REGLAMENTO SOBRE SEGURIDAD INFORMATICA

TITULO I

OBJETIVOS Y ALCANCE

ARTICULO 1: El presente Reglamento tiene por objeto establecer las medidas de Seguridad y Protección de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías informáticas y de comunicaciones, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información en ellas contenida; así como la Disciplina Informática, que regirá el trabajo con dichas tecnologías dirigida a preservar su integridad .

ARTICULO 2: A los efectos de este Reglamento el conjunto de las medidas de Seguridad y Protección de la Información, y de Disciplina Informática constituirán la Seguridad Informática, que comprende medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo o constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías informáticas y de comunicaciones; así como el correcto uso y conservación de las mismas.

ARTICULO 3: Este Reglamento será de aplicación en todos los Organos y Organismos de la Administración Central del Estado y sus dependencias, otras entidades estatales, empresas mixtas, y en todas aquellas empresas que operen en el territorio nacional, siendo de obligatorio cumplimiento por todas las personas que participen en la elaboración, uso, aplicación, explotación, y mantenimiento de las Tecnologías Informáticas y de Comunicaciones.

El responsable del cumplimiento de lo dispuesto en el párrafo anterior será el jefe máximo de cada entidad.

ARTICULO 4: La información que se procese, intercambia, reproduzca y conserve a través de los medios técnicos de computación se considera un bien de cada entidad.

ARTICULO 5: Se considerará información sensible a los efectos de esta norma aquella que sin ser clasificada pueda considerarse vital por las entidades para sus operaciones científicas, comerciales, económicas, entre otras, y cuya pérdida o modificación no autorizada altere o pueda alterar la capacidad de gestión de la misma, ocasione ó pueda ocasionar, pérdidas en valores, o pueda ser perjudicial para la integridad física o moral de una persona.

Su acceso, uso y divulgación inadecuada implicará la responsabilidad que corresponda.

TITULO II

DEL ESTABLECIMIENTO DE LAS MEDIDAS ADMINISTRATIVAS SOBRE LA SEGURIDAD INFORMATICA.

CAPITULO I

POLITICAS Y PLANES DE SEGURIDAD INFORMATICA

Sección 1

Políticas sobre Seguridad Informática.

ARTICULO 6: Cada administración adecuará la política, que establecerá en su entidad acorde a las regulaciones vigentes, que regirá la seguridad de la información que se procese, intercambie, reproduzca o conserve a través de las tecnologías informáticas y de comunicaciones; determinar los tipos de información y recursos para su protección; y crear y establecer los mecanismos de control para garantizar el cumplimiento de las regulaciones previstas en este reglamento.

ARTICULO 7: Con el fin de garantizar la correcta adecuación de la política a seguir para lograr la Seguridad Informática en cada entidad, se hará un análisis de la gestión informática, que debe abarcar : su organización, flujo de la información, tecnologías de información disponibles, alcance de la actividad informática dentro y fuera de la entidad, categoría de clasificación de la información que se procesa, determinación de la información sensible para la actividad fundamental de la entidad y los controles establecidos; que brinden los elementos indispensables para evaluar la vulnerabilidad del sistema y los principales riesgos a que esté expuesto.

Sección 2

Plan de Seguridad Informática.

ARTICULO 8: Cada entidad garantizará , según corresponda a la actividad informática que se desarrolle, que se elabore, ponga en vigor, cumpla y actualice periódicamente el Plan de Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidad realizados.

ARTICULO 9: El Plan de Seguridad Informática y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia entidad y por el Ministerio del Interior.

Sección 3

Plan de contingencia para la Seguridad Informática.

ARTICULO 10: El Plan de contingencia para la Seguridad Informática se instituye como una exigencia para todas las entidades, con el fin de garantizar la continuidad de los procesos informáticos ante cualquier desastre que pueda ocurrir.

ARTICULO 11: El Plan de contingencia para la Seguridad Informática, contendrá las funciones que permitan, en caso de desastres, la evacuación, preservación y traslado, de los medios y soportes destinados al procesamiento, intercambio y conservación de información clasificada o sensible. Así mismo,contemplará las medidas pertinentes para la conservación y custodia de los ficheros creados con fines de salvaguarda.

CAPITULO II

MEDIDAS DE PROTECCION FISICA PARA LA SEGURIDAD INFORMATICA.

Sección 1

Medidas de protección física en áreas vitales.

ARTICULO 12: Se consideran áreas vitales aquellas donde se procese, intercambie, reproduzca y conserve a través de los sistemas informáticos y de comunicaciones información clasificada, en dichas áreas se aplicarán las medidas de protección física siguientes:

a) se ubicarán en locales de construcción sólida, cuyas puertas y ventanas estén provistas de cierres seguros y dispositivos de sellaje, preferiblemente en los niveles más bajos de la edificación; debiendo cumplir con los requerimientos básicos que reduzcan al mínimo las probabilidades de captación de las irradiaciones electromagnéticas que los medios técnicos de computación y comunicaciones emiten;

b) a los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que eviten la visibilidad hacia el interior del mismo; y

c) aplicar sistemas de detección y alarma en todos los lugares que lo requieran.

ARTICULO 13: La entrada o permanencia en las áreas vitales estará en correspondencia con el nivel de acceso a la información clasificada que se le haya otorgado a las personas. En el caso del personal de limpieza, mantenimiento de equipos u otro que eventualmente precise permanecer en el área lo hará siempre en presencia de las personas responsables y con la identificación visible.

ARTICULO 14: Se aplicarán accesorios o medidas alternativas que permitan la creación de una barrera física o tecnológica de protección a las tecnologías informáticas y de comunicaciones, que posibiliten el control de acceso a la información, al uso de las

facilidades de intercambio no autorizadas, o impidan el uso de estos medios para cometer acciones malintencionadas o delictivas.

Sección 2

Medidas de protección física en áreas reservadas.

ARTICULO 15: Se consideran áreas reservadas aquellas donde el volumen o sensibilidad de la información que se procese, intercambie, reproduzca y conserve a través de los medios de los sistemas informáticos resulte de importancia para la gestión principal de la entidad, en aquellas áreas se aplicarán las normas técnicas establecidas de acuerdo a las características de cada lugar.

ARTICULO 16: La entrada o permanencia de las personas en las áreas reservadas deber ser controlada, requiriéndose la autorización expresa de la persona facultada para ello. En el caso del personal de limpieza, mantenimiento de equipos u otro que eventualmente precise permanecer en el área lo hará siempre en presencia de las personas responsables y con la identificación visible.

Sección 3

Medidas de protección física a los soportes.

ARTICULO 17: Todos los soportes removibles que contengan información clasificada serán controlados y custodiados en la oficina de control de la información clasificada o en el área responsabilizada, según lo establecido para su protección, y se crearán las condiciones para su conservación.

ARTICULO 18: Los soportes pertenecientes a una entidad, serán controlados por los responsables designados, debiendo reflejar además los datos del control en los soportes removibles que lo permitan, señalizándolos de forma clara y visible, con la categoría de clasificación de la información de más alto valor contenida en el mismo.

ARTICULO 19: Para utilizar soportes de propiedad personal o de otra entidad, será necesario contar con la autorización del jefe administrativo del lugar, debiendo ser revisados contra virus u otros programas dañinos, aplicándose los controles establecidos.

ARTICULO 20: En los casos que el jefe de la entidad autorice a que se procese o conserve información clasificada en soportes de otra entidad, los mismos serán controlados con las medidas establecidas para la protección del Secreto Estatal. Una vez concluído su uso, se efectuará la destrucción física de la información.

ARTICULO 21: El traslado de los soportes tiene que realizarse respetando las normas de conservación de los mismos, con el objetivo de garantizar la integridad y confidencialidad de la información que contienen y cumplirán las medidas de protección establecidas de acuerdo a la categoría de clasificación de la misma.

ARTICULO 22: La información clasificada contenida en soportes de información se destruirá físicamente una vez concluida su utilización, mediante el uso de desmagnetizadores, sobrescrituras (al menos cinco escrituras).

ARTICULO 23: La entrada y salida de soportes no clasificados en las áreas donde se procese información clasificada se hará con la autorización del Jefe de la misma, el cual será el responsable de que a su salida no sean contentivos de información clasificada.

CAPITULO III

SEGURIDAD TECNICA O LOGICA

ARTICULO 24: Las medidas y controles para la seguridad técnica o lógica de las tecnologías informáticas y de comunicación, que se establecen en este Capítulo, serán de imple-mentación a nivel de software y hardware y estarán en correspondencia directa con las políticas y modelos de seguridad que se determinen en cada entidad .

ARTICULO 25: A las tecnologías informáticas y de comunicación en que se procese, intercambie, reproduzca y conserve información clasificada o sensible, se les implementarán mecanismos de identificación y autenticación de usuarios que no permitan su duplicidad y dificulten su detección.

ARTICULO 26: Siempre que sea factible, se implementarán mecanismos de control que permitan contar con una traza o registro de los principales eventos que se ejecuten y puedan ser de interés para la detección o esclarecimiento ante violaciones de la seguridad Informática.

ARTICULO 27: Solamente podrá intercambiarse información clasificada a través de las tecnologías informáticas y de comunicación utilizando sistemas de protección criptográfica diseñados y producidos por entidades debidamente certificadas por el Ministerio del Interior.

ARTICULO 28: A partir de la entrada en vigor de este Reglamento, las aplicaciones destinadas al procesamiento de información clasificada tendrán que estar en capacidad de asignar en la pantalla y en cada hoja de la salida por la impresora, la categoría de clasificación de la información, o el término de advertencia "Para uso del servicio", según corresponda. En los casos de los documentos o bases de datos multinivel, se visualizará la categoría de clasificación de mayor nivel contenida en los mismos .

ARTICULO 29: Todas las aplicaciones destinadas al procesamiento de información clasificada o sensible, reunirán los requisitos siguientes:

a) incluir claramente documentadas las políticas de acceso que por características propias de la gestión de la entidad, sean necesarias aplicar, partiendo del nivel de confidencialidad de la información que procesan,

b) marcar los objetos con los distintos niveles de clasificación de la información que permita la aplicación del control, acorde a los niveles de acceso otorgado a los sujetos informáticos;

c) contar con la capacidad de registrar todas las operaciones principales, realizadas en el tratamiento de bases de datos que contengan información clasificada o sensible.

ARTICULO 30: Se dotarán de protección contra ataques o alteraciones no autorizadas, a los mecanismos de seguridad técnica que se apliquen, tanto a nivel de sistema operativo como de aplicaciones.

ARTICULO 31: Se contará con salvas actualizadas de las informaciones, con el fin de recuperarlas o restaurarlas en los casos de pérdida, destrucción o modificación mal intencionadas o fortuitas, de acuerdo a la clasificación o importancia de la información que protegen.

ARTICULO 32: Las entidades estarán obligadas a proteger por vía del software y del hardware a los programas y datos que no requieran actualización periódica, así como a garantizar que los soportes removibles estén también protegidos físicamente contra escritura.

ARTICULO 33: En dependencia de las características técnicas de los equipos se aplicarán detectores automatizados de violaciones, que permitan conocer y neutralizar las acciones que constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información.

ARTICULO 34: Todo software antes de su puesta en explotación, se someterá a una cuarentena técnica con el objetivo de detectar acciones de los mismos que pongan en riesgo la integridad, confidencialidad y disponibilidad de la información en el lugar donde vayan a ser utilizados.

ARTICULO 35: Todo software que se adquiera debe quedar controlado en un registro que se confeccionará en cada entidad.

ARTICULO 36: En las tecnologías informáticas y de comunicación en que se procese información clasificada, se aplicarán mecanismos de protección que controlen el acceso a través de los dispositivos de soportes removibles no autorizados.

TITULO III

SEGURIDAD DE OPERACIONES

CAPITULO I

GENERALIDADES

ARTICULO 37: Toda entidad tiene que mantener actualizado el inventario de las tecnologías informáticas y de comunicaciones que posean, identificando además aquellos que sean utilizados para procesar información clasificada.

ARTICULO 38: La reparación o mantenimiento de los equipos destinados al procesamiento de información clasificada se realizará una vez borrada físicamente la información. En los casos en que la información, por imposibilidad técnica o de explotación, no pueda ser borrada, el personal responsabilizado con su reparación queda obligado a cumplir lo dispuesto por la Ley del Secreto Estatal, y a destruir todos los ficheros y materiales resultantes de las pruebas técnicas realizadas que puedan contener información clasificada .

ARTICULO 39: Cuando las tecnologías informáticas y de comunicaciones no reúnan los requisitos técnicos que permitan garantizar el cumplimiento de lo establecido por este reglamento para la conservación y tratamiento de la información clasificada, el usuario estará obligado a borrar la información clasificada que en ellas se contenga.

CAPITULO II

DE LA DESIGNACION Y FUNCIONES DEL RESPONSABLE DE LA SEGURIDAD INFORMATICA.

Sección 1

Designación

ARTICULO 40: Las entidades en las que se operen tecnologías informáticas y de comunicaciones, en dependencia de sus características y necesidades designarán, de entre aquellas personas que trabajen directamente con las mismas, aquella con la experiencia y confiabilidad suficientes para ser Responsable de la Seguridad Informática. El máximo responsable de la Seguridad Informática en cada área será el Jefe administrativo de la misma.

ARTICULO 41: Cuando las características propias de la entidad y el volumen y dispersión de las tecnologías informáticas y de comunicaciones instaladas así lo aconsejen, se podrá designar más de un funcionario para la atención de la Seguridad Informática en las diferentes áreas de trabajo.

Sección 2

Funciones

ARTICULO 42: Son funciones del Responsable de la Seguridad Informática en cada entidad las siguientes:

a) Participar en la elaboración del plan de contingencia y el Reglamento Técnico Organizativo para garantizar la Seguridad Informática en la entidad.

b) Elaborar los procedimientos indispensables para garantizar la correcta explotación de los sistemas informáticos.

c) 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.

d) Verificar de forma sistemática la integridad de todo software que se encuentre autorizado para su explotación.

e) Comunicar al Jefe administrativo de su área cuando en ella no se posean los productos de protección actualizados y certificados de acuerdo a las normas recogidas en el presente Reglamento, y a las condiciones del trabajo del área.

f) 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.

g) Crear las condiciones necesarias para la ejecución de las disposiciones establecidas por el artículo 34 de este Reglamento, con relación a las cuarentenas y revisión de los soportes que se introduzcan en la entidad.

h) Apoyar el trabajo del Jefe de Protección y el Jefe Administrativo, en cuanto al estudio y aplicación del sistema de seguridad a los sistemas informáticos, y en la determinación de las causas y condiciones que propician un hecho de violación en el uso y conservación de los sistemas informáticos y la información que se procese en ellos.

i) Velar por la capacitación del personal con el objetivo de contribuir al conocimiento y cumplimiento de las medidas establecidas en este reglamento por el personal vinculado a esta actividad.

j) 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.

k) Analizar periódicamente los registros de auditoría

l) Elaborar y mantener el plan de contingencia

CAPITULO III

DEL TRABAJO EN REDES

Sección 1

Seguridad de las operaciones en el ambiente de las redes de datos.

ARTICULO 43: Los jefes de las entidades responderán por la designación del personal técnico y administrativo que opere en las redes de datos, los que deberán contar con la preparación y confiabilidad requeridas. Asimismo, determinarán la información que suministrarán a la red.

ARTICULO 44: Cada entidad establecerá las reglamentaciones necesarias para la organización, estructura y funciones de las redes de datos.

ARTICULO 45: Se prohíbe la conexión de las máquinas donde se procese información clasificada a las redes de datos de alcance global.

ARTICULO 46: Son de obligatoria implementación los mecanismos de seguridad de los cuales están provistos las redes de datos; así como de aquellos que permitan filtrar o depurar la información que se intercambie, de acuerdo a los intereses predeterminados por cada una de ellas.

ARTICULO 47: Quien detecte indicios de difusión de mensajes contrarios al interés social, la moral y las buenas costumbres, o la integridad o seguridad del Estado, debe comunicarlo al administrador de la red.

Sección 2

Funciones del administrador de una red, en relación con la Seguridad Informática.

ARTICULO 48: Toda red de computadoras deberá contar para su operación con la existencia de un Administrador que tendrá entre sus funciones básicas:

a) Administrar los recursos de la red.

b) Velar por la protección de los datos que en ella se procesan o se transmiten.

c) Proteger la integridad del funcionamiento de la red.

d) Establecer un código para la protección contra intrusos en la red.

e) Definir y hacer conocer a todos sus usuarios las normas éticas que regirán el trabajo y las transmisiones de dicha red.

f) Velar porque la misma no sea utilizada para otros fines distintos a aquellos para los que fue creada, y que conste en la Licencia otorgada a la red.

g) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de acciones nocivas que se identifiquen.

h) Contar con un mecanismo de coordinación y aviso con el resto de las redes nacionales y el MININT que permita accionar de conjunto ante la ocurrencia de hechos.

TITULO IV

SOBRE LA PRESTACION DE SERVICIOS DE SEGURIDAD INFORMATICA A TERCEROS.

ARTICULO 49: Solo estarán autorizadas a brindar servicios de Seguridad Informática a terceros aquellas entidades que cuenten con el correspondiente certificado de autorización emitido de forma conjunta por el Ministerio del Interior y por el Ministerio de la Industria Sideromecánica y la Electrónica.

ARTICULO 50: Los criterios a tener en cuenta para emitir el certificado de autorización para prestar servicios de Seguridad Informática serán los siguientes:

a) Nivel técnico de los especialistas que laboren en la entidad.

b) Que el objeto social de dicha entidad coincida con estos fines.

c) Que dicha entidad cuente con mecanismos eficientes que garanticen la calidad y respuesta rápida de los servicios, y la confiabilidad del personal.

d) Que la entidad esté realmente 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 durante su trabajo tenga acceso.

f) Que los productos informáticos que utilicen estén debidamente certificados por la Dirección Nacional de Informática.

g) Que el capital sea enteramente nacional y el personal encargado de brindar los servicios sea ciudadano cubano residente permanentemente en el país.

TITULO V

DE LA PROTECCION CONTRA VIRUS INFORMATICOS.

ARTICULO 51: Toda entidad donde se operen tecnologías informáticas y de comunicaciones, está obligada a implementar medidas de protección contra virus informáticos, en correspondencia con sus condiciones específicas.

ARTICULO 52: Ante indicios de contaminación por un virus informático nuevo o desconocido se deberá aislar el mismo o preservarlo hasta la llegada de los especialistas, quedando prohíbido el intercambio de códigos de virus entre cualesquieras otras personas o grupos de personas.

ARTICULO 53: La contaminación por un virus informático nuevo o desconocido deberá ser reportada a una entidad especializada en Servicios de Protección contra virus Informáticos, autorizada a operar en el territorio nacional y se procederá como se establece en el artículo 66 del presente Reglamento, además de entregar los informes.

ARTICULO 54: La Dirección Nacional de Informática del SIME actuará como centro coordinador, a fin de garantizar la actualización de todas las entidades autorizadas a prestar servicios de protección contra virus informáticos, en lo referido a virus de nueva aparición.

ARTICULO 55: Los productos antivirus que se utilicen deberán estar certificados por un Grupo de Expertos que a tal efecto convocará la Dirección Nacional de Informática del SIME, casuísticamente. Este Grupo de Experto estará conformado por especialistas de los Organismos de la Administración Cental del Estado.

ARTICULO 56: Estos Grupos de Expertos para emitir su dictamen deberán tener en cuenta los siguientes aspectos:

a) Adecuación a las plataformas tecnológicas de uso en el país.

b) Efectividad contra virus informáticos nacionales.

c) Grado de actualización del producto. (que tome en cuenta los últimos virus informáticos detectados en Cuba).

d) Completamiento (que proteja contra la mayor cantidad de virus informáticos conocidos posible).

e) Otros aspectos que considere importantes.

ARTICULO 57: En los casos de trabajo en redes deberán implementarse medios de protección antivirus para la verificación de los programas que se recepcionen.

ARTICULO 58: Los organizadores en Cuba de eventos, exposiciones o ferias que hagan uso de sistemas informáticos, garantizarán, por si mismos o mediante contratación, servicios de detección y protección contra virus informáticos para todos los medios que se utilicen en dichas actividades.

TITULO VI

EVENTOS, EXPOSICIONES O FERIAS

ARTICULO 59: Las entidades que organicen o participen en eventos, exposiciones o ferias nacionales o internacionales, responden porque en los mismos no se introduzcan y diseminen virus informáticos, para lo cual tomarán las medidas correspondientes antes y durante el evento.

ARTICULO 60: Los medios técnicos de computación y los soportes que sean utilizados en eventos, exposiciones o ferias, no podrán contener información clasificada, ni información que comprometa de alguna manera la gestión de la entidad.

ARTICULO 61: El Comité Organizador del evento, exposición o ferias, exigirá al participante, un documento en el que se autorice, por el máximo jefe de la entidad de que proceden, o en quien este delegue, el traslado al recinto ferial de los equipos y soportes de computación de su entidad.

ARTICULO 62: Los equipos y soportes de computación, que hayan sido utilizados en eventos, exposiciones o ferias, tanto nacionales como internacionales, deben ser sometidos a una cuarentena técnica antes de su reutilización por la entidad.

TITULO VII

SALIDA AL EXTERIOR DE LAS TECNOLOGIAS INFORMATICAS Y SUS SOPORTES.

ARTICULO 63: El traslado al extranjero de tecnologías informáticas y de comunicación, con información clasificada o sensible, solo será autorizado de acuerdo con lo establecido en la Legislación vigente.

ARTICULO 64: La persona responsabilizada con el Control de la Información Clasificada, en coordinación con el Responsable de Seguridad Informática comprobará si las tecnologías informáticas y de comunicación y los soportes que se trasladarán al extranjero, contienen solo la información que se autoriza para ello, así como que estén libres de virus informáticos.

ARTICULO 65: Las tecnologías informáticas y de comunicación, y los soportes que hayan sido trasladados al exterior, antes de ser utilizados nuevamente en las entidades deberán ser sometidos a cuarentena técnica.

TITULO VIII

ENFRENTAMIENTO A LOS HECHOS DETECTADOS EN EL FUNCIONAMIENTO Y EL USO DE LOS MEDIOS TECNICOS DE COMPUTACION.

ARTICULO 66: El Responsable de Seguridad Informática, ante posibles violaciones de las medidas de protección establecidas en este Reglamento informará de inmediato al Jefe de Protección o al Jefe de la entidad, quien creará una comisión encargada de realizar las investigaciones necesarias para determinar si constituye un hecho y comunicarlo al Organo de Protección del Ministerio del Interior.