RESOLUCIÓN 128

Contenido

POR CUANTO: El Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional", de 5 de junio de 2019 en su Disposición Final Primera establece, que 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 referido Decreto.

POR CUANTO: A partir de la experiencia acumulada en la aplicación de las Resoluciones 127 del Ministro de la Informática y las Comunicaciones, que aprobó el **Reglamento de Seguridad de las Tecnologías de la Información, de 24 de julio de 2007 y la 192, de 20 de marzo de 2014, del Ministro de Comunicaciones, que puso en vigor el Reglamento** para contrarrestar el envío de mensajes masivos dañinos a través de las redes de telecomunicaciones; resulta necesario emitir una nueva disposición normativa que actualice el contenido normativo de las referidas disposiciones, para atemperarlas a las exigencias del proceso de informatización de la sociedad y en consecuencia **proceder a su derogación**.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:
RES. 128 REGLAMENTO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1. El presente Reglamento tiene por objeto complementar las disposiciones del Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional"de 5 de junio de 2019, y **establecer las funciones de los sujetos que intervienen en esta**, así como garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Artículo 2. **Este Reglamento 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 formas de propiedad y gestión no estatal, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales, en lo adelante la entidad.

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

Artículo 3. El Sistema de Seguridad de las TIC tiene como objetivo minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos.

Artículo 4. Las formas de propiedad y gestión no estatal y las personas naturales, **cumplen lo dispuesto en el presente Reglamento,** en lo que corresponda, aunque no cuenten con el personal especializado.

Artículo 5. El jefe de la entidad a cada nivel es el máximo responsable de la seguridad de las Tecnologías de la Información y la Comunicación, en lo adelante seguridad de las TIC, en su organización, **y garantiza la actualización de los Planes de Seguridad** de las TIC y considera para ello los factores siguientes:
a) **La aparición de nuevas vulnerabilidades**;
b) los efectos de los **cambios de tecnología o de personal;**
c) **la efectividad del sistema**, demostrada por la naturaleza, número y **daño ocasionado por los incidentes de seguridad registrados**.

Artículo 6. Los especialistas en seguridad de las TIC a cada nivel, **cumplen las funciones siguientes:**
a) **Participar en el diseño del Sistema de Seguridad** y en la elaboración, evaluación y actualización **del Plan de Seguridad** de las TIC, supervisar su aplicación y disciplina en su cumplimiento;

b) **establecer y mantener los controles**, en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado;
c) **participar en la evaluación de riesgos y vulnerabilidades** de su entidad;
d) **controlar y supervisar la disponibilidad de los bienes informáticos**;
e) asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las TIC;
f) establecer los controles necesarios para **impedir la instalación de cualquier tipo de hardware o software,** sin la autorización de la dirección de la entidad;
g) participar en la **elaboración de los procedimientos de recuperación, ante incidentes** de seguridad y en sus pruebas periódicas;
h) **informar a los usuarios de las regulaciones establecidas**.

Artículo 7. Los responsables de la seguridad de las TIC a cada nivel, **responden por la protección de los bienes informáticos** que le han sido asignados **y tienen los deberes siguientes:**
a) **Identificar los requerimientos de seguridad** de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, **determinar el nivel de acceso de los usuarios** y la vigencia de estos accesos;
b) **participar en el diseño del Sistema de Seguridad** y en la elaboración, evaluación y actualización del Plan de Seguridad de las TIC en la parte que concierne a su esfera de acción y garantizar su cumplimiento;
c) **participar en la evaluación de riesgos y vulnerabilidades de su entidad;**
d) **aplicar las medidas y procedimientos** establecidos **en su área** de responsabilidad;
e) **especificar al personal subordinado**, las medidas y procedimientos establecidos **y controlar su cumplimiento;**
f) **participar en la elaboración de los procedimientos de recuperación ante incidentes** de seguridad y en sus pruebas periódicas;
g) **imponer o proponer sanciones ante violaciones del Sistema de Seguridad**, en correspondencia con su naturaleza y con los daños ocasionados.

Artículo 8. Los usuarios de las TIC en sus entidades, **tienen los deberes siguientes**:
a) **Adquirir la preparación necesaria y los conocimientos de Seguridad** de las TIC imprescindibles para el desempeño de su trabajo;
b) **contar con la autorización expresa del jefe facultado**, para obtener acceso a cualquiera de los bienes informáticos;
c) **cumplir las medidas de seguridad establecidas**;
d) **proteger las tecnologías o la terminal de red que le ha sido asignada** y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usar la información que contiene o utilizar de manera impropia el sistema al que esté conectado;
e) **contar con la autorización del jefe facultado para instalar** o utilizar en las tecnologías, equipamientos, o programas, o modificar su configuración;
f) **cumplir las reglas establecidas para el empleo de las contraseñas;**
g) **informar al dirigente facultado de cualquier anomalía de seguridad detectada.**

CAPÍTULO III DEL EMPLEO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

SECCIóN PRIMERA Bienes informáticos

Artículo 9. **Los bienes informáticos están bajo la custodia documentada legalmente de la persona designada** para hacer uso del bien**, quien es responsable de su protección**.

Artículo 10. El jefe de la entidad instrumenta los procedimientos que se requieran para garantizar **la autorización y el control** sobre la utilización y movimiento **de los bienes informáticos.**

Artículo 11. **El jefe del área o unidad organizativa** que atiende las TIC **define el procedimiento de uso** de empleo y responsabilidad **de los bienes informáticos que son móviles** (portátiles o removibles), para las personas que utilizan estos bienes dentro y fuera de la entidad, que incluye:
a**) Comunicar de inmediato por el ususario a la dirección de la entidad la pérdida o extravío del bien;**
b) **no contener datos importantes e información sensible,** cuando se extraigan de la entidad, y tener implementadas medidas de protección;
c**) no conservar datos personales o sobre la entidad** a través de los que se pueda acceder a sus sistemas.

SECCIóN SEGUNDA De la Dirección del personal

Artículo 12. Las funciones y responsabilidades de seguridad de las TIC, tanto generales como específicas, **son debidamente documentadas** e incluidas dentro de las responsabilidades laborales del personal de la entidad.

Artículo 13. El jefe del área o unidad organizativa que atiende las TIC de la **entidad está obligado a preparar y exigir responsabilidad al trabajador** en materia de seguridad de las TIC, **así como a aplicar las sanciones** en caso de que este incumpla los requerimientos establecidos.

Artículo 14. La dirección de cada entidad establece previamente **la utilización** de las TIC **y** sus **servicios asociados** conforme a la **necesidad de uso en interés de la propia entidad**.

Artículo 15. La introducción, ejecución, distribución o conservación de programas en los medios de cómputo que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, **solo se efectúan por las personas debidamente autorizadas por el jefe del área o unidad organizativa que atiende las TIC**; se excluye el uso de aplicaciones destinadas a la comprobación de los sistemas instalados en la organización para el control interno de las operaciones realizadas y en ningún caso, este tipo de programas o información se expone mediante las TIC para su libre acceso.

SECCIóN TERCERA **Seguridad Física**

Artículo 16. **En los edificios** e instalaciones de cada entidad, **su dirección determina las áreas o zonas controladas con requerimientos específicos**, protegidas por un

perímetro de seguridad definido, en dependencia de la importancia de los bienes informáticos que contiene y su utilización de acuerdo con la denominación siguiente:
a) **Áreas limitadas:** en las que se concentran bienes informáticos de valor medio, cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.
b) **Áreas restringidas:**donde se concentran bienes informáticos de alto valor e importancia crítica, cuya afectación pueda paralizar o afectar severamente la gestión de sectores de la economía o de la sociedad; territorios o entidades.
c) **Áreas estratégicas:** en las cuales se concentran bienes informáticos de alto valor e importancia crítica, que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública, y el suministro de agua u otra que por su importancia se considere necesaria.

Artículo 17. Las áreas o zonas controladas se protegen para garantizar el acceso exclusivamente al personal autorizado y la dirección de la entidad establece las medidas que correspondan.

Artículo 18. En la selección y diseño de **las áreas controladas se tiene en cuenta la posibilidad de daño por fuego, inundación, explosión**, perturbaciones del orden y otras
formas de desastre natural o artificial.

Artículo 19. El equipamiento instalado en las áreas controladas se protege contra fallas de alimentación y otras anomalías eléctricas, lo que **incluye el uso de fuentes de alimentación alternativas** para los procesos que deben continuar en caso de un fallo de electricidad prolongado, así como **se ubica y protege de manera tal que se reduzcan los riesgos** de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

Artículo 20. En las áreas limitadas se aplican las **medidas de protección física** siguientes:
a) Seleccionar para su ubicación locales cuyas **puertas y ventanas** estén **provistas de cierres seguros;**
b) aplicar medidas que **garanticen su seguridad y eviten la visibilidad** hacia el interior de los locales con ventanas que se comuniquen al exterior de la instalación;
c) **prohibir el acceso de personal no autorizado** por la dirección de la entidad;
d) permitir la permanencia del **personal fuera del horario laboral con la debida justificación y autorización** por escrito de la dirección de la entidad; las autorizaciones referidas se conservan por un término mínimo de seis meses.

Artículo 21. En las áreas restringidas además de las medidas requeridas en las áreas limitadas, **se aplican** las siguientes:
a) **Se mantienen cerradas** incluso cuando permanezcan personas laborando, y el **acceso se controla mediante los registros** que para ello se establezcan;
b) **establecer por la entidad requisitos de idoneidad**, al personal que accede a estas áreas;

c) **utilizar sistemas de detección y alarma** que permitan una respuesta efectiva ante accesos no autorizados, cuando no se encuentre el personal que en ellas labora;
d) **implementar mecanismos y procedimientos de supervisión** de la actividad que se realiza en estas áreas;
e) **prohibir la introducción de soportes ópticos y magnéticos personales**, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad; así como de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a esta.

Artículo 22. En las áreas estratégicas además de las medidas requeridas en las áreas restringidas y limitadas, se aplican las siguientes:
a) **Establecer una identificación individual** que especifique las áreas de trabajo **para el personal que labore** o que por razones de servicio sea autorizado a permanecer en estas; **la cual debe llevarse por cada trabajador en un lugar visible;**
b) **implementar medios especiales de supervisión** de la actividad que en ellas se realiza;
c) **el acceso por personas ajenas solo se autoriza de manera excepcional**, restringida y bajo supervisión, mediante un permiso especial, emitido por la dirección de la entidad, el que se conserva por un término mínimo de seis meses.

Artículo 23. Los recursos relacionado con las TIC, independientemente de su importancia, **se protegen contra alteraciones o sustracciones**, ya sea de estas, de sus componentes o de la información que contienen.

Artículo 24. El jefe de la entidad es el responsable de que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante, **con el fin de asegurar su disponibilidad e integridad**; en caso de necesidad de envío del equipamiento fuera de las instalaciones para que reciban mantenimiento, este se realiza en correspondencia con los procedimientos establecidos por la dirección de la entidad a tales efectos, según las regulaciones vigentes en el país en materia de protección de la información.

Artículo 25. El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información **se autoriza por su dirección**, mediante el documento correspondiente; la seguridad que se le garantice por el autorizado tiene que ser equivalente a la establecida en las instalaciones habituales del equipamiento usado para este propósito.

Artículo 26. El equipamiento antes de causar baja o ser destinado a otras funciones, **se le aplica el procedimiento de borrado seguro,** para evitar que la información que contiene pueda resultar comprometida; **los dispositivos** de almacenamiento **que contengan información crítica para la entidad son destruidos físicamente**.

Artículo 27. Se prohíbe el movimiento de los equipos de la entidad y de los programas y aplicaciones informáticas **sin la autorización escrita del jefe facultado**; en caso de que se autorice se registra el movimiento a la salida del medio y a su entrada al reintegrarse a su origen; así como se realizan los controles sorpresivos para detectar las extracciones no autorizadas.

CAPÍTULO IV SEGURIDAD DE LAS OPERACIONES

Artículo 28. Las acciones para cubrir las brechas de seguridad y la corrección de los errores de los sistemas y aplicaciones **son minuciosamente controladas en cada entidad**, **por sus respectivos jefes;** los procedimientos aseguran en lo fundamental que:
a) **Sean eliminadas o minimizadas las vulnerabilidades** conocidas;
b) **solo el personal identificado y autorizado tenga acceso** a sistemas en funcionamiento y a los datos;
c) **todas las acciones de emergencia tomadas sean documentadas** detalladamente;
d) **la acción de emergencia sea reportada a la dirección de la entidad** y realizada de manera
ordenada.

Artículo 29. En caso de ser necesario compartir recursos a través de la red, *se define*, por la persona autorizada, **de forma precisa con los usuarios se hará, el nivel de acceso y la duración del intercambio.**

Artículo 30. En **el uso de credenciales de acceso, cuya contraseña es textual**, como método de autenticación de usuarios, se cumplen los requisitos siguientes:
a) **Ser privadas e intransferibles;**
b) **su estructura, fortaleza y frecuencia de cambio se corresponden con el riesgo** estimado para el acceso que protegen, implementado a través de mecanismos automatizados de validación;
c) **la composición de los caracteres es alfanumérica** (letras, números y símbolos) sin un significado trivial, con una longitud mínima de 8 caracteres;
d) no pueden ser visualizadas en pantalla mientras se teclean;
e) **no se almacenan en texto claro, sin cifrar,** ni son recordadas en ningún tipo de terminal.

Artículo 31. En el caso de mecanismos de autenticación **diferentes** al mencionado anteriormente**, se cumple las normas de seguridad establecidas** para estos.

Artículo 32. El jefe de la entidad apueba los derechos y privilegios de acceso a sistemas y datos que tiene cada usuario, asi como el procedimiento escrito en cada caso para otorgar o suspender estos accesos.

Artículo 33. Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procede al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, y se preserva para su posterior análisis y descontaminación por personal especializado; **además, se revisan los soportes con los que haya interactuado el medio contaminado.**

Artículo 34. La contaminación por programas malignos se considera un incidente de seguridad y se cumple en este caso lo establecido en el Artículo 48 del presente Reglamento; en todos los casos **se tiene que determinar el origen y la responsabilidad** de las personas involucradas.

Artículo 35. El usuario que a través de sus equipos terminales de telecomunicaciones **reciba mensajes masivos dañinos**, **tiene el derecho de presentar** a su operador o proveedor **una queja con las pruebas relativas de los hechos ocurridos**; al que le corresponde tomar las medidas que procedan para eliminar la situación surgida.

CAPÍTULO V SEGURIDAD DE LAS REDES

Artículo 36. El administrador de una red informática tiene, en relación con la seguridad de las TIC, **los deberes siguientes**:
a) **Garantizar** la aplicación de mecanismos que implementen **las políticas de seguridad definidas en la red;**
b) realizar el **análisis sistemático de los registros de auditoría** que proporciona el sistema operativo de la red;
c) **garantizar que los servicios** implementados **sean utilizados para los fines** que fueron creados;
d) **comunicar a la dirección de la entidad** los **nuevos controles técnicos** que estén disponibles y **cualquier violación** o anomalía detectada en los existentes;
e) **activar los mecanismos** técnicos y organizativos **de respuesta** ante distintos tipos de incidentes y acciones nocivas que se identifiquen, y **preservar toda la información** requerida para su esclarecimiento;
f) participar en la **elaboración de los procedimientos de recuperación ante incidentes** y en sus pruebas periódicas;
g) **informar** a los usuarios de **las regulaciones** de seguridad establecidas **y controlar su cumplimiento;**
h) garantizar que en el **registro de trazas** se incluya las relacionadas **con la navegación a Internet,** que permitan **correlacionar la dirección IP real de salida** al proveedor de servicios de Internet, **con las IP privadas** empleadas en las redes internas de la entidad;
i) participar en la **confección y actualización del Plan de Seguridad** de las TIC;
j) implementar y operar los controles que se establezcan para **gestionar los riesgos** de seguridad.

Artículo 37. En el empleo de las **redes inalámbricas** se tienen en cuenta, además de los aspectos de su seguridad, los siguientes:
a) **Contar con la autorización**, a través del procedimiento establecido, de la entidad facultada para su despliegue y explotación;
b) **utilizar protocolos de cifrado de datos** aprobados para la red de telecomunicaciones inalámbrica que lo requiera;
c) **utilizar filtrado de direcciones MAC** (conocida como Media Access Control) **cuando** sea posible y **no se afecten los servicios** para la que están destinadas;
d) **configurar la potencia de irradiación al nivel establecido** por la autoridad facultada a esos efectos.

Artículo 38. El jefe de la entidad orienta la ejecución de **procedimientos periódicos de verificación** de la seguridad de las redes, **con el fin de detectar** posibles **vulnerabilidades**, **incluye** para ello, cuando sea procedente, **la comprobación de forma remota por entidades facultadas** oficialmente, debido a la sensibilidad de estas

acciones.

Artículo 39. En las redes donde se establezcan servicios de **intercambio de datos o mensajes con otras redes o usuarios externos**, **se implementan mecanismos** de seguridad que garanticen la **confidencialidad**, **la integridad**, **el control de accesos**, **la autenticación y el no repudio**, según corresponda.

Artículo 40. En los casos de **redes corporativas** que prevean la **extrapolación de servicios internos**, **la conexión** se realiza **por puertos bien identificados** y mediante la protección **con dispositivos que garanticen el acceso** a esos servicios por el **personal autorizado**.

Artículo 41. Los servicios que ofrecen las redes de datos de una entidad **mediante conexiones externas,** solo se utilizan en interés de esta; **la asignación de cuentas** para su empleo **se aprueba**, en todos los casos, **por la dirección de la entidad**, sobre la base de las necesidades requeridas para su funcionamiento.

Artículo 42. Los servicios ofrecidos al público que son autorizados a una entidad específica, **no forman parte de la red corporativa.**

Artículo 43. La configuración del **servicio de correo electrónico** tiene que garantizar que **solo el propietario de una cuenta pueda enviar y recibir mensajes** desde esta.

Artículo 44. Se prohíbe vincular cuentas de correo, con el fin de redireccionar y acceder a los mensajes a través de este.

CAPÍTULO VI DE LOS INCIDENTES DE SEGURIDAD

Artículo 45. La estrategia que se formule en la entidad **ante cualquier incidente o violación de la seguridad** es consecuente con sus objetivos básicos, donde **se define el Plan de Prevención de Riesgos;** además tiene en consideración:

a) **Los riesgos** que enfrenta en términos de **probabilidad y su impacto**, **incluye** una identificación y **asignación de prioridades a los procesos críticos**;

b) **el impacto probable** de las interrupciones **sobre la gestión de la entidad**;

c) la **comprobación y actualización** de manera **periódica** de los **planes y procesos** establecidos;

d) las **acciones para la recuperación**.

Artículo 46. Los procedimientos para **la gestión de incidentes y violaciones** de seguridad de las TIC, tienen los **requisitos siguientes**:

a) **El reporte** inmediato de la acción **a la autoridad correspondiente**;

b) la **comunicación con los afectados o los involucrados** en la recuperación del incidente;

c) el **análisis y la identificación de las causas**;

d) el **registro de todos los eventos vinculados**;

e) la **recolección y preservación de las trazas** de auditoría y otras evidencias;

f) la **planificación y la implementación de medidas** para prevenir la recurrencia, si fuera necesario.

Artículo 47. Ante cualquier incidente que afecte la seguridad de las TIC de una entidad, **su dirección designa una comisión**, integrada por especialistas no comprometidos directamente con este hecho, **encargada de realizar las investigaciones** necesarias para esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

Artículo 48. La dirección de cada entidad queda obligada, al producirse un incidente o violación de la seguridad informática, **reportarlo inmediatamente a la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones y a la instancia superior de la entidad;** este reporte incluye:
a) **En qué** consistió el incidente o violación;
b) **fecha y hora** de comienzo del incidente y de su detección;
c) **implicaciones y daños** para la entidad y para terceros;
d) **acciones iniciales tomadas**;
e) **evaluación preliminar.**

CAPÍTULO VII PRESTACIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA A TERCEROS

Artículo 49. La Dirección General de Informática del Ministerio de Comunicaciones es la unidad organizativa que **autoriza las entidades** que pueden brindar servicios de seguridad informática a terceros.

Artículo 50. Los requerimientos que cumple la entidad **para solicitar la autorización** que le permita prestar servicios de seguridad de las TIC a terceros, son los siguientes:
a) **Que su objeto social se relacione con los servicios** de las TIC;
b) que cuente con **mecanismos que garanticen la calidad de los servicios y la idoneidad del personal;**
c) **preparación técnico-profesional de los especialistas** que laboren en la entidad;
d) **que esté en condiciones de cumplir los reglamentos y disposiciones establecidos** en esta materia;
e) **que cuente con medios de protección de la información a la que tenga acceso durante su trabajo**;
f) **que los productos de seguridad informática utilizados**, **estén debidamente autorizados** por las entidades facultadas;
g) **que sea una entidad estatal** cuyo personal resida de forma permanente en el país.

Artículo 51. Las entidades autorizadas por la Direccion General de Informática para brindar servicios de seguridad informática en las redes de otras entidades, **están en la obligación de:**
a) **Mantener el máximo de discreción** en relación con las posibles vulnerabilidades detectadas;
b) **abstenerse de la utilización del conocimiento obtenido** sobre la red comprobada **en beneficio propio;**
c) **informar a las entidades designadas para el control del ciberespacio**, **los resultados de las comprobaciones** realizadas.

CAPÍTULO VIII DE LA INSPECCIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 52. La inspección estatal a la seguridad de las TIC **tiene como objetivos** principales, los siguientes:
a) **Evaluar** los **conocimientos y la aplicación de la base legal** vigente;
b) **realizar diagnósticos sobre la efectividad de los sistemas** de seguridad informática aplicados en las entidades;
c) **verificar el** grado **de control y supervisión** que se ejerce **sobre los bienes informáticos**, así como **los resultados de la gestión** de la seguridad informática;
d) **evaluar la efectividad de los planes de seguridad informática** elaborados **y su actualización** y correspondencia con las necesidades de cada entidad;
e) **valorar la gestión** e influencia **que ejercen las instancias superiores** sobre esta actividad.

Artículo 53. Los inspectores de seguridad de las TIC tienen las **facultades** siguientes:
a) **Realizar** la **inspección** con o sin aviso previo;
b) **evaluar el estado de cumplimiento y aplicación de la base legal** de la Seguridad Informática vigente;
c) **identificar las violaciones y vulnerabilidades** detectadas en el Sistema de Seguridad Informática;
d) **hacer evaluaciones, recomendaciones y disponer acciones correctivas** ante violaciones de la base legal establecida;
e) **proponer sanciones administrativas** según las previstas en el Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional";
f) r**ecomendar** la realización de **auditorías**;
g) **proponer la suspensión de los servicios**, cuando se viole lo establecido en el presente Reglamento;
h) **verificar el cumplimiento de las acciones correctivas** que hayan sido aplicadas como resultado de inspecciones anteriores, si las hubiere;
i) **exigir la entrega de las trazas o registros de auditoría** de las TIC u otras posibles evidencias que se consideren necesarias;
j) **ocupar para su revisión los medios informáticos involucrados** en cualquier tipo de incidente de seguridad y proponer su decomiso definitivo a las instancias correspondientes.

DISPOSICIÓN ESPECIAL

ÚNICA: Se facultan a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, a adecuar para sus sistemas lo dispuesto en la presente Resolución.

DISPOSICIONES FINALES

PRIMERA: Se faculta al Director General de la Oficina de Seguridad las Redes Informáticas perteneciente a este Ministerio, para **implementar las acciones** que se requieran con el fin de dar cumplimiento a lo que por la presente se dispone.

SEGUNDA: El Viceministro que atiende la Informática en el Ministerio de las Comunicaciones, **instrumenta las medidas que se requieran** en el control de los parámetros que sean necesarios **para la contención de los mensajes masivos dañinos**.

TERCERA: Derogar las resoluciones 127 del Ministro de la Informática y las Comunicaciones, de 24 de julio de 2007 **y la 192** del Ministro de Comunicaciones, de 20 de marzo de 2014.

NOTIFÍQUESE a los directores generales de Defensa y de la Oficina de Seguridad para las Redes Informáticas, a los directores territoriales de control, todos del Ministerio de Comunicaciones.
COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones, del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella