RESOLUCIÓN MINISTERIAL No.176/07

POR CUANTO: Corresponde al Ministerio de Educación, en virtud de lo dispuesto en el Acuerdo No. 4006, adoptado por el Comité Ejecutivo del Consejo de Ministro con fecha 25 de abril del 2001, dirigir, ejecutar y controlar la aplicación de la política del Estado y el Gobierno en cuanto a la actividad educacional.

POR CUANTO: El Acuerdo No. 2817 de fecha 25 de noviembre de 1994, adoptado por el Comité Ejecutivo del Consejo de Ministros, establece los deberes, atribuciones y funciones comunes a los jefes de los Organismos de la Administración Central del Estado.

POR CUANTO: Este Reglamento de Seguridad Informática, se basa en lo legislado en los decretos ley 186 de fecha 17 de junio del 1998 y el decreto ley 199 de fecha 25 de noviembre del 1999, en las resoluciones 6 del Ministerio del Interior de fecha 13 de noviembre de 1996, la 204 de la Industria Siderometalúrgica de fecha 20 de noviembre del 1996 y la Resolución 127 de fecha 9 de julio del 2007 del Consejo de Estado, donde se establece que se elaboren y pongan en vigor un Reglamento que rija la seguridad de las tecnologías de la información y garantice un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país y del Organismo que las adecua.

POR CUANTO: Es necesario establecer las regulaciones sobre el Plan de Seguridad Informática y el Código de Ética para todo el sistema informático del Ministerio de Educación, sus entidades y dependencias, organizándolo de forma que se ajuste a lo normado por los ministerios del Interior y el de Informática y Comunicaciones.

POR CUANTO: Por Acuerdo del Consejo de Estado de la República de Cuba, de fecha 25 de noviembre de 1990, el que resuelve fue designado Ministro de Educación.

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

RESUELVO:

PRIMERO: Aprobar el Reglamento de Seguridad Informática en la Actividad Educacional del Ministerio de Educación.

SEGUNDO: Derogar la Resolución Ministerial No. 230/98, de fecha 7 de diciembre de 1998.

TERCERO: La presente Resolución entra en vigor a partir del 1 de diciembre del 2007.

NOTIFIQUESE: Al Ministro de la Informática y las Comunicaciones.

COMUNIQUESE: La presente a viceministros, directores nacionales, directores provinciales y municipales de educación, los rectores de los institutos superiores pedagógicos, directores de los institutos politécnicos de informática, directores de empresas e instituciones y a cuantas personas naturales o jurídicas proceda y archívese el original de la misma en la Asesoría Jurídica.

Dada en La Habana, a los 27 días del mes de noviembre de 2007
"AÑO 49 DE LA REVOLUCIÓN"

Luis I. Gómez Gutiérrez
Ministro de Educación

CAPITULO I
GENERALIDADES
OBJETIVOS Y ALCANCE

ARTÍCULO 1: El término de las tecnologías de la información utilizado en este Reglamento está relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos. El empleo de otros términos tales como: seguridad de la información, seguridad de los ordenadores, seguridad de datos o seguridad informática tienen, a los efectos de lo que aquí se establece, el mismo significado. Todos los términos aquí tratados y adecuados se someten a lo establecido en los decretos ley 186 y 199.

ARTÍCULO 2: El presente Reglamento tiene por objeto establecer los principios que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

ARTÍCULO 3: Cada entidad, de acuerdo con sus características y en consonancia con el presente Reglamento, establecerá las políticas de seguridad informática de su sistema, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos teniendo en cuenta, entre otros, los siguientes aspectos:

a) Tratamiento de la información oficial que se procese según su categoría.
b) Empleo conveniente y seguro de las tecnologías instaladas y los servicios que se prestan.
c) Definición de los privilegios y derechos de acceso a los activos de información para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación, mediante la especificación de las facultades y obligaciones de los dirigentes, especialistas y usuarios.
d) Efectivo control de acceso a los activos y recursos, incluyendo los accesos remotos y a los locales informáticos.
e) Salvas y conservación de la información.
f) Acceso a redes externas, especialmente las de alcance global.
g) Requerimiento de seguridad informática de tecnologías de nueva adquisición y producto de software.
h) Principio de monitoreo del correo electrónico y trazas de navegación, así como registros de auditorias y acceso a los ficheros de usuario.
i) Mantenimiento, reparación y traslado de las tecnologías y el personal encargado de ello.
j) Principios generales para el tratamiento de incidentes y violaciones.
k) Los principios, regulaciones, objetivos y definiciones establecidas en los decretos ley 186 y 199.
l) Resultados del Estudio de Riesgos y Amenazas, que se realice al sistema de la entidad.

CAPÍTULO II
DEL SISTEMA DE SEGURIDAD INFORMÁTICA

ARTÍCULO 4: Los directores de los Centros de Informática y Comunicaciones estarán en la obligación de diseñar, implantar y actualizar un sistema de seguridad Informática que garantice:

a) Minimización de los riesgos sobre los sistemas informáticos.
b) Continuidad de los procesos informáticos.

ARTÍCULO 5: Se confeccionará un plan de seguridad informática como expresión gráfica del Sistema de Seguridad Informática incluyendo el estudio de Riesgos y Amenazas con el objetivo de que el plan de seguridad informática responda a las realidades objetivas del sistema informático de la entidad a la que se quiera proteger. Para la confección de dicho sistema se constituirá un equipo multidisciplinario formado por lo que funcionalmente responden por el procesamiento de la información.

ARTÍCULO 6: El diseño del Sistema de Seguridad Informática y la elaboración del plan de seguridad informática de cada entidad del MINED se realizará en correspondencia con la metodología establecida al respecto por la Oficina de Seguridad para las Redes Informáticas y deberá estar dirigido a lograr un sistema de protección a la información y bienes informáticos, la conectividad que requieran ó los servicios que ofrezcan.

ARTÍCULO 7: Los jefes de entidades son los que aprueban los planes de seguridad informática; además, respondiendo por la actualización y vitalidad de estos, considerando para ello los siguientes factores:

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, números y daños ocasionados por los incidentes de seguridad registrados.

ARTÍCULO 8: La dirección de cada entidad definirá el propósito de las tecnologías informáticas instaladas, así como el acceso a estas. El empleo de estos medios con otros fines, solo se realizará de forma excepcional y debidamente autorizada en cada caso.

ARTÍCULO 9: La dirección de la entidad tiene la obligación de supervisar el uso, cuidado y conservación de los bienes informáticos que le han sido asignados, así como el servicio que estas prestan. La dirección establecerá los mecanismos (tantos como sean necesarios) para garantizar la efectividad de las supervisiones y auditorias según lo establecido en su Sistema de Seguridad Informática. Además responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones:

a) El director de la entidad organizará, aprobará y controlará el trabajo del equipo multidisciplinario encargado del diseño del Sistema de Seguridad Informática, apoyándose para este trabajo en el Jefe, Especialista ó Técnico de Seguridad y Protección y en el Responsable de Seguridad Informática.
b) Establecerá los niveles de seguridad apropiado durante el empleo de las tecnologías de la información.
c) Garantizará la elaboración, aprobación, puesta en vigor y cumplimiento de las regulaciones a cumplir en Seguridad Informática.
d) Autorizará y controlará el procedimiento que se realice para proteger la información clasificada y limitada que se procese en las tecnologías de información, de acuerdo a lo establecido en el Decreto Ley No. 199-99.
e) El Director del Centro de Informática y Comunicaciones, supervisará, autorizará y controlará la introducción y utilización de software básico y de aplicaciones en las tecnologías de la información.
f) El Director del Centro de Informática y Comunicaciones, asegurará que las tecnologías de la información que se adquieran mediante compra, donación o cualquier otra vía garanticen los requerimientos de seguridad establecidos para cada una de ellas.

ARTÍCULO 10: Las entidades que operan con tecnologías de información, designarán un responsable de seguridad informática con la experiencia y confiabilidad requerida, para que responda por la vitalidad del sistema informático de la entidad. Cuando las características propias de la entidad, su volumen y dispersión de las tecnologías de información instaladas, así lo requieran, se designarán, más de un responsable para la atención de la seguridad informática en las diferentes áreas de trabajo.

a) En el caso de las direcciones municipales de educación deberá designarse un responsable de seguridad informática a nivel de Dirección Municipal y en cada centro donde exista tecnología informática, por resolución del Director Municipal a partir de la importancia de los bienes a proteger y los riesgos a que están sometidos.
b) En los Institutos Superiores Pedagógicos deberá designarse por resolución rectoral un responsable de seguridad informática al nivel de instituto y por las sedes universitarias, con plenos poderes para el acceso y revisión de las tecnologías informáticas. Además, se designarán responsables por áreas, de acuerdo con las funciones de estas y el volumen de los recursos informáticos que posean.

ARTÍCULO 11: Los requisitos para la selección de los responsables de seguridad informática de una entidad deben ser los siguientes:

a) Poseer experiencia de trabajo comprobado en la actividad de informática.
b) Conocer los aspectos básicos de la informática.

c) No poseer antecedentes penales.
d) No haber cometido con anterioridad violaciones de la seguridad informática.

ARTÍCULO 12: Los responsables de Seguridad Informática seleccionados, serán nombrados por el jefe de la entidad y contarán con plenos poderes para el acceso y revisión de las tecnologías informáticas de todo el sistema informático, por lo que tendrán las siguientes atribuciones, funciones y obligaciones:

a) Controlar la aplicación del Plan de Seguridad Informática y participar en su actualización. Supervisar su aplicación y disciplina de cumplimiento.
b) Comunicar al jefe administrativo cuándo en un área no poseen los productos de seguridad informática actualizados, de acuerdo con las normas establecidas en este Reglamento, y a las condiciones de trabajo de la misma, así como cualquier otro tipo de violación.
c) Apoyar el trabajo de la dirección de la entidad en cuanto al estudio y aplicación del Sistema de Seguridad Informática establecido, valorando permanentemente su efectividad y proponiendo las modificaciones que se requieran ante el surgimiento de nuevas amenazas o la variación de la probabilidad de ocurrencia de las existentes.
d) Proponer y controlar la capacitación del personal vinculado a esta actividad, con el objetivo de contribuir al conocimiento y cumplimiento de lo establecido en el Plan de Seguridad Informática y este Reglamento.
e) Controlar la utilización y realizar un análisis periódico de los registros de seguridad informática establecidos.
f) Participar en las comisiones que se constituyan para la investigación de incidentes.
g) Organizar y controlar la actividad de seguridad informática.
h) Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.
i) Supervisar el trabajo del personal que responde por la Seguridad Informática en las entidades y organizar su preparación.
j) Proponer medidas ante violaciones de la base legal establecida en la materia
k) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática
l) Garantizar disponibilidad de los bienes informáticos.
m) Establecer controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la dirección de la entidad.
n) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
o) Informar a los usuarios de las regulaciones establecidas.
p) Supervisar el empleo de las tecnologías de la información por parte de los usuarios, administradores de red y todo personal que posea un bien informático.

q) Establecer el chequeo previo y posterior de todo soporte removible que participe en eventos, ferias, exposiciones u otras actividades similares de carácter nacional e internacional, con el objetivo de evitar la posible propagación de algún virus informático, y sus consecuencias.
r) Colaborar con el Jefe administrativo del área en la exigencia y control de la implementación de mecanismos de protección contra acceso no autorizado a las redes que existan o funcionen en su radio de acción.
s) Controlar que se cumplan en su radio de acción las disposiciones de este reglamento, y el resto de las normativas que sobre materia se emitan.

ARTÍCULO 13: Los jefes de las diferencias instancias, dependencias del sistema nacional de educación responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones que se utilicen en su área de responsabilidad, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos, empleo de música y video según las necesidades de cada centro.
b) Participar y aprobar el diseño del Sistema de Seguridad, basado en un análisis de riesgos y en la elaboración, evaluación y actualización del plan de seguridad informática y garantizar su cumplimiento.
c) Aplicar las medidas y procedimientos establecidos en su área de responsabilidad.
d) Especificar a los usuarios las medidas y procedimientos establecidos para una razonable seguridad informática y controlar su cumplimiento.
e) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
f) Imponer y proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.
g) Actuarán en correspondencia con lo establecido según el Artículo 136 de este reglamento acorde en la política de sanciones, recogido en el documento, ante la ocurrencia de incidentes y violaciones de seguridad informática.
h) Designará el personal que responde por la dirección, ejecución y control del Sistema de Seguridad Informática y garantizará su preparación.
i) Dominar la clasificación de los activos de información que maneja.
j) No divulgar información clasificada o limitada sin la autorización del dirigente facultado.

ARTÍCULO 14: La dirección de la entidad, a través de los jefes de cada nivel, garantizará que el personal vinculado a las tecnologías de la información se entrene previamente para la utilización de las mismas. El personal vinculado a dichas tecnologías deberá firmar un documento impreso en el cual se declaren los deberes y derechos que a cada cual corresponde, en relación con el Sistema de Seguridad Informática implementado (según las leyes establecidas en la Asamblea Nacional).

ARTÍCULO 15: Los asesores de informática de las direcciones provinciales de educación en cada entidad tienen las siguientes obligaciones:

a) Participar en el diseño del sistema de seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina de cumplimiento.
b) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado.
c) Garantizar la disponibilidad de los bienes informáticos.
d) Asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las tecnologías de la información.
e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de los jefes del Centro de Informática y Comunicaciones.
f) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
g) Informar a los usuarios de las regulaciones establecidas.
h) Apoyar el trabajo de la dirección de la entidad, en cuanto al estudio y aplicación del Sistema de Seguridad Informática establecido, valorando permanentemente su efectividad y proponer las modificaciones que se requieran, ante el surgimiento de nuevas amenazas o la variación de la probabilidad de ocurrencia de las existentes.
i) Velar porque se cumpla el Capítulo III, Sección Segunda, Artículo 26 de este Reglamento

ARTÍCULO 16: Los usuarios de las tecnologías de la información asumen, en primera instancia, la responsabilidad de las consecuencias que se deriven de la utilización impropia de las mismas.

ARTÍCULO 17: Los usuarios de las tecnologías de información tienen las siguientes obligaciones:

a) Adquirir la preparación necesaria y los conocimientos de seguridad informática imprescindibles para el desempeño de su trabajo.
b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualesquiera de los bienes informáticos.
c) Utilizar las tecnologías de información sólo en interés de la entidad.
d) No transgredir ninguna de las medidas de seguridad establecidas.
e) 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, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.
f) No instalar ni utilizar en las tecnologías, equipamientos o programas, ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.

g) Cumplir las reglas establecidas para el empleo de las contraseñas.
h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada, así como las que se informen en las auditorias que se realicen.

ARTÍCULO 18: Cada persona que tenga a su cargo tecnologías informáticas deberá suscribir un documento que exprese la responsabilidad material que ha adquirido sobre el citado bien que le ha sido asignado.

CAPÍTULO III
EMPLEO CONVENIENTE Y SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

SECCIÓN PRIMERA
CLASIFICACIÓN Y CONTROL DE LOS BIENES INFORMÁTICOS

ARTÍCULO 19: Los bienes de una entidad se determinan por la función que tienen en el cumplimiento de su objeto social, económico y riesgos a los que están sometidos, lo cual permitirá establecer una estrategia para el tratamiento de la seguridad de la actividad. Se definirán claramente los recursos críticos para el funcionamiento de la entidad (aquellos imprescindibles para el cumplimiento de las funciones de la entidad). Este debe expresar claramente sus pautas y no contener ambigüedades.

ARTÍCULO 20: Toda entidad tiene que mantener identificadas y controladas las tecnologías de la información que posea, instrumentando las medidas y procedimientos para garantizar el control sobre su existencia y las entradas o salidas de las mismas. Se establece como principio que cada uno de los bienes informáticos en cada entidad tiene que ser asignado a una persona, que actuando por delegación de la dirección de la entidad, es responsable de su protección.

ARTÍCULO 21: Adicionalmente cada entidad establecerá cuantos registros sean conveniente para lograr el control de sus recursos y el cumplimiento de las medidas de seguridad informática establecidas, así como mantendrá actualizado el inventario de las tecnologías informáticas, incluyendo sus componentes y las especificaciones técnicas de aquellos que pudieran ser suplantados.

ARTÍCULO 22: Cada bien informático tiene que tener su expediente técnico o formulario técnico, donde se consignen todos sus datos y números de series de todas sus partes y componentes, cambios de piezas o arreglos de las máquinas por parte del personal técnico autorizado, sellos de garantía y seguridad, que los ubica la entidad que garantiza los servicios técnicos, en cada territorio. En caso que no se tenga el expediente se debe llevar estos controles en modelos por el técnico de laboratorio o responsable de seguridad informática.

SECCIÓN SEGUNDA
DEL PERSONAL

ARTÍCULO 23: El acceso de cada usuario a los sistemas de la entidad tiene que ser aprobado previamente por la dirección de la misma, debiendo existir un procedimiento (manual o automático) para autorizar la inclusión de nuevos identificadores de usuarios en los sistemas y que incluya la notificación del director y del usuario.

ARTÍCULO 24: Las funciones y responsabilidades sobre seguridad, tanto las generales como las específicas, serán documentadas y se incluirán dentro de las responsabilidades laborales del personal.

ARTÍCULO 25: El personal previsto para ocupar cargos vinculados a la actividad informática en todas las dependencias que pertenezcan al Sistema Nacional de Educación, estudiantes insertados y otros casos similares con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas, deberá ser seleccionado adecuadamente.

ARTÍCULO 26: En el caso de los estudiantes extranjeros se acogerán a todos los artículos comprendidos en este reglamento.

ARTÍCULO 27: Los términos y condiciones del contrato de empleo incluirán la obligación de la entidad contratante en cuanto a la preparación del contratado, así como la responsabilidad del trabajador ante la Seguridad Informática, precisando que este último aspecto mantiene su vigencia una vez finalizada la relación laboral. Deberán incluirse las acciones a tomar en caso de que el trabajador pase por alto los requerimientos de seguridad.

ARTÍCULO 28: La utilización de las tecnologías y sus servicios asociados en cada entidad será aprobada previamente por la dirección de la misma y basado en cada caso en la necesidad de uso por interés de la propia entidad.

ARTÍCULO 29: El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una violación de los derechos de la entidad que es sancionable. Es un deber y un derecho de la dirección de cada entidad la supervisión del empleo de las tecnologías de la información.

ARTÍCULO 30: Los jefes de cada nivel, garantizarán que el personal vinculado a las tecnologías de la información esté capacitado para la utilización de las mismas, así como que conozca sus deberes y derechos en relación con el Sistema de Seguridad Informática implementado, los cuales deberán firmar una declaración como constancia de su conocimiento y compromiso de cumplimiento, que se incluirá en el contrato de trabajo.

ARTÍCULO 31: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por parte de personal que no forme parte de la plantilla será en todos los casos objeto de una estricta autorización y control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir se establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

ARTÍCULO 32: Los usuarios de las tecnologías de la información están en la obligación de informar de inmediato cualquier incidente de seguridad, debilidad o amenaza a sistemas o servicios y las direcciones correspondientes exigirán su cumplimiento.

ARTÍCULO 33: Constituye una violación grave de la seguridad la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

ARTÍCULO 34: Cada director de entidad o usuario es responsable de su información, por lo que debe garantizar las copias de seguridad de la misma para recuperarla en casos de fallo de las tecnologías de la información.

ARTÍCULO 35: Ningún usuario está autorizado a introducir, ejecutar, distribuir o conservar en los medios informáticos a él asignados, programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad de la red de la entidad. De ser necesaria la utilización de programas de este tipo como herramienta de diagnóstico, tendrá que ser aprobado previamente por la dirección de la entidad. En ningún caso este tipo de programas o información se expondrá mediante las tecnologías para su libre acceso por cualquier persona.

ARTÍCULO 36: Toda persona que detecte indicios de difusión e intercambio de información contrarios al interés social, la moral, buenas costumbres, integridad o Seguridad del Estado, deberá comunicarlo de inmediato al Responsable de Seguridad Informática, administrador de red y jefe inmediato superior.

ARTÍCULO 37: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por parte del personal que no forme parte de la plantilla, será en todos los casos objeto de una estricta autorización y control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir, se establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

SECCIÓN TERCERA
SEGURIDAD FÍSICA AMBIENTAL

ARTÍCULO 38: La dirección de cada entidad determinará las tecnologías de información que, por las funciones a que estén destinadas, la información que contengan y las condiciones de los locales en que se encuentren ubicadas, requieran la aplicación específica de medidas de protección física.

ARTÍCULO 39: En las instalaciones de cada entidad se determinarán áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la importancia de los bienes informáticos contenidos en ellas y su utilización, de acuerdo con los criterios y denominaciones siguientes:

a) **Áreas limitadas**, son aquellas donde 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**, son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica, cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.

ARTÍCULO 40: Las áreas o zonas controladas estarán protegidas con medidas adecuadas para garantizar el acceso exclusivamente del personal autorizado.

ARTÍCULO 41: La selección y diseño de las áreas controladas tomará en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

ARTÍCULO 42: El equipamiento instalado en las áreas controladas estará protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado y será ubicado y protegido de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado, incluir la protección contra incendios.

ARTÍCULO 43: En las áreas limitadas de la entidad, se aplicarán las medidas de protección física siguientes:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros y dispositivos de sellos.
b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo.
c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.

d) Garantizar la seguridad de los soportes ópticos y magnéticos personales.
e) Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su verificación en caso de necesidad.

ARTÍCULO 44: En las áreas restringidas, además de las medidas requeridas en las áreas limitadas, se aplicarán las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas y el acceso a las mismas debe ser controlado mediante los documentos de registro que para ello se establezcan.
b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.
c) Se aplicarán sistemas de detección y alarma que permitan una respuesta efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas.
d) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas.

ARTÍCULO 45: Todas las tecnologías de información, incluyendo los laboratorios, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen; además, deben cumplir lo que está establecido en el Artículo 43 incisos a), b), d) y e).

ARTÍCULO 46: En las redes de las entidades los cables de alimentación o de telecomunicaciones que transporten datos o apoyen los servicios de información se protegerán contra la intersección o el daño. Los cables de alimentación eléctrica deberán estar separados de los cables de comunicaciones para evitar la interferencia.

ARTÍCULO 47: El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información, tiene que estar autorizado legalmente por la dirección de la misma mediante el documento correspondiente. La seguridad que se le garantice deberá ser equivalente a la que tiene en las instalaciones habituales el equipamiento usado para el mismo propósito, tomando en cuenta los riesgos de trabajar fuera de la instalación.

ARTÍCULO 48: El equipamiento que cause baja o sea destinado para otras funciones será objeto de un procedimiento adecuado para evitar que la información que contiene pueda resultar comprometida. Los dispositivos de almacenamiento que contengan información crítica para la entidad deberán destruirse físicamente o sobrescribirse mediante un proceso completo en lugar de borrarlos como usualmente se hace.

ARTÍCULO 49: Los soportes magnéticos de la entidad o personales (flash, discos externos, Cd, Mpeg3, mpeg4, IPOD y otros), que contengan información clasificada serán registrados en la Oficina de la OCIC.

ARTÍCULO 50: Los cos que viajen al exterior y porten soportes magnéticos de la entidad o personales (flash, discos externos, Cd, Mpeg3, mpeg4, IPOD y otros), lo entregarán al responsables de Seguridad Informática para su revisión conjuntamente con los compañeros del Dpto. de Seguridad y Protección. Además se les entregará un documento que avale que no contenga información clasificada ni virus.

ARTÍCULO 51: Se prohíbe el movimiento sin autorización de los equipos, la información o el software y en caso de que se autorice será realizado mediante un documento oficial que demuestre su legalidad y será revisada su información por el responsable de la seguridad informática, el movimiento deberá registrarse a la salida y a la entrada al reintegrarse el medio a su origen. Se deberán realizar auditorias sorpresivas para detectar las extracciones no autorizadas.

ARTÍCULO 52: Los servidores que están dedicados a brindar servicios de red e intranet no podrán ser movidos, o trasladados de lugar, o hacia otra entidad, independientemente que son medios básicos de la entidad, sin previa aprobación de la Dirección de Informática del Ministerio de Educación o del Viceministro Primero del Organismo.

ARTÍCULO 53: Los bienes informáticos deben estar ubicados en locales que no tengan problemas constructivos, ni eléctricos, no guarden humedad, que tengan buena ventilación y la climatización indicada por el fabricante.

SECCIÓN CUARTA
SEGURIDAD DE OPERACIONES

ARTÍCULO 54: Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que:

a) El personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos.
b) Todas las acciones de emergencia tomadas sean documentadas detalladamente.
c) La acción de emergencia sea reportada a la dirección y realizada de manera ordenada.

ARTÍCULO 55: Se prohíbe la instalación de cualquier software no debidamente autorizado por la dirección de la entidad, bajo la supervisión personal del jefe del Centro de Informática y Comunicaciones. Para tal caso, el software debe guardar total relación con las funciones del área donde será instalado y deberá pasar por un proceso de cuarentena técnica definido por el responsable de seguridad informática.

ARTÍCULO 56: Cada entidad garantizará la instalación de software especializado que permitan la detección de vulnerabilidades en la red, así como el control de esta por parte del responsable de seguridad informática y el administrador de red.

ARTÍCULO 57: Se prohíbe la instalación de cualquier equipo a la red informática sin la debida autorización de la dirección de la entidad, así como realizar conexión a otras redes informáticas de una tercera entidad.

ARTÍCULO 58: Cada entidad debe garantizar que el mantenimiento de las tecnologías se realice en presencia y bajo la supervisión del personal responsable administrativo de estas y en caso de su salida de la entidad, debe protegerse la información que contenga, realizando los procedimientos que se establezcan previamente para ello.

ARTÍCULO 59: Entre las medidas de seguridad de operaciones tenemos que:

a) La reparación o mantenimiento de los equipos destinados al procesamiento de información clasificadas se realizará una vez borrada físicamente la información. En el caso que la información por alguna causa no pueda ser borrada, el personal responsabilizado con su reparación queda obligado a cumplir lo establecido por la ley del Secreto Estatal.
b) Cuando las tecnologías informáticas y de comunicación no reúnan los requerimientos técnicos que permitan garantizar el cumplimiento de este Reglamento para mantener la información clasificada, el usuario estará obligado a borrar la información clasificada que en ella se contenga.
c) Salvar toda la documentación, base de datos, sistemas, configuraciones (router, servidores de correo, firewall).
d) Salvar toda la información que sea de importancia para la entidad en soporte magnético y entregarla para ser protegida al jefe del Centro de Informática y Comunicaciones.
e) El personal que esté frente a una máquina debe conocer los elementos mínimos de computación.
f) Desconectar los equipos cuando se concluya la jornada laboral.

SECCIÓN QUINTA
IDENTIFICACIÓN, AUTENTIFICACIÓN Y CONTROL DE ACCESOS.

ARTÍCULO 60: En las máquinas en que es posible el acceso por múltiples usuarios de correos se dispondrá para cada uno de ellos de un identificador de usuario personal y único. Las personas a las que se asignen identificadores de usuarios responden por las acciones que con ellos se realicen. En cada entidad donde exista más de un dominio el usuario tendrá la misma identificación.

ARTÍCULO 61: La asignación de nuevos identificadores de usuarios en los sistemas se realizará a partir de un procedimiento que incluya la notificación del jefe inmediato. En caso de terminación de la necesidad del uso de los sistemas por el cese de la relación laboral u otras causas, se procederá de forma análoga para la eliminación del identificador de usuario y el procedimiento que se establezca debe incluir los controles para prevenir el acceso del usuario al sistema, inmediatamente después de la notificación de su director.

ARTÍCULO 62: Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro y debe definirse, además, un proceso periódico para asegurar que no existan identificadores de usuarios pertenecientes a trabajadores que hayan causado baja de la entidad, así como identificadores inactivos que puedan ser empleados como vía de acceso no autorizado al sistema.

ARTÍCULO 63: El uso de las contraseñas e identificadores de usuario debe cumplir las siguientes condiciones:

a) Serán personales e intransferibles.
b) No podrán ser mostradas en pantalla mientras se teclean.
c) No podrán ser almacenadas en texto plano en ninguna tecnología.
d) No podrán ser “recordadas” en las tecnologías desde donde se operen.
e) Se guardará una copia de las mismas, en sobre sellado en la oficina del jefe de área para ser usado en caso excepcional en ausencia del propietario, siempre que las razones así lo justifiquen, por el jefe y responsable de seguridad informática.
f) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen.
g) Combinarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de seis caracteres.

ARTÍCULO 64: Se definirá, por parte de las entidades, la utilización de una estructura estándar en la creación de identificadores y, de ser posible, tratar de que un usuario tenga el mismo identificador en todos los sistemas que necesite utilizar. Cada identificador de usuario se asignará a una persona, que será responsable de las actividades realizadas con él.

SECCIÓN SEXTA
SEGURIDAD PROGRAMAS MALIGNOS

ARTÍCULO 65: Se prohíbe el diseño, la distribución o intercambio de códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para el análisis e investigación de programas malignos.

ARTÍCULO 66: En cada entidad se implementarán los controles y procedimientos para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su generalización.

ARTÍCULO 67: Para la protección contra virus se utilizarán los programas antivirus de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados.

ARTÍCULO 68: Los ficheros adquiridos por cualquier vía deberán pasar por un proceso exhaustivo de descontaminación que garantice la eliminación de cualquier virus informático o programa maligno.

ARTÍCULO 69: En casos de contaminación por virus informático u otro programa maligno se procederá inmediatamente a la desconexión del equipo de la red informática y se le informará al responsable de seguridad informática que determinará las medidas a tomar y cuándo el equipo estará en disposición de reanudar su trabajo.

ARTÍCULO 70: La contaminación por virus informáticos u otros programas malignos se considera un incidente de seguridad y se cumplirá en este caso lo establecido en el Artículo 137 del presente Reglamento. En todos los casos se determinará el origen y la responsabilidad de las personas involucradas.

ARTÍCULO 71: Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procederá al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, preservándolos para su posterior análisis y descontaminación por personal especializado y se revisarán los soportes con los cuales haya interactuado el medio contaminado.

ARTÍCULO 72: El responsable de la seguridad informática de las entidades es el encargado del control de virus y protección en virtud del cual se establece:

a) Entrenar al responsable de seguridad informática de cada área de cómo utilizar los detectores.
b) Cada área es responsable del control de virus informático en sus equipos y soportes informáticos.

ARTÍCULO 73: La contaminación por un virus informático nuevo, debe ser reportada por el responsable de seguridad informática a la entidad especializada **SEGURMÁTICA** o en su defecto la filial provincial, además de entregar los informes regulados para estos casos a la **Oficina de Seguridad para las Redes Informáticas**.

ARTÍCULO 74: La actualización de los antivirus se debe realizar desde el nodo central RIMED y los territorios en los nodos provinciales. El nodo central RIMED deberá mantener diariamente actualizado los antivirus en el servicio de protocolo de transferencia de fichero **(File Transfer Protocol)**.

SECCIÓN SÉPTIMA
RESPALDO DE LA INFORMACIÓN

ARTÍCULO 75: Todas las entidades están en la obligación de implementar un sistema fiable de respaldo de la información esencial para su funcionamiento que permita la recuperación después de un ataque informático, desastre o fallo de los medios, para lo cual ejecutarán los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

ARTÍCULO 76: Cada entidad debe garantizar la generación de salvas de la información que en ella se procesa, la periodicidad de estas estará en correspondencia con su importancia y razón de cambio. Estas salvas estarán identificadas adecuadamente y no serán expuestas al acceso público a través de las tecnologías de la información.

ARTÍCULO 77: La información de respaldo, conjuntamente con informes precisos y completos de las copias de respaldo y los procedimientos de recuperación documentados, deberá almacenarse en la Norma de Control. (OCIC), previendo una ubicación que le permita no afectarse en caso de desastre en la ubicación principal, situación excepcional u otra anomalía.

ARTÍCULO 78: La información de respaldo deberá tener una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal. Los controles aplicados a los medios en la ubicación principal dieran extenderse a la ubicación de los medios de respaldo.

ARTÍCULO 79: Se prohíbe la transmisión de información clasificada sin protección criptográfica, estará sujeta a lo establecido en el Decreto Ley No. 199. No obstante, no se utilizarán sistemas de encriptación, sin la debida autorización del Ministerio del Interior.

ARTÍCULO 80: De acuerdo con la información clasificada que se procese en cada área, estas serán definidas como VITALES o RESERVADAS, según su nivel de clasificación y atendiendo a lo establecido en los decretos ley No. 186 y 199.

ARTÍCULO 81: Las tecnologías en las que se procese información clasificada no estarán conectadas a ninguna red de datos. En caso de que por extrema necesidad deban hacerlo, se garantizarán todas las medidas necesarias para la protección de esta información.

ARTÍCULO 82: Los medios de respaldo deberán probarse regularmente y verificar su estado de actualización con el fin de asegurar que pueda confiarse en ellos para un uso de emergencia cuando sea necesario.

ARTÍCULO 83: Para la información clasificada se deben tener en cuenta las siguientes medidas:

a) El procesamiento, generación, clasificación y divulgación de información clasificada contenida en soportes, en máquinas u otro medio informático, deberá estar sujeta a lo reglamentado en el Decreto Ley No. 199.
b) La información clasificada contenida en los soportes se debe destruir después de concluida su utilización.
c) En los casos en que el jefe del Organismo autorice a que se procese o almacene información clasificada en soportes de otras áreas, unidades o empresas subordinadas, estos serán controlados a través de las medidas establecidas por el Decreto Ley No. 199.
d) La entrada y salida de soportes con información no clasificada a las áreas que se determinen que tienen información clasificada, deberá ser autorizada por el jefe de la misma, el cual es responsable que en su salida no se copie información de esa área.
e) A partir de la entrada en vigor de esta Reglamento, las aplicaciones destinadas al procesamiento de información clasificada deberán cumplir los parámetros establecidos por el Decreto Ley No. 199.
f) Todas las aplicaciones destinadas al procesamiento de información clasificada o restringida, deberán cumplir los siguientes requerimientos:

    1) Clasificar los objetos con los distintos niveles de clasificación de la información que permita la aplicación del control acorde a los niveles de acceso.
    2) Documentar claramente las políticas de acceso que caracterizan a la gestión de la entidad que sea necesario aplicar, teniendo en cuenta el nivel de confidencialidad, integridad y disponibilidad de la información.

SECCIÓN OCTAVA
SEGURIDAD EN REDES

ARTÍCULO 84: La Entidad que coloque información en servidores externos o internos con acceso público deberá garantizar la disponibilidad e integridad de la información, así como la correspondencia de su contenido con los intereses de la propia entidad y el país.

ARTÍCULO 85: Las dependencias que integran el Sistema Nacional de Educación están en la obligación de implementar los mecanismos de seguridad de los cuales están provistas las redes, así como será responsable de aquellos que permitan filtrar o depurar la información que se intercambie: los administradores de redes, las acciones que desde su red, sean realizadas en perjuicio de los sistemas informáticos de su entidad y de otras entidades. El administrador de red velará por las acciones.

ARTÍCULO 86: En todas las redes se habilitarán las opciones de seguridad con que cuentan los sistemas operativos, de forma tal, que se garantice la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan el monitoreo y auditoria de los principales eventos conservándolos por un tiempo no menor de un año.

ARTÍCULO 87: Para la fiscalización y el monitoreo del empleo que se le da a las redes de datos y de los servicios en ellas implementadas, las entidades instalarán los productos autorizados en el país para esos propósitos.

ARTÍCULO 88: La arquitectura y la configuración de los diferentes componentes de seguridad de una red y la implementación de sus servicios, estarán en correspondencia con las políticas definidas y aprobadas para su empleo y en ningún caso deben ser el resultado de la iniciativa de una persona, con independencia de la preparación que esta posea.

ARTÍCULO 89: Todas las redes de computadoras deberán contar con un administrador de red. En los casos en que el servicio de dicha red se mantenga de forma permanente en el día, la red debe contar con cuantos administradores sean necesarios para el funcionamiento adecuado de esta.

ARTÍCULO 90: Requisitos, funciones y atribuciones del administrador de red.

a) Poseer el nivel de preparación que garantice el ejercicio de sus funciones.
b) Carecer de antecedentes penales.
c) No haber sido sancionado administrativamente por problemas relacionados con la seguridad informática.

ARTÍCULO 91: El administrador de red de una entidad tiene las siguientes atribuciones y funciones:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en su red.
b) Informar a los usuarios de las regulaciones de seguridad establecidas.

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 implementados y cualquier anomalía o violación detectadas en los existentes.
e) Activar los mecanismos técnicos y organizativos den respuesta ante los distintos tipos de acciones nocivas que se identifiquen.
f) Administrar los recursos de la red (utilización correcta de los recursos de la intranet, configuración de los servidores, establecimiento de cuotas para los usuarios, instalación y modificación de los servidores en dependencia de las necesidades de la intranet, funcionamiento de los dispositivos de red instalados en las diferentes áreas para garantizar la conectividad de la red que administra).
g) Velar por la protección de los datos que en ella se procesan o se transmiten, mediante la instalación y actualización del software necesario para ello (sistemas de registro, de detección de intrusos, antivirus a nivel de servidores).
h) Proteger la integridad del funcionamiento de la red.
i) Garantizar mediante recursos lógicos la utilización correcta de los servicios de Internet y correo electrónico (definición de usuarios con acceso local, nacional, internacional e Internet, configuración de listas de accesos (ACL), filtros y cuantas medidas sean necesarias para tal objetivo).
j) Garantizar la conectividad y los servicios de los clientes conectados a su red.
k) Asesorar en el acceso a redes y trabajo con los servicios al personal encargado de administrar los recursos de las redes clientes.
l) Realizar el análisis sistemático de los registros de auditoria que proporciona el sistema operativo de la red.
m) Participar en la confección y actualización del plan de seguridad informática.
n) Realizar los registros de las salvas de las trazas diarias y conservarla en un tiempo de un año.
o) Descargar diariamente la actualización de los antivirus.

ARTÍCULO 92: La gestión de administración de las redes implica la concesión de máximos privilegios, por lo tanto se realizará directamente en los servidores de las mismas. Se prohíbe la administración remota de estas redes mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.

ARTÍCULO 93: Cada entidad definirá sus procedimientos para emitir las autorizaciones de los usuarios a la utilización de las tecnologías, garanticen un control razonable y efectivo de estos accesos. El control de los servicios de correo electrónico, Internet, File Transfer Protocol (FTP) privado, acceso remoto, conversación en tiempo real (Chat), deberán establecerse a través de listados con el nombre y procedencia de estos usuarios y el tipo de acceso autorizado, así mismo se emitirá igual documento en caso de cambio o modificación de los accesos de cada uno de estos.

ARTÍCULO 94: Se implementarán mecanismos que garanticen al nivel de máquina, el control de acceso a estas. Además, en el caso del uso de servicios como correo electrónico o Internet se implementarán mecanismos de caducidad de las sesiones abiertas y de las contraseñas para garantizar su actualización y evitar el robo de las mismas, así como la entrada no autorizada a las cuentas de usuario.

ARTÍCULO 95: En las máquinas que se encuentren conectadas a redes externas se establecerán los mecanismos necesarios para garantizar la confidencialidad y protección de la información que esta contiene, y se asegurará de que no sirva de puerta de entrada a la red interna; en caso de que así fuera, deberán implementarse los mecanismos técnicos para el control de acceso a esta red interna según el nivel que corresponda.

ARTÍCULO 96: Los usuarios que han recibido la autorización para el empleo de estos servicios son responsables por su propia conducta. Las debilidades de la seguridad de un sistema no representan una licencia para penetrar o abusar del mismo. Se infiere que los usuarios conocen las políticas de seguridad de las computadoras y redes a que ellos acceden y su adhesión a estas políticas. Una clara consecuencia de esto es que un acceso no autorizado a una computadora o el uso de una red es explícitamente una violación de las reglas de conducta, independientemente de la fragilidad de la protección de estas computadoras o redes.

ARTÍCULO 97: En las redes que prevean conexiones desde o hacia el exterior de una entidad es obligatorio instalar los medios técnicos que aseguren una barrera de protección entre las tecnologías de información de la entidad y la red externa, mediante los mecanismos de seguridad que sea necesario implementar.

ARTÍCULO 98: Las entidades instrumentarán la ejecución de procedimientos periódicos de verificación de la seguridad de las redes con el fin de detectar posibles vulnerabilidades, incluyendo para ello cuando sea procedente, la comprobación de forma remota por entidades autorizadas oficialmente a esos efectos, debido a la sensibilidad de estas acciones.

ARTÍCULO 99: En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos se implementará el control de mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

ARTÍCULO 100: Queda prohibido la colocación de páginas o sitios Web desde entidades en servidores extranjeros que ofrecen estos servicios de forma gratuita.

ARTÍCULO 101: Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas solo se utilizarán en interés de la misma. La asignación de cuentas para el empleo de estos servicios será aprobada en todos los casos por el Viceministro Primero del Organismo sobre la base de las necesidades requeridas para su funcionamiento.

ARTÍCULO 102: No se permite vincular cuentas de correo electrónico de un servidor de una entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo.

ARTÍCULO 103: No se podrá adicionar algún equipo o la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la dirección de la entidad, garantizando su compatibilización con las medidas de seguridad establecidas para la protección de dicha red.

ARTÍCULO 104: Ningún trabajador tiene derecho a establecer una cuenta de correos en servidores que se encuentran en el exterior y brindan estos servicios de forma gratuita. Si de manera puntual se necesita de esta, tiene que ser aprobada previamente por el Viceministro Primero del Organismo, a partir de la valoración de las razones existentes. Especificando claramente el tipo de información que se va a transmitir y el plazo de vigencia de esta modalidad. En ningún caso estas cuentas se utilizarán para la comunicación con otras redes cubanas.

ARTÍCULO 105: Queda prohibido la difusión a través de las redes públicas de transmisión de datos, información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional, por cualquier persona natural o jurídica. Las entidades instalarán los controles y mecanismos que permitirán detectar y obstaculizar este tipo de actividades. Las violaciones detectadas serán informadas oportunamente a las instancias pertinentes.

ARTÍCULO 106: Se evitará, dentro de las posibilidades de la entidad, que los servidores conectados a las redes externas sean los mismos que garanticen los servicios de la red interna.

ARTÍCULO 107: Para el envío de ficheros adjuntos a través del correo electrónico tiene que estar compactado en Winrar, revisado por un antivirus y es obligatorio que se llene el asunto, para evitar equivocación de que pueda ser un virus. El asunto debe ser escrito con frases o palabras legibles.

ARTÍCULO 108: Se implementarán mecanismos que garanticen el control de las trazas de auditoria, para su análisis por parte del responsable de la seguridad informática o el administrador de red.

ARTÍCULO 109: Se salvarán los logs semanalmente y serán guardados por un período de un año en un lugar seguro y que en los soportes donde se encuentren las salvas, el responsable de seguridad informática es el encargado de guardar las salvas.

CAPITULO IV
ACCESO A REDES DEL ALCANCE GLOBAL

ARTÍCULO 110: La política de accesos a redes de alcance global debe garantizar que la información que se difunda sea fidedigna, y la que se obtenga este en correspondencia con los principios éticos de la revolución.

ARTÍCULO 111: El acceso a redes de alcance global, tanto de personas jurídicas (entidades), como naturales (usuarios de una entidad y accesos remotos) tendrá un carácter selectivo. La petición de los accesos a redes de alcance global será enviada al Centro de Informática y Comunicaciones del Organismo, bien fundamentada, para ser aprobada por el Viceministro Primero del Organismo, que es la persona autorizada para ello.

ARTÍCULO 112: Una vez establecida la estrategia a seguir, las entidades dispondrán las medidas y procedimientos que correspondan, con el fin de garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos.

ARTÍCULO 113: Cada entidad tomará las medidas que se requieran para evitar la sobrecarga de los canales de comunicaciones, restringiendo el envío o recepción de grandes volúmenes de información o la generación de mensajes a múltiples destinatarios.

ARTÍCULO 114: Se prohíbe la generación de cartas y el envió de mensajes de correos a más de 15 destinatarios. De requerirse excepcionalmente el envío de un mensaje a más destinatarios que los señalados, tendrá que ser visto con los administradores de red y por el Director del Centro de Informática y Comunicaciones.

ARTÍCULO 115: Las entidades implementarán controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva (Spam) a través de las redes.

ARTÍCULO 116: Las entidades con redes destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas están en la obligación de cumplir los aspectos siguientes:

a) Se enviarán las listas con los nombres, cargo, nivel científico y fundamentación para el servicio, para el Centro de Informática y Comunicaciones Nacional, para posteriormente ser aprobado por el Viceministro Primero Francisco Fereira Báez. Solamente él puede dar su aprobación.
b) Establecer las medidas y procedimientos de seguridad informática que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que lo reciben.
c) 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.
d) Dar a conocer a los clientes de estos servicios los requerimientos de seguridad informática que deben cumplir en correspondencia con las políticas de seguridad establecidas en la red que les da servicios.
e) Facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar con las mismas en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

ARTÍCULO 117: Ninguna persona, natural o jurídica está autorizada para explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas.

ARTÍCULO 118: Las cuentas de un servidor de correo electrónico de una entidad no podrán ser vinculadas a un servidor en el exterior para el acceso a los mismos a través de ellos.

ARTÍCULO 119: Cada entidad debe implementar mecanismos en los servidores de acceso para identificar y autenticar a los usuarios en correspondencia con el servicio que se les ha otorgado, y en los casos que se requiera, mecanismos que garanticen el registro y conservación de todos los accesos e intentos fallidos de acceso.

ARTÍCULO 120: La suscripción a cualquier tipo de lista de correo electrónico y el empleo de servicios de conversación en tiempo de real (Chat) y de voz sobre Internet, será autorizada en todos los casos por el Viceministro Primero del Organismo en correspondencia con los intereses de la misma.

ARTÍCULO 121: Los administradores serán responsables de la mejoría de los dominios que administran; cualquier problema que comprometa los valores de nuestra Revolución debe ser detectado e informado a los responsables de seguridad informática.

ARTÍCULO 122: Los administradores de redes deben crear las condiciones para que el responsable de seguridad informática, con la previa aprobación del jefe del Centro de Informática y Comunicaciones pueda monitorear los servidores; esa información será confidencial.

ARTÍCULO 123: No se deben usar los servicios de la red de alcance global para enviar información de trabajo.

ARTÍCULO 124: El nodo nacional garantizará:

a) El transporte de la mensajería de toda la Internet.
b) Eliminación de virus en los correos.
c) Entrada de spam y hoax siempre que este proceso no afecte el rendimiento de los servidores.
d) Lista de discusión como servicio complementario.

ARTÍCULO 125: Los administradores de los subnodos son responsables de tener instalados sistemas contra los programas malignos y virus, así como para spam y hoax.

ARTÍCULO 126:: El transporte de los servidores de correos se hará hacia los subdominios provinciales de segundo nivel.

ARTÍCULO 127: Si por necesidades de conectividad u otros intereses se requiere hospedar un sitio en servidores ubicados en un país extranjero, siempre se hará como espejo o replica del sitio principal en servidores ubicados en Cuba, estableciendo las medidas requeridas para garantizar su seguridad, particularmente durante el proceso de actualización de la información.

ARTÍCULO 128: Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sea de carácter informativo, comercial, cultural, social, con intenciones de engaño (hoax) u otros.

ARTÍCULO 129: Los subnodos deben garantizar la eliminación de spam y la entrada de virus, con un antivirus adecuado.

ARTÍCULO 130: Los ficheros adjuntos deben tener como máximo 1 MB, los ficheros que sean grandes se deben pasar por el protocolo de transferencia de ficheros (FTP) para evitar coalición en los servidores.

ARTÍCULO 131: No se deben mandar imágenes, ni propagandas y se deben utilizar formatos en txt; deben hacerse restricciones para evitar transferencias innecesarias.

ARTÍCULO 132: Cada entidad establecerá sus propios mecanismos para el tratamiento de incidentes y violaciones de la seguridad informática, asegurando la depuración de responsables de estas y las posibles alternativas a emplear para garantizar los servicios. Dicha estrategia deberá ser consecuente con los objetivos básicos de la entidad y tomará en consideración:

a) Los riesgos que la entidad enfrenta en términos de su probabilidad y su impacto, incluyendo una identificación y asignación de prioridades a los procesos críticos.
b) El impacto probable de las interrupciones sobre la gestión de la entidad.
c) Comprobar y actualizar regularmente los planes y procesos establecidos.

ARTÍCULO 133: El responsable de seguridad informática, ante la ocurrencia de violaciones de esta, estará en la obligación de comunicarlo inmediatamente a la dirección de la entidad la que, a su vez, deberá constituir de inmediato una comisión que investigue los hechos. En esta comisión deberá estar presente el responsable de seguridad informática, así como en los análisis correspondientes, y todas las personas que sean necesarias para el esclarecimiento de los hechos, siempre que no estén relacionadas con estos.

ARTÍCULO 134: Una vez establecida la estrategia a seguir, las entidades dispondrán las medidas y procedimientos que correspondan con el fin de garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos.

ARTÍCULO 135: Las medidas y procedimientos de recuperación serán definidos a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos y garantizarán las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios.

ARTÍCULO 136: Los procedimientos para la gestión de incidentes y violaciones de seguridad informática, especificarán los pasos a seguir para garantizar una correcta evaluación de lo que ha ocurrido, a quién, cómo y cuándo debe ser reportada la incidencia, la respuesta adecuada, así como los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial. Para ello se considerará lo siguiente:

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 de los incidentes.
d) El registro de todos los eventos vinculados con el incidente.

e) La recolección y preservación de las trazas de auditoria y otras evidencias.
f) Impacto y consecuencias de la incidencia.
g) La planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario.

ARTÍCULO 137: Los directores de los nodos o responsables de seguridad informática garantizarán que al producirse un incidente o violación de la seguridad informática, cualesquiera que sean, se informará de este acontecimiento inmediatamente a la Oficina de Seguridad para las Redes Informáticas y a la instancia superior de la entidad. Este reporte incluirá como mínimo:
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 V
OTRAS MEDIDAS DE PROTECCIÓN FÍSICAS

ARTÍCULO 138: Para la conexión o desconexión de los equipos a la red eléctrica, estos deben estar apagados, las líneas de alimentación eléctrica para las tecnologías informáticas deben ser independientes de la red común, o al menos no alimentar a equipos de fuerza o altos consumos.

ARTÍCULO 139: En caso de ocurrencia de tormentas eléctricas severas se apagarán y desconectarán todas las tecnologías informáticas, salvo aquellas que por necesidad imperiosa haya que dejar funcionando, en cuyo caso se crearán las condiciones necesarias para su protección.

ARTÍCULO 140: Las tecnologías informáticas fundamentales para la gestión de cada entidad deben estar conectadas a fuentes de respaldo de energía con estabilizadores de voltaje.

ARTÍCULO 141: Los locales en los cuales se encuentren instaladas tecnologías informáticas deberán estar debidamente climatizados según los requerimientos del fabricante.

ARTÍCULO 142: Los locales donde se encuentran los servidores deben estar seguros con cierres y alarmas y el acceso debe ser limitado.

ARTÍCULO 143: Los laboratorios de computación de los centros docentes deben cumplir con todo lo establecido en las normas y medidas de seguridad que se recogen en este Reglamento. Las máquinas de los laboratorios deben estar selladas y el técnico docente del laboratorio debe tener en su poder el formulario de las máquinas. El técnico docente del laboratorio es responsable, como el de seguridad informática, ambos deben velar por esto; además, se debe tener un estricto control en la cerradura de los laboratorios.

ARTÍCULO 144: En los laboratorios de computación de los centros docentes los usuarios de cada puesto de trabajo son los máximos responsables del orden del mobiliario, la limpieza y del cuidado de los equipos que se le han asignado en ese tiempo y deberán ordenar el puesto de trabajo y hacer entrega de los mismos antes de salir del local.

ARTÍCULO 145: En los laboratorios de computación de los centros docentes el responsable de seguridad informática conjuntamente con el técnico al frente del laboratorio, deberá mantener actualizada la libreta de incidencias del laboratorio de computación, el control del tiempo de máquina (nombre del usuario, carné de identidad, fecha y horario de entrada y salida, el puesto que ocupó, si es estudiante o profesor, lugares y sitios visitados y la firma del usuario) y llevar el formulario de cada equipo.

ARTÍCULO 146: En los laboratorios de computación de los centros docentes los técnicos de las entidades encargadas de la reparación del equipamiento es el único personal autorizado para abrir las computadoras.

ARTÍCULO 147: En los laboratorios de computación de los centros docentes las personas para trabajar con dispositivos de almacenamiento externos (disquetes, CD-ROM, memoria flash, discos externos) deberán solicitar al encargado del laboratorio su revisión (detección de virus y material que contiene).

ARTÍCULO 148: En los centros docentes, ante hechos de violación de la seguridad informática, se aplicarán las sanciones de acuerdo con lo establecido en el Capítulo de Sanciones.

CAPITULO VI
DE LA INSPECCIÓN A LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

ARTÍCULO 149: La supervisión a la seguridad de las tecnologías de la información se realizará mediante actividades de control e inspección.

ARTÍCULO 150: El Ministerio de la Informática y las Comunicaciones y el Ministerio del Interior tienen como atributo estatal la ejecución de inspecciones en materia de la Informática y las Comunicaciones.

ARTÍCULO 151: La inspección estatal en esta materia será ejecutada exclusivamente por los inspectores del Ministerio de la Informática y las Comunicaciones y del Ministerio del Interior.

SECCIÓN PRIMERA
OBJETIVOS.

ARTÍCULO 152: La inspección estatal a la Seguridad a las Tecnologías de la Información tiene los objetivos siguientes:

a) Evaluar los conocimientos y la aplicación de la base legal de seguridad informática 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) Valorar 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.

SECCIÓN SEGUNDA
FACULTADES DE LOS INSPECTORES

ARTÍCULO 153: Los inspectores de seguridad informática tienen las facultades siguientes:

a) Realizar la inspección con aviso previo o sin él.
b) Evaluar el estado del cumplimiento y aplicación de la base legal de 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 u otras de las previstas en el Artículo 155, Capítulo VIII de este Reglamento.
f) Recomendar la realización de auditorias.
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 hubiese.
i) Exigir la entrega de las trazas o registros de auditoria de las tecnologías de la información 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.

CAPÍTULO VII
VIOLACIONES INFORMÁTICAS

ARTÍCULO 154: Los usuarios que incurran en los siguientes tipos de violaciones, se les aplicará las sanciones propuestas en el Capítulo VIII y IX, teniendo en cuenta el impacto del hecho:

VIOLACIONES LEVES:

1. Mala manipulación.
2. Préstamo de identificadores de usuario de dominio.
3. Envió de cartas en cadenas.
4. Instalar juegos sin la debida autorización.
5. Jugar juegos que no sean didácticos.
6. Mala manipulación de los sistemas informáticos.
7. Instalación o desinstalación de software sin la autorización del responsable de seguridad informática.
8. No comunicar la presencia de virus informáticos u otros programas malignos en los activos informáticos.
9. Emplear falsa identificación o Nick Names en los recursos de comunicación.
10. No llevar un control debidamente actualizado de los usuarios con las tecnologías y locales informáticos por parte del responsable de los registros.
11. No poseer y utilizar programas antivirus no actualizados.
12. No escanear los dispositivos de almacenamiento extraíbles con el antivirus.
13. Poseer y utilizar en los laboratorios docentes o cualquier local destinado directamente a esta actividad, música, video o películas (**con fines no educativos**).
14. Poseer música, videos, películas o cualquier activo informático de modo que comprometa la utilización del medio.
15. Compartir recursos en la red sin los permisos y protecciones establecidas.
16. Enviar informes sin compactar en Winrar**.**
17. Enviar ficheros más de 1 MB.
18. No atender debidamente a los usuarios de la red.

VIOLACIONES GRAVES:

1. Crear cuentas de correo e Internet no autorizados.
2. Configurar máquinas sin la debida autorización.
3. Prestar cuenta de Internet o correo electrónico internacional a sujetos no autorizados a este servicio.

4. Prestar o mover medios sin la debida autorización.
5. Utilizar un bien informático con fines de lucro.
6. Introducir códigos malignos en cualquier bien informático.
7. Suplantar identidad.
8. Abrir medios o recursos informáticos por parte de personal no autorizado.
9. No controlar debidamente bienes o recursos informáticos bajo su protección.
10. Instalar programas sin la debida cuarentena técnica y autorización del personal facultado para ello.
11. Conectar equipos a la red sin la debida autorización.
12. No proteger debidamente los recursos informáticos o la red de agentes, intrusas, variaciones de tensión o descargas eléctricas.
13. Emplear los recursos informáticos para enviar cartas en cadenas con contenidos obscenos.
14. No cumplir con el sistema y reglamento de la Seguridad Informática en cualquiera de sus partes.
15. Divulgar y hacerse ecos, de informaciones no oficiales mediante la utilización de bienes informáticos
16. Hacer uso de cuentas ajenas de Internet o correo electrónico.
17. Encriptar información o protegerla mediante el uso de contraseñas sin la autorización del organismo facultado.
18. Enviar y reenviar información oficial a terceras personas no autorizadas a utilizar su contenido.
19. Emplear programas o utilitarios de informes o comunicación sin la debida autorización.

VIOLACIONES MUY GRAVES:

1. Utilización, acceso, difusión, publicación, transmisión y descarga de material contrario a los principios éticos, políticos y morales de la sociedad cubana.
   1.1. Subversión política.
   1.2. Pornografía y nudismo.
2. Transmisión y difusión de información confidencial o con cualquier tipo de clasificación según lo establecido en las legislaciones vigentes y en este Reglamento de nivel institucional como estatal.
3. Alterar y sustraer componentes del equipamiento informático.
4. Trasgresión de la seguridad de la red interna o de terceros mediante:
   4.1. Ejecución de software para la detección de vulnerabilidades de la red.
   4.2. Acceso, modificación o copia de las configuraciones de los servidores de la red en cuestión.
5. Creación de identificadores de usuarios (cuentas) a personas no autorizadas.
6. Creación de identificadores de usuarios (cuentas) a cualquier persona con ánimos de lucro.

7. Propiciar información, herramientas (informáticas o no) o medios que permitan vulnerar la seguridad de la red interna.
8. Abandono y negligencia por parte de los administradores en la configuración de las redes y servidores que propicien agujeros de seguridad en la red interna o comprometan de cualquier manera su funcionamiento.

CAPÍTULO VIII
DE LOS INCUMPLIMIENTOS

ARTÍCULO 155: Toda persona natural o jurídica que incumpla lo dispuesto en la presente Resolución Ministerial 176/07y en las disposiciones legales vigentes en la materia o cometa alguna de las violaciones anteriores, estará sujeta a la aplicación de las siguientes medidas:

a) Invalidación temporal o definitiva de las autorizaciones administrativamente concedidas por el Ministerio de la Informática y las Comunicaciones al infractor, entre ellas, cancelación de licencias, permisos, autorizaciones, desconexión parcial o total de las redes privadas de datos y otras.
b) Suspensión o cancelación, temporal o definitiva, de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano.
c) Ocupación cautelar de los medios, instrumentos, equipamientos y otros utilizados para cometer la infracción, con la finalidad de disponer posteriormente el decomiso de los mismos, según proceda.
d) La aplicación de las medidas que correspondan, de conformidad con lo legalmente establecido.

CAPÍTULO IX
SANCIONES

ARTÍCULO 156: Toda persona que incurra en las violaciones leves se les aplicará las medidas que se relacionan a continuación y según sea su impacto y consecuencia para la entidad se considerarán graves o muy graves.

Las sanciones son:
1. Llamada de atención.
2. Amonestación pública ante el colectivo del infractor.
3. Suspensión del servicio de correo electrónico e Internet.
4. Limitación inmediata del acceso al recurso informático.
5. Suspensión definitiva del servicio:
   5.1 Hasta 3 meses
   5.2 Hasta 6 meses
   5.3 Hasta 1 año
   5.4 Definitivo
6. Separación definitiva de la entidad

ARTÍCULO 157: Toda persona que incurra en las violaciones graves y muy graves u otro delito informático que no se recoja en este Reglamento, se analizará el impacto y las consecuencias de las mismas y se le aplicará las sanciones previstas en lo expresado en el Código Penal vigente.

ARTÍCULO 158: Toda persona natural o jurídica sujeta a la aplicación de las medidas descritas anteriormente, puede apelar la medida impuesta. Las apelaciones serían:

a) La apelación se realizará al Nodo Provincial en el plazo de 10 días hábiles contados a partir de la fecha de aplicada la medida. El jefe máximo donde se encuentra el Nodo Provincial dispondrá de 30 días hábiles para dar respuesta a dicha reclamación.
b) Según el fallo de la apelación del Nodo Provincial, podrá apelar ante el Ministerio de Educación en un plazo de 15 días hábiles contados a partir de que se emitió la respuesta de la apelación. A su vez, el Ministro dispondrá de 90 días hábiles para dar respuesta a dicha reclamación. La decisión de esta última instancia será inapelable.

ARTICULO 159: El Centro de Informática y Comunicaciones pondrá a la aprobación del Ministro, la medida de Prohibición de Servicio para entidades, instalaciones, empresas u otro tipo de objetivo educacional, que por detectarse en su sistema informático violaciones que representen peligro potencial para la red RIMED, deban ser separadas del sistema hasta que eliminen las deficiencias detectadas.

ARTICULO 160. La medida de prohibición de Servicio se aplicará a aquellas entidades, instalaciones, empresas u otro tipo de objetivo educacional, que presenten violaciones de esta magnitud:

a) Incumplimiento en cualquiera de los acápites del Acuerdo Marco firmado con el Nodo Rimed.
b) Incumplimiento o violaciones del Código de Ética firmado dentro del Convenio Marco con el Nodo Rimed.