RESOLUCION No. 204 / 96

POR CUANTO: **Conforme a los dispuesto en el Decreto Ley No. 147 de 21 de abril de 1994, el actualmente denominado Ministerio de la Industria Sidero Mecánica y la Electrónica, creado por la Ley No. 1282 de 26 de diciembre de 1974, permanece como un Organismo de la Administración del Estado._____**

POR CUANTO: **El que resuelve fue designado Ministro de la Industria Sidero Mecánica por Acuerdo del Consejo de Estado de fecha 1ro. de noviembre de 1990 y ratificado en el actualmente denominado Ministerio de la Industria Sidero Mecánica y la Electrónica por Acuerdo del propio Consejo de Estado del 21 de abril de 1994._**

POR CUANTO: **En el Decreto 209 del Consejo de Ministros de 1996, se determinan las Normas y Regulaciones para el acceso desde Cuba a redes Informáticas de alcance global y se establecen las misiones para los Organismos en el marco de su competencia._____**

POR CUANTO: **La Resolución No. 3 del extinguido Instituto Nacional de Sistemas Automatizados y Técnicas de Computación (INSAC), puesta en vigor en fecha 4 de marzo de 1992 reguló los aspectos relativos a la protección de programas informáticos, específicamente en cuanto a la protección contra virus; la que ya resulta insuficiente, dada la problemática actual._____**

POR CUANTO: **El desarrollo de los Sistemas de Informáticos requiere una disposición que contenga las normas básicas de Protección y Seguridad Técnica de los Sistemas Informáticos, entendida ésta como el correcto uso y conservación de dichos sistemas._____**

POR TANTO: **En uso de las facultades que me están conferidas, dicto el siguiente:**

REGLAMENTO SOBRE LA PROTECCION Y SEGURIDAD TECNICA DE LOS SISTEMAS INFORMATICOS

CAPITULO I

OBJETIVOS Y ALCANCE

ARTICULO 1: El presente Reglamento tiene por objeto establecer las medidas de Protección y Seguridad Técnica a aplicar en el trabajo con las tecnologías informáticas, las que incluyen los medios técnicos y los programas, así como establecer las normas de Disciplina Informática.

ARTICULO 2: A los efectos de este Reglamento se entenderá por Protección y Seguridad Técnica de los Sistemas Informáticos al conjunto de medidas administrativas, organizativas, físico-tecnológicas, técnicas, legales y educativas dirigidas a preservar la integridad de las tecnologías informáticas.

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, asociaciones económicas internacionales, que se constituyan conforme a la ley, y a los efectos de este Reglamento "entidades"; siendo de obligatorio cumplimiento por todas las personas que participen en la elaboración, uso, aplicación, explotación, y mantenimiento de las tecnologías informáticas en estos organismos o entidades.

En el caso de las empresas de capital totalmente extranjero u otras instituciones extranjeras o no gubernamentales que operen en el territorio nacional será de obligatorio cumplimiento lo que en este Reglamento se dispone en los Capítulos V, VI, VII y VIII.

CAPITULO II

ESTABLECIMIENTO DE LAS MEDIDAS ADMINISTRATIVAS PARA LA PROTECCION Y SEGURIDAD DE LOS SISTEMAS INFORMATICOS.

ARTICULO 4: Cada entidad debe tomar en consideración para la elaboración del Plan de Seguridad Informática orientado por el Ministerio del Interior, la estrategia de desarrollo y aplicación de la Informática, orientada por el Ministerio de la Industria Sideromecánica y la Electrónica (en lo adelante SIME) , a través de su unidad organizativa que asesora y ejerce la rectoría de la actividad Informática en el país.

ARTICULO 5: Cada entidad elaborará su Reglamento de Seguridad Informática adecuando a sus condiciones específicas los aspectos planteados en el Reglamento de Seguridad Informática del Ministerio del Interior (en lo adelante MININT) y en el presente Reglamento.

ARTICULO 6: En el Plan de Contingencias orientado por el MININT, se considerarán además los diversos componentes del sistema, tales como: Aplicaciones, equipos de procesamiento, software, salvas, documentación y el personal. Además, contemplará todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: Suministro de potencia, sistemas de climatización, instalaciones y toda otra cuestión que influya en el correcto funcionamiento de las tecnologías informáticas.

ARTICULO 7: El Plan de Contingencias para la Seguridad Informática y su aplicación serán objeto de control por parte del SIME, sin perjuicio de los controles que puedan realizar otros organismos facultados para ello.

ARTICULO 8: La persona que sea designada Responsable de la Seguridad Informática en cada entidad, tiene además de las asignadas por el MININT, las siguientes funciones:

a) Establecer el chequeo previo y posterior de toda las tecnologías informáticas y los soportes tecnológicos de información que participen en eventos, ferias, exposiciones u otras actividades similares de carácter nacional e internacional, o que hayan sido trasladados por cualquier razón fuera de la entidad, antes de ser utilizados nuevamente, con el objetivo de evitar la posible propagación de virus informáticos, u otros efectos que puedan atentar contra el correcto funcionamiento de estos;

b) controlar que se verifique de forma sistemática la integridad de todo software que se encuentre en explotación;

c) comunicar a los jefes administrativos cuando las áreas de trabajo no se posean las herramientas tecnológicas de protección actualizadas y certificadas de acuerdo a las normas recogidas en el presente Reglamento;

d) definir las condiciones necesarias para la ejecución de las disposiciones establecidas en este Reglamento, con relación a las cuarentenas técnicas establecida en el artículo 23, y revisión de los soportes tecnológicos de información que se introduzcan en la entidad;

e) proponer el plan para la capacitación del personal vinculado a esta actividad, con el objetivo de contribuir al conocimiento y cumplimiento de las disposiciones de este Reglamento, así como el resto de las normativas que sobre esta materia se emitan;

f) analizar periódicamente los registros de auditoría informática;

ARTICULO 9: Se establece con carácter obligatorio el uso del ¨ Libro de Incidencias¨ para las áreas de las entidades donde se utilicen las tecnologías informáticas, y en el mismo se anotarán todos aquellos eventos que revistan un interés especial , tales como, roturas,

mantenimientos, traslados, uso de estas tecnologías por personal ajeno a la entidad, aparición de virus informáticos, y otros.

CAPITULO III

REQUERIMIENTOS TECNICOS PARA LA PROTECCION Y SEGURIDAD DE LAS TECNOLOGIAS INFORMATICAS.

ARTICULO 10: Al instalar las tecnologías informáticas se tendrá en cuenta la protección contra los siguientes fenómenos físicos:

a) Desastres naturales como penetraciones del mar, fuego, huracán y terremotos;

b) accidentes como inundaciones del inmueble, cortes de energía eléctrica e interferencias, derrumbes y otros.

ARTICULO 11: Para la conexión o desconexión de los equipos a la red eléctrica, estos deben estar apagados. Todos las tecnologías informáticas y los tomacorrientes deberán tener señalizado el voltaje a que trabajan o suministran.

ARTICULO 12: Las líneas de alimentación eléctrica para las tecnologías informáticas deben ser independientes de la red común de la edificación o al menos no alimentar a equipos de fuerza o altos consumos a la misma red.

ARTICULO 13: En caso de ocurrencia de tormentas eléctricas severas se apagarán y desconectarán todas las tecnologías informáticas, salvo aquellas que por imperiosa necesidad de explotación contínua haya que dejar funcionando.

ARTICULO 14: Debe garantizarse la climatización y/o ventilación especificada por el fabricante de las tecnologías informáticas, así como el cumplimiento del mantenimiento periódico de las mismas. En todos los casos se debe evitar los efectos de la humedad y el polvo.

ARTICULO 15: Las tecnologías informáticas fundamentales para la operación de sistemas informáticos, tales como los servidores, deberán estar conectados a fuentes de respaldo de energía y éstas deberán poseer limitadores de voltaje.

ARTICULO 16: Los soportes tecnológicos de información que contengan las salvas de la copias de los programas y sistemas pertenecientes a cada entidad, serán registrados, debiéndose reflejar los datos de control establecidos.

ARTICULO 17: La instalación de las tecnologías informáticas debe realizarse de forma alejada de aquellos equipos que emitan cualquier tipo de señal electromagnética que pueda afectar el correcto funcionamiento de las mismas.

CAPITULO IV

MEDIDAS DE SEGURIDAD TECNICA O LOGICA

ARTICULO 18: A los efectos de este Reglamento, se entenderá por Seguridad Técnica o Lógica al conjunto de medidas que se implementan mediante medios de programas o medios tecnológicos encaminada a proteger las tecnologías informáticas, y sus soportes tecnológicos de información, los cuales estarán en correspondencia directa con las políticas y modelos de seguridad que se determinan en cada entidad.

ARTICULO 19: Toda entidad tiene que mantener actualizado el inventario de las tecnologías informáticas que posean.

ARTICULO 20: Siempre que los sistemas operativos lo permitan, deben ser implementados mecanismos de control lógicos que permitan contar con una traza o registro de los principales eventos que se ejecuten durante el uso de las tecnologías informáticas.

ARTICULO 21: Un juego de soportes tecnológicos de información conteniendo las salvas de la copia de seguridad tanto de los programas y sistemas informáticos vitales para el trabajo de cada entidad, como de aquellos que fueron elaborados a la medida para el trabajo de la misma, se conservará en la entidad y otro en al menos un lugar distante a la misma, que cumpla con las condiciones técnicas y seguridad necesarias, para evitar su destrucción en caso de accidentes.

ARTICULO 22: Todas las entidades estarán obligadas a proteger por vía del software y por medios técnicos a los programas y sistemas informáticos que no requieran actualización periódica, así como a garantizar que los soportes tecnológicos de información que contienen las salvas de los programas y sistemas, estén también protegidos físicamente contra escritura.

ARTICULO 23: Se entiende por cuarentena técnica al proceso de comprobar los parámetros de los programas y sistemas de aplicación informáticos para detectar cualquier anomalía en los mismos, que pueda afectar el normal funcionamiento de los equipos.

ARTICULO 24: Todo software adquirido, antes de su puesta en explotación, se someterá a una cuarentena técnica.

ARTICULO 25: En el caso de que los Sistemas Informáticos de Aplicación lo requieran, se utilizarán sistemas operativos y sistemas de aplicación seguros, así como se tendrán en cuenta los aspectos de seguridad establecidos para realizar el diseño, la programación, la puesta a punto y el mantenimiento de los programas.

CAPITULO V

DE LA PROTECCION CONTRA VIRUS INFORMATICOS Y OTRAS MEDIDAS DE SEGURIDAD TECNICA.

ARTICULO 26: Toda entidad donde se operen tecnologías informáticas, está obligada a implementar medidas de protección contra virus informáticos, en correspondencia con sus condiciones específicas.

ARTICULO 27: Las medidas básicas de protección contra virus informáticos que deben ser implementadas en cada entidad, son las siguientes:

a) Poseer los productos antivirus certificados;

b) poseer los productos antivirus actualizados;

c) mantener actualizados los patrones identificativos de los programas que están en explotación;

d) efectuar el correspondiente chequeo a todos los soportes tecnológicos de información ajenos a la entidad, antes de su utilización;

e) mantener protegido contra escritura a los soportes tecnológicos de información originales de los software básicos (sistemas operativos, utilitarios, lenguajes) y sistemas de aplicación, que no requieran de actualización periódica;

f) antes de transmitir y posterior a recibir sistemas y programas mediante los soportes de comunicaciones se utilizará un programa identificador/ descontaminador de virus para revisar los ficheros ejecutables.

ARTICULO 28: Ante indicios de contaminación por algún virus informático nuevo o desconocido se deberá aislar el mismo o apagar y preservar el equipo infectado, debiendo reportarlo y entregarlo a una de las entidades nacionales autorizadas para brindar los servicios técnicos de Seguridad Informática, quienes a su vez deberán informarlo a los órganos correspondientes del MININT.

ARTICULO 29: Queda totalmente prohíbido el intercambio de códigos de virus informáticos entre personas o grupos de personas, excepto los autorizados por la Dirección de Informática del SIME.

ARTICULO 30: La Dirección 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.

ARTICULO 31: Los productos antivirus que se utilicen deberán estar certificados por un Grupo de Expertos que a tal efecto convocará la Dirección de Informática del SIME, casuísticamente. Este Grupo de Expertos estará conformado por especialistas seleccionados de distintas entidades.

ARTICULO 32: El Grupo de Expertos para emitir su dictamen deberá tener en cuenta los siguientes aspectos:

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

b) efectividad para la detección y descontaminación de virus informáticos internacionales y nacionales;

c) grado de actualización del producto, el cual debe permitir su actualización periódica;

d) completamiento (que detecte la presencia de nuevas versiones y nuevos virus);

e) otros aspectos que se consideren importantes.

ARTICULO 33: Se prohibe la utilización, distribución y comercialización de herramientas tecnológicas de protección y seguridad técnica de los sistemas informáticos que no cuenten con la aprobación previa de la Dirección de Informática del SIME.

CAPITULO VI

PRESTACION A TERCEROS DE SERVICIOS DE PROTECCION Y SEGURIDAD TECNICA DE LOS SISTEMAS INFORMATICOS.

ARTICULO 34: Solo estarán autorizadas a brindar a otras instituciones servicios de protección y seguridad técnica de los sistemas informáticos, aquellas entidades que cuenten con el correspondiente certificado de autorización emitido por el SIME.

ARTICULO 35: Los criterios a tener en cuenta para emitir el certificado de autorización para prestar servicios de protección y seguridad técnica de los sistemas informáticos 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;

d) que la entidad esté realmente en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;

f) que las herramientas tecnológicas de protección y seguridad técnica de los sistemas informáticos que utilicen estén debidamente certificados por la Dirección de Informática del SIME;

g) que el personal encargado de brindar los servicios técnicos tenga la ciudadanía cubana.

CAPITULO VII

SEGURIDAD TECNICA EN ENTORNO DE REDES

ARTICULO 36: Cada entidad que administre y opere una red de transmisión de datos debe elaborar el Reglamento para el funcionamiento interno de la misma.

ARTICULO 37: Deben ser implementados medios de detección de virus para la verificación de los programas que se recepcionen, los cuales deben estar debidamente actualizados y certificados.

ARTICULO 38: En cada entidad donde opere una red de transmisión de datos, debe ser dsignado el Administrador de la red, el cual deberá contar con la preparación técnica y confiabilidad requeridas.

ARTICULO 39: En materia de protección y seguridad técnica, son funciones del administrador de una red de transmisión de datos las siguientes:

a) Administrar los recursos de la red;

b) velar por la protección de la integridad del funcionamiento de la red;

c) elaborar y hacer conocer el Reglamento Interno que regirá el trabajo y las transmisiones de dicha red;

d) implementar el cumplimiento de lo establecido en el Reglamento Interno, así como proponer las medidas necesarias con los infractores.

ARTICULO 40: Cada administración de una red de transmisión de datos está en libertad de seleccionar el protocolo para la comunicación entre sus diferentes miembros, al igual que el sistema operativo que utilizará.

ARTICULO 41: Cada cuenta o buzón de correo electrónico tendrá un operador, que será la persona responsabilizada con su uso, así como con la actualización periódica que garantice la confidencialidad de la palabra de acceso.

ARTICULO 42: En el caso específico de redes locales, éstas contarán con un responsable, que será un especialista miembro de la misma y que tendrá entre sus funciones las siguientes:

a) Proteger y administrar los recursos de la red;

b) mantener actualizados los productos antivirus;

c) implementar las opciones de seguridad que brindan los sistemas operativos para el trabajo en red;

d) proteger la integridad del funcionamiento de la red.

CAPITULO VIII

MEDIDAS ESPECIFICAS PARA LA PARTICIPACION EN EVENTOS, EXPOSICIONES, FERIAS Y VIAJES AL EXTERIOR

ARTICULO 43: Las entidades que organicen eventos, exposiciones o ferias nacionales o internacionales, responderán porque en los mismos no se introduzcan y diseminen virus informáticos, para lo cual garantizarán los servicios de protección contra virus informáticos antes y durante el evento.

ARTICULO 44: El Comité Organizador de eventos, exposiciones o ferias en que participen tecnologías informáticas está en la obligación de ofrecer los servicios de detección y descontaminación de virus informáticos durante el evento, bien directamente o a través de una entidad autorizada a prestar servicios a terceros, contratada a tal efecto.

ARTICULO 45: Las tecnologías informáticas y los soportes tecnológicos de información que hayan sido utilizados en eventos, exposiciones o ferias, tanto nacionales como internacionales, así como los que por otras razones hayan salido al exterior, serán sometidas a una cuarentena técnica antes de su reutilización por la entidad.

CAPITULO IX

DISPOSICIONES FINALES

PRIMERO: El "Reglamento sobre Protección y Seguridad Técnica de los Sistemas Informáticos" entrará en vigor a partir de la fecha de publicación de la presente Resolución en la Gaceta Oficial de la República.

SEGUNDO: Se deroga la Resolución No. 3 del INSAC, de 4 de marzo de 1992.

TERCERO: Notifíquese a los Organos y Organismos de la Administración Central del Estado, Organos del Poder Popular y Organizaciones Políticas y de Masas, y a cuantas más personas naturales o jurídicas proceda, y publíquese en la Gaceta Oficial de la República para general conocimiento.

DADA en la Ciudad de la Habana, a los 20 días del mes de noviembre de 1996. "Año del Centenario de la Caída en Combate de Antonio Maceo".

Ignacio González Planas
Ministro de la Industria
Sideromecánica y la Electrónica