si cumple los criterios de seguridad apropiados.

Artículo 60. Los sistemas informáticos en que es posible el acceso por múltiples usuarios disponen de un identificador de usuario personal y único; y las personas a las que se le asignen identificadores de usuarios responden por las acciones que con ellos se realicen; en caso del cese de la relación laboral u otras causas que se determine por la dirección de la entidad se procede a eliminar el identificador del usuario; en todos los casos se preservan las trazas de uso de las credenciales de acceso, por un tiempo no menor de un año.

Artículo 61. La entidad establece un procedimiento para la asignación de los identificadores de usuarios en los sistemas, que incluye en el caso de los nuevos la solicitud previa al jefe inmediato superior y su posterior notificación al interesado.

Artículo 62. La entidad implementa un sistema fiable de respaldo de la información esencial para su funcionamiento, que permita su recuperación después de un ataque informático, desastre o fallo de los medios, para ello ejecuta los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

Artículo 63. La información de respaldo, conjuntamente con informes precisos y completos de sus copias y los procedimientos de recuperación documentados, se almacenan en otra ubicación, que le permita no afectarse en caso de desastre en la ubicación principal.

Artículo 64. La información de respaldo requiere una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal; los controles realizados a los medios en la ubicación principal se extienden a los medios de respaldo.

Artículo 65. Los medios de respaldo se prueban regularmente y se verifica el estado de actualización de la información almacenada, con el fin de asegurar la confiabilidad en ellos para un uso de emergencia, cuando sea necesaria la ejecución de un proceso de recuperación.

Artículo 66. El jefe de la entidad establece la utilización obligatoria del antivirus nacional y su despliegue en la red privada.

Artículo 67. El Ministerio de Comunicaciones aprueba la utilización de un antivirus extranjero para su uso en el país, cuando este se justifique, y promueve el fortalecimiento del motor del antivirus nacional a partir de la asimilación de otros motores de antivirus.

Artículo 68. El Ministerio de Comunicaciones promueve el desarrollo y la comercialización de los servicios de instalación y actualización del antivirus nacional y las licencias para su uso por las personas naturales y jurídicas.

Artículo 69. La entidad puede adquirir la infraestructura y el equipamiento especializado necesario para la captura de muestras de programas malignos que incorpora a la base de datos del antivirus nacional.

Artículo 70. El Ministerio de Comunicaciones, en coordinación con los Ministerios de Educación y Educación Superior, diseña e implementa proyectos de investigación y desarrollo sobre la seguridad de las TIC en colaboración con centros académicos y de investigación del país, dentro de los que se incluyen los de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior.

Sección Quinta
De la seguridad en el empleo de las redes

Artículo 71. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de conjunto con los ministerios de Economía y Planificación y el de Finanzas y Precios, evalúan el respaldo financiero para incrementar la Seguridad de las TIC en las redes informáticas, de manera estable y sostenida, a partir de considerar la importancia de la información y los servicios que sustentan, el que se define en el Plan anual de la Economía.

Artículo 72. En todas las redes de datos se habilitan las opciones de seguridad con que cuentan los sistemas operativos, de forma tal que garanticen la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan la supervisión y auditoría de los principales eventos por un tiempo no menor de un año.

Artículo 73. El jefe del área o de la unidad organizativa que atiende las TIC responde por la implementación y ejecución de los procedimientos y normas que garanticen el empleo seguro de las TIC de forma general y la protección de la seguridad de la red por niveles para evitar interferencias, daños o accesos no autorizados, fugas de datos, robos o falsificación de forma particular; para lograr este objetivo tiene las responsabilidades siguientes:

a) determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan, así como aquellos que permitan filtrar o depurar la información que se intercambie.

b) adoptar las medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;

c) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos; y

d) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles, el cifrado y las trazas de los servicios utilizados para acceder al ciberespacio por parte de las personas naturales y jurídicas.

Artículo 74. El jefe del área o de la unidad organizativa que atiende las TIC asegura la instalación de las herramientas de seguridad autorizadas por el Ministerio de Comunicaciones para la fiscalización y la supervisión del empleo de las redes de datos y de los servicios implementados.

Artículo 75. La arquitectura y la configuración de los diferentes componentes de seguridad de una red de datos y la implementación de sus servicios están en correspondencia con el Plan de Seguridad de las TIC, y en ningún caso son el resultado de la iniciativa de una persona, con independencia de la preparación que posea.

Artículo 76. Toda red de datos requiere para su operación de la presencia de, al menos, una persona encargada de su administración.

Artículo 77. La gestión de administración de las redes de datos implica la concesión de privilegios requeridos para la tarea que cumple, los que se realizan directamente desde el puesto de trabajo que ocupe; se prohíbe la administración remota de estas redes de datos a través de redes públicas sin mecanismos criptográficos autorizados por los organismos competentes.

Artículo 78. Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las redes son responsables de su propia conducta; para ello conocen y cumplen los planes de seguridad de las TIC.

Artículo 79. Los jefes de las redes de datos o equipos que prevean conexiones desde o hacia el exterior de una entidad, instalan los medios técnicos que aseguren una barrera de protección entre las TIC de la entidad de que se trate y la red externa, con los mecanismos de seguridad que sea necesario implementar.

Artículo 80. La dirección de la entidad instrumenta la ejecución de procedimientos periódicos de verificación de la seguridad de sus redes de datos, con la finalidad de detectar posibles vulnerabilidades, incluido para ello, cuando sea procedente y debido a la sensibilidad de estas acciones, la comprobación de forma remota por entidades autorizadas oficialmente.

Artículo 81. El jefe del área o de la unidad organizativa que atiende las TIC que coloque información en servidores para su acceso público establece las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con sus intereses y los del país.

Artículo 82. Cuando por necesidades de conectividad u otros intereses, la entidad requiere hospedar un sitio en servidores ubicados en un país extranjero, esto se realiza como espejo o réplica del sitio principal en servidores ubicados en Cuba y se establecen las medidas requeridas para garantizar su seguridad, en particular durante el proceso de actualización de la información.

Artículo 83. Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior y los de uso interno deben estar instalados en zonas diferentes de la red, de forma tal que evite la conexión entre estos.

Artículo 84. La dirección de la entidad autoriza el acceso de su personal a Internet y los servicios asociados a este, en correspondencia con sus intereses y necesidades, según las normas particulares establecidas para estos servicios, y documenta esta autorización de manera que pueda ser objeto de comprobación.

Artículo 85. Las redes proveedoras de servicios han de tener las medidas que se requieran para impedir la sobrecarga de los canales de comunicaciones, restringir el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples destinatarios.

Artículo 86. La dirección de la entidad implementa controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

Artículo 87. La dirección de una entidad con redes de datos destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas, cumple los requisitos siguientes:

a) establecer las medidas y procedimientos de seguridad de las TIC que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que los reciben;

b) implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año;

c) informar a los clientes de estos servicios los requerimientos de seguridad informática que tienen que cumplir, en correspondencia con el Plan de Seguridad de las TIC establecido en la red que los brinda; y

d) facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

Artículo 88. La entidad autorizada es la única que puede explorar o monitorear las redes públicas de transmisión de datos, en busca de vulnerabilidades o información sobre sus usuarios.

Artículo 89. Los productores de equipos, los proveedores de servicios de red y de programas, aplicaciones y servicios informáticos, tanto nacionales como extranjeros, responden por la implementación de los requerimientos que garanticen el empleo seguro de los equipos y servicios que suministran.

Artículo 90. Las personas naturales o jurídicas, nacionales y extranjeras, usuarios de las TIC, responden por la utilización adecuada de los servicios y productos que emplean.

Artículo 91. Los cables de alimentación o de comunicaciones de las redes que transporten datos o apoyen los servicios de información se protegen contra la intercepción o el daño; el tendido de los cables de alimentación eléctrica se realiza de acuerdo con las normas establecidas a esos efectos, separados adecuadamente de los de comunicaciones para evitar posibles interferencias.

Artículo 92. El jefe de cada entidad garantiza que la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad se realicen en correspondencia con los requerimientos de la seguridad y defensa nacional, y que cumplan los requisitos establecidos en estándares nacionales elaborados a esos efectos y que sean aprobados por una entidad autorizada.

Artículo 93. La entidad aprobada por la autoridad competente para la creación de productos o soluciones informáticas, que implementan herramientas criptográficas, se rige por la legislación vigente.

Sección Sexta
Gestión de incidentes de seguridad

Artículo 94. La gestión de incidentes es el proceso que se realiza con el objetivo de prevenir, detectar y enfrentar los de Ciberseguridad y

comprende las acciones que se realizan antes, durante y después de su ocurrencia.

Artículo 95. El jefe de la entidad dispone de las medidas y procedimientos que garanticen la continuidad, el restablecimiento y la recuperación de los procesos informáticos, como respuesta a incidentes de Ciberseguridad y en correspondencia con el Modelo de Actuación Nacional.

Artículo 96. Las medidas y procedimientos de recuperación son definidos a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos e incluyen las acciones de respuesta, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

Artículo 97. Los procedimientos para la gestión de incidentes y violaciones de Seguridad de las TIC especifican la obligación de informar su ocurrencia y los pasos a seguir para garantizar una correcta evaluación de lo sucedido, a quién, cómo y cuándo se reporta la respuesta, los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Artículo 98. El Ministerio de Comunicaciones potencia la incorporación del Equipo de Respuesta a Incidentes Computacionales de Cuba a los mecanismos regionales e internacionales que agrupan a ese tipo de organizaciones.

CAPÍTULO III
INFRAESTRUCTURAS CRÍTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 99. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, es el responsable de elaborar y actualizar el Catálogo Nacional de Infraestructuras Críticas de las TIC y el Plan Nacional para la Protección de las Infraestructuras Críticas de las TIC.

Artículo 100. Los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, según corresponda, establecen y organizan sus Infraestructuras Críticas de las TIC relacionadas con la Seguridad y Defensa Nacional.

Artículo 101. El Ministerio de Comunicaciones, en coordinación con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, organiza el trabajo de protección de las Infraestructuras Críticas de las TIC para dotarlas de la seguridad requerida y controla su correcto despliegue por parte de las entidades especializadas, en correspondencia con el nivel de seguridad requerido.

Artículo 102. El Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC es el conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de las infraestructuras críticas de las TIC, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como se dispone un flujo de información que abarque a todos sus integrantes.

Artículo 103. El Plan Nacional de Protección a las Infraestructuras Críticas de las TIC tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

Artículo 104. El Ministerio de Comunicaciones, de conjunto con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, coordina las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten el funcionamiento de las Infraestructuras Críticas de las TIC.

Artículo 105. El jefe de la entidad responde por la garantía de la confidencialidad de los datos sobre Infraestructuras Críticas de las TIC a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada; además garantiza que el personal vinculado a las infraestructuras críticas de las TIC esté capacitado para su utilización, posean compromiso político, ético y de responsabilidad social y material; así como que conozcan sus deberes y derechos específicos en relación con estas.

Artículo 106. Los sistemas, las comunicaciones y la información referida a la protección de las Infraestructuras Críticas de las TIC tienen las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

CAPÍTULO IV
DE LA INSPECCIÓN Y LOS INCUMPLIMIENTOS EN LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 107. El Ministerio de Comunicaciones tiene como función estatal la ejecución de las inspecciones en materia de seguridad de las TIC, la que se realiza por sus inspectores y entidades autorizadas por este .

Artículo 108. El jefe de la entidad faculta a especialistas debidamente preparados para realizar controles en materia de seguridad informática a otras entidades atendidas, adscritas, subordinadas y patrocinadas.

Artículo 109. Las entidades y las personas naturales que incumplan lo dispuesto en el presente Decreto y en las disposiciones legales vigentes, están sujetas a la aplicación de las medidas siguientes:

a) Notificación preventiva;

b) invalidación temporal, parcial o cancelación de las autorizaciones administrativas concedidas por el Ministerio de Comunicaciones;

c) suspensión temporal, parcial o la cancelación de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano;

d) decomiso de los medios, instrumentos, equipamientos y otros, utilizados para cometer la infracción; y

e) la aplicación de otras medidas que correspondan, de conformidad con lo legalmente establecido.

Artículo 110. Las entidades y las personas naturales sujetas a la aplicación de las medidas descritas en el Artículo anterior tienen derecho a interponer recurso en la vía administrativa, según lo dispuesto en el Decreto-Ley No. 370, del 17 de diciembre del 2018, "Sobre la Informatización de la Sociedad en Cuba".

CAPÍTULO V
CAPACITACIÓN Y DIVULGACIÓN SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 111. El Ministerio de Finanzas y Precios, en coordinación con el Ministerio de Economía y Planificación, define las fuentes de financiamiento, orientadas a la adquisición de tecnologías de seguridad y a la preparación técnica de los especialistas en seguridad de las TIC.

Artículo 112. Los ministerios de Educación y de Educación Superior crean programas educativos y estrategias de trabajo que contribuyan a incrementar la conciencia en la sociedad acerca de la importancia de preservar la información personal.

Artículo 113. El Ministerio de Comunicaciones, en coordinación con el Instituto Cubano de Radio y Televisión, el Ministerio de Cultura y otras instituciones, promueve el uso de los medios de difusión para la trasmisión de mensajes educativos relacionados con la seguridad de las TIC.

Artículo 114. Cada entidad es responsable por la superación de los especialistas en las diferentes áreas del conocimiento, relacionadas con la seguridad de las TIC de acuerdo con su nivel de especialización.

Artículo 115. El jefe de la entidad implementa acciones que contribuyan y propicien la permanencia y el tratamiento diferenciado del personal que cumple funciones como especialistas de seguridad informática, en correspondencia con su categorización.

Artículo 116. La preparación en las materias objeto del presente Decreto de los cuadros, funcionarios y especialistas se desarrolla mediante acciones de carácter educativo-preventivas que estén relacionadas con los planes de estudios de las escuelas o centros docentes que correspondan.

Artículo 117. Los ministerios de Educación y Educación Superior insertan en los planes de estudio los temas referentes a la Seguridad de las TIC en todos los niveles de enseñanza, e implementan planes de estudios para los especialistas en seguridad de las TIC, actualizados por normas internacionales, así como fomentan los intercambios académicos e investigativos con universidades y centros de investigaciones nacionales e internacionales con alta preparación en la temática.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas lo establecido en el presente Decreto, de conformidad con sus estructuras.

DISPOSICIONES FINALES

PRIMERA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización y establecen las coordinaciones que resulten necesarias relativas a la aplicación del presente Decreto.

SEGUNDA: El Ministerio de Trabajo y Seguridad Social actualiza los calificadores y jerarquiza los cargos, a partir de las competencias requeridas para el perfil ocupacional del especialista en seguridad de las TIC.

TERCERA: El glosario de términos y definiciones anexo forma parte del contenido del presente Decreto.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 31 días del mes de mayo de 2019.

Miguel Díaz-Canel Bermúdez
Presidente de los consejos
de Estado y de Ministros

Jorge Luis Perdomo Di-Lella
Ministro de Comunicaciones

ANEXO
GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) **Entidad:** Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.

2) **Infraestructuras críticas de las Tecnologías de la Información y la Comunicación:** son aquellas que soportan los componentes, procesos y servicios esenciales que garantizan las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

3) **Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular:** Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado, las organizaciones superiores de dirección empresarial que incluye a la Empresa de Telecomunicaciones de Cuba S.A.