RESOLUCION No. 39 /2002

POR CUANTO: El Decreto Ley No. 204 de fecha 11 de enero del 2000 cambió la denominación actual del Ministerio de Comunicaciones por la del Ministerio de la Informática y las Comunicaciones, que desarrollará las tareas y funciones que hasta el presente realizaba el Ministerio de Comunicaciones, así como las de Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero-Mecánica y la Electrónica.

POR CUANTO: El Consejo de Estado de la República de Cuba, mediante Acuerdo de fecha 12 de enero del 2000, designó al que resuelve Ministro de la Informática y las Comunicaciones.

POR CUANTO: De conformidad con el Acuerdo No. 2817 de 25 de noviembre de 1994, adoptado por el Comité Ejecutivo del Consejo de Ministros, corresponde a los Jefes de los Organismos de la Administración Central del Estado, dictar, en el límite de sus facultades y competencia, reglamentos, resoluciones y otras disposiciones de obligatorio cumplimiento para el sistema del organismo, y en su caso, para los demás organismos, el sector mixto, privado y la población.

POR CUANTO: El Decreto Ley no. 199 de fecha 25 de noviembre de 1999, " Sobre la Seguridad y Protección de la Información Oficial", se establece la responsabilidad de los Organismos de la Administración Central del Estado ante las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de la información.

POR CUANTO: La Resolución No. 6 de fecha 18 de noviembre de 1996, del Ministerio del Interior, puso en vigor el Reglamento sobre la Seguridad Informática, que estableció los principios, requerimientos y criterios de seguridad informática que garanticen la confiabilidad, integridad y disponibilidad de la información que se procese, intercambia, reproduce y conserva mediante el uso de las tecnologías de la información.

POR CUANTO: La Resolución No. 204 de fecha 20 de noviembre de 1996, del Ministerio de la Industria Sideromecánica y la Electrónica, puso en vigor el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, que estableció 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.

POR CUANTO: Resulta necesario a partir del análisis de los riegos previamente realizados establecer las Políticas de Seguridad Informática del Ministerio de la Informática y las Comunicaciones.

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

RESUELVO:

PRIMERO: Poner en vigor las Políticas de Seguridad Informática del Ministerio de la Informática y las Comunicaciones, que se anexan a la presente formando parte de la misma.

SEGUNDO: Notificar a los Viceministros, Jefe de Despacho, Directores Ministeriales, Presidentes de Grupos Empresariales, Directores de Empresas y a cuantas más personas deban conocerla. Archívese el original en la Dirección Jurídica del Ministerio de la Informática y las Comunicaciones.

Dada en la ciudad de la Habana, a los 3 días del mes de abril del 2002.
"Año de los Héroes Prisioneros del Imperio".

Ignacio González Planas
Ministro

CERTIFICO:

Que la presente Resolución Ministerial es fotocopia de la *original que obra en nuestros archivos y fuera firmada por el Ministro. Y para que así conste, firmo la presente a los 4 días del mes de abril del 2002.*

Lic. Zenaida C. Marrero Ponce de León
Directora Jurídica

ANEXO

Políticas de Seguridad Informática del Ministerio de la Informática y las Comunicaciones

I Aspectos generales

I.1 Cada empresa o entidad del MIC, sobre la base de lo regulado en las disposiciones legales expuestas en los Por Cuantos Tercero, Cuarto y Quinto de la presente Resolución y en las Políticas de Seguridad Informática del MIC, está en la obligación de diseñar, implantar y mantener actualizado, un Sistema de Seguridad Informática ajustado a sus características, con el fin de alcanzar los siguientes objetivos:

a) a) Minimizar los riesgos sobre los sistemas informáticos.
b) b) Garantizar la continuidad de los procesos informáticos.

I.2 Las empresas y entidades diseñarán sus Sistemas de Seguridad Informática considerando el conjunto de bienes informáticos, a partir de su importancia, los riesgos a que están sometidos y el papel que representan para el cumplimiento de su actividad, conformando con ello la estrategia de cómo tratar los aspectos de seguridad. Debe prestarse una especial atención a la determinación de los activos y recursos críticos para la gestión de la entidad. Se consideran activos y recursos críticos aquellos sin los cuales el trabajo de la entidad no tuviera sentido o no puede ser ejecutado.

I.3 El proceso de diseño del Sistema de Seguridad Informática de cada empresa o entidad se realizará mediante la creación de un equipo multidisciplinario formado por los que funcionalmente responden por el procesamiento de la información. Como expresión gráfica del Sistema de Seguridad Informática diseñado se elaborará o actualizará el Plan de Seguridad Informática.

I.4 Las Entidades que operen con tecnologías de información, designarán un Responsable de Seguridad Informática con la experiencia y confiabilidad requerida. Cuando las características propias de la Entidad y el 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.

Así mismo todas las redes de computadoras deberán contar para su operación con la existencia de una persona que se encargue de su administración.

I.5 A partir de las políticas establecidas, cada Entidad implementará las medidas

y procedimientos específicos que se deberán cumplir para la protección de los bienes informáticos, en correspondencia con el nivel de riesgo que se haya estimado para cada uno de ellos, debiendo ser definidas de manera clara y precisa, evitando interpretaciones ambiguas por parte de los responsabilizados con su cumplimiento.

II Empleo conveniente y seguro de las tecnologías.

II.1 La utilización de las tecnologías y sus servicios asociados en cada Entidad tiene que estar aprobado previamente por la dirección de la misma y basado, en cada caso, en una vigente necesidad de uso por razones de la actividad de la propia Entidad. El empleo de estos medios con otros fines, solo se realizará de forma excepcional y debidamente autorizada en cada caso.

II.2 El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una violación de los derechos de la entidad y se considera un abuso de confianza que es sancionable.

II.3 Es un derecho de la dirección de cada Entidad la supervisión del empleo de las tecnologías de la información por parte de los usuarios.

II.4 Los Jefes a cada nivel, garantizarán que el personal vinculado a las tecnologías de la información se entrene previamente para la utilización de las mismas, así como que suscriban un documento impreso donde conste que conocen los deberes y derechos que a cada cual corresponde en relación con el Sistema de Seguridad Informática implementado.

II.5 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 entrada y salida de la misma. Se establece como principio que cada uno de los bienes informáticos en cada entidad tienen que ser asignados a una persona, que actuando por delegación de la Dirección de la Entidad, es responsable de su protección.

II.6 Cada Entidad responderá por las acciones, que desde las tecnologías en ella instaladas, se realicen contra los sistemas informáticos de otras Entidades.

II.7 Ningún usuario está autorizado a introducir, ejecutar, distribuir o conservar en los medios de cómputo programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres. De ser necesaria la utilización de programas de este tipo como herramienta de autodiagnóstico 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.

III Atribuciones, Funciones y Obligaciones en materia de Seguridad Informática.

III.1 Atribuciones, Funciones y Obligaciones de los Directores de Empresas y Entidades en cuanto al control y cumplimiento de lo establecido en materia de Seguridad Informática:

a) Establecer los niveles de seguridad apropiados durante el empleo de las tecnologías de la información.
b) Garantizar la elaboración, aprobación, puesta en vigor y cumplimiento de los Planes de Seguridad Informática.
c) Autorizar y controlar el procesamiento de información clasificada y limitada en las tecnologías de información.
d) Autorizar y controlar la introducción y utilización de software básico y de aplicaciones en las tecnologías de la información.
e) Asegurar 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.
f) Actuar en correspondencia con lo establecido ante la ocurrencia de incidentes y violaciones de Seguridad Informática.
g) Designar el personal que responde por la dirección, ejecución y control del Sistema de Seguridad Informática y garantizar su preparación.

II.2 Atribuciones, Funciones y Obligaciones de los Jefes de Direcciones, Departamentos, Areas y Grupos de trabajo en cada Empresa o Entidad en relación con los bienes informáticos que le han sido asignados:

a) a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos.
b) b) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática en la parte que concierne a su esfera de acción y garantizar su cumplimiento.
c) c) Aplicar las medidas y procedimientos establecidas en su área de responsabilidad.
d) d) Especificar a los usuarios las medidas y procedimientos establecidos y controlar su cumplimiento.
e) e) Participar en la elaboración de los procedimientos de recuperación ante contingencias y en sus pruebas periódicas.
f) f) Imponer o proponer sanciones ante violaciones del sistema de seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

III.3 Atribuciones, Funciones y Obligaciones del Jefe de la actividad Informática en cada Empresa o Entidad:

a) a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática de la Entidad, velar por su aplicación y disciplina de cumplimiento.
b) b) Establecer y mantener los controles en correspondencia con el nivel de protección requerido por el Sistema de Seguridad Informática diseñado para la Entidad.
c) c) Garantizar la disponibilidad de los bienes informáticos.
d) d) Asesorar a los distintos niveles sobre los aspectos técnicos vinculados con la Seguridad Informática.
e) e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la Dirección de la Entidad, así como que se cumplan en éstos los requerimientos de Seguridad Informática.
f) f) Participar en la elaboración de los procedimientos de recuperación ante contingencias y en sus pruebas periódicas.
g) g) Informar a los usuarios de las regulaciones establecidas.

III.4 Funciones y Obligaciones del Responsable de Seguridad Informática de cada Entidad:

a) a) Controlar la aplicación del Plan de Seguridad Informática y participar en su actualización.
b) b) Comunicar al Jefe administrativo cuando en un área no se posean los productos de seguridad informática actualizados, de acuerdo a las normas establecidas y a las condiciones de trabajo de la misma, así como cualquier otro tipo de violaciones de la seguridad.
c) 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 alguna de las existentes.
d) 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 en la base legal vigente.
e) e) Controlar la utilización y realizar el análisis periódico de los registros de Seguridad Informática que se establezcan.
f) f) Participar en las comisiones que se constituyan para la investigación de incidentes.

III.5 Funciones y Obligaciones del Administrador de una red con relación a la Seguridad informática:

a) a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
b) b) Informar a los usuarios de las regulaciones de seguridad establecidas.
c) c) Garantizar que los servicios implementados sean utilizados para los fines

que fueron creados.

d) d) Comunicar a la dirección de la Entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
e) e) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de acciones nocivas que se identifiquen.

III.6 No deberán coincidir en una misma persona las funciones de Responsable de Seguridad Informática y las de administración de una red.

III.7 Obligaciones de los usuarios de las tecnologías de información en cada Entidad:

a) a) Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.
b) b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquier activo o recurso.
c) c) Utilizar las tecnologías de información solo en interés de la Entidad.
d) d) No intentar transgredir ninguna de las medidas de seguridad establecidas.
e) 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 el sistema al que esté conectada.
f) f) No introducir ni utilizar en las tecnologías ningún producto ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
g) g) Conocer la clasificación de los activos de información que maneja.
h) h) No divulgar información clasificada o limitada sin la autorización del dirigente facultado.
i) i) Cumplir las reglas establecidas para el empleo de las contraseñas.
j) j) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

III. 8 Al determinar las Atribuciones, Funciones y Obligaciones que se asignan al personal se tendrá en cuenta el principio de distribución de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona, a fin de reducir oportunidades de alteración no autorizada o mal uso de los sistemas informáticos. Esto es particularmente importante en sistemas que procesen información económica, donde deben estar separadas, por ejemplo, las funciones de programación, de las de explotación.

IV Identificación, autenticación y control de accesos

IV.1 Implementar mecanismos a las tecnologías de información para identificar y autenticar a los usuarios en correspondencia con el empleo a que estén

destinadas y a la información que en ellas se procese, intercambie, reproduzca y conserve, y en los casos que se requiera, mecanismos que garanticen el registro y conservación de todos los accesos e intentos fallidos de acceso. Cuando se trate de sistemas contables y otros sistemas críticos solo se deberá acceder a sus bases de datos mediante los procedimientos establecidos para ello.

IV.2 Definir 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.

IV.3 En caso de que un identificador de usuario tenga que ser compartido por un grupo de personas, no se puede acceder con él a información que el resto del grupo no deba conocer y siempre que sea posible, la contraseña no debe ser compartida, para permitir la identificación de la persona que lo está utilizando, así como implementar controles que eviten su uso no autorizado.

IV.4 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 responsable del usuario.

IV.5 En caso de terminación de la necesidad del uso de los sistemas por el cese de la relación laboral, 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 de un usuario a un sistema inmediatamente después de la notificación de su director. 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.

IV.6 Para la utilización de contraseñas como método de autenticación de usuarios, se cumplirán los siguientes requisitos:

a) a) Tienen que ser privadas e intransferibles.
b) b) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen.
c) c) No pueden ser visualizadas en pantalla mientras se teclean.

d) d) No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.

e) e) Se guardará copia de las mismas, de forma que garantice su privacidad, para su empleo como excepción en caso de ausencia del propietario.

IV.7 Definir en cada Entidad los procedimientos que se requieran para otorgar o suspender acceso a usuarios a los sistemas informáticos y los perfiles de trabajo de los mismos. Estos procedimientos incluirán la conformación de un listado de usuarios autorizados con sus derechos de acceso, garantizando la eliminación de aquellos que ya no los requieran por razones de trabajo o por el cese de la relación laboral, así como de los identificadores, junto a todos los derechos de acceso que le fueron concedidos.

IV.8 Implementar en cada Entidad los mecanismos de seguridad que eviten la modificación, destrucción y pérdida de los ficheros y datos.

IV.9 Establecer las medidas para proteger los programas del sistema y sus mecanismos de control de que cualquier usuario pueda utilizarlos, borrarlos o modificarlos con el fin de evitar los controles de seguridad.

V Protección Física

V.1 Identificar y controlar por parte de las Entidades las tecnologías de información que posea, instrumentando las medidas y procedimientos para garantizar el control sobre su entrada y salida de la misma.

V.2 Determinar en cada Entidad 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 de medidas de protección física a ellas directamente aplicadas. Para ello se definirán áreas vitales y reservadas que garanticen la aplicación de medidas alternativas que permitan la creación de una barrera de protección a estos medios e impidan su empleo para cometer acciones malintencionadas o delictivas.

V.3 Las tecnologías de información se protegerán contra posibles hurtos, ya sea de éstas o sus componentes, así como del robo de la información que contienen.

V.4 Para la conexión o desconexión de los equipos a la red eléctrica, éstos 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.

V.5 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.

V.6 Las tecnologías informáticas fundamentales para la gestión de cada entidad deben estar conectadas a fuentes de respaldo de energía con estabilizadores de voltaje.

VI Protección contra virus y otros programas dañinos.

VI.1 Implementar en cada Entidad las medidas y procedimientos que sean necesarios para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización. Para ello contará con las versiones actualizadas de los productos de software antivirus nacionales y si se emplea conexión a Internet también poseerán un antivirus internacional. En ambos casos se entrenará al personal para su correcta utilización.

VI.2 Cada software y programa de aplicación que llegue a la entidad se someterá a un proceso de revisión para detectar cualquier anomalía, así mismo se chequeará sistemáticamente la integridad del software que está en explotación.

VI.3 Ante indicios de contaminación por un virus informático se aislará y preservará el medio presumiblemente afectado y se informará al Responsable de Seguridad Informática, el cual establecerá la vía de contaminación y controlará el proceso de revisión de los soportes con los cuales haya trabajado el medio contaminado.

VI.4 Al trabajar con aplicaciones de Microsoft Office se activarán las protecciones estándares, que posibilitan abrir ficheros sin “macros” y proteger la plantilla normal.dot.

VI.5 Para el envío de “anexos” a través del correo electrónico es necesario que el remitente exprese al destinatario que le adjunta un fichero y además su nombre y longitud en bytes.

VI.6 Al recibirse un anexo por correo electrónico el mismo será sometido al proceso de revisión. Como norma todo anexo que se reciba de parte de alguien desconocido, que no haya sido solicitado, debe borrarse.

VI.7 Durante el acceso a Internet se conformarán adecuadamente las zonas de seguridad disponibles en el navegador que se esté utilizando, de forma tal que permita un trabajo seguro. Se tomarán además las medidas que correspondan

para evitar la descarga de algún tipo de software procedente de sitios de dudosa seguridad o el establecimiento de cualquier conexión que posibilite la instalación subrepticia de programas maliciosos.

VI. 8 Para la utilización de soportes de propiedad personal o de otra entidad, será necesario contar con la autorización del Jefe facultado para ello, y efectuar la correspondiente revisión contra programas dañinos.

VII Salvas de Información.

VII.1 Establecer en cada Entidad los procedimientos que garanticen las copias de seguridad (salvas) actualizadas de programas y datos, con el fin de recuperarlos o restaurarlos en los casos de pérdida, destrucción o modificación mal intencionada o fortuita, así como su salvaguarda, de manera que garantice la confidencialidad e integridad de la información ante cualquier contingencia.

VII.2 Se deben conservar salvas adicionales de la información de importancia crítica para la Entidad y del software y las aplicaciones más importantes en locales alternativos alejados de las áreas donde se procesa normalmente, con el fin de lograr su restablecimiento en caso de ocurrir alguna catástrofe.

VII.3 Realizar sistemáticamente copias de seguridad o salvas de la información de los servidores y del software de las aplicaciones que se utilizan en la entidad. La periodicidad de estas salvas estará en correspondencia con la actualización de la información y las aplicaciones.

VII.4 Cada 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.

VII.5 La Administración de cada Entidad garantizará a los usuarios los soportes informáticos que permitan realizar sus copias de seguridad.

VIII Seguridad en Redes

VIII.1Implementar los mecanismos de seguridad de los cuales están provistas las redes, 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.

VIII.2 Prohibir la adición de 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 del Director de la Entidad, garantizando su

compatibilización con las medidas de seguridad establecidas para la protección de dicha red.

VIII.3 Habilitar en todas las redes las opciones de seguridad con que cuentan los sistemas operativos de forma tal que se garantice la protección de los servidores, el acceso a la información solamente por personal autorizado y los elementos que permitan el monitoreo y auditoria de los principales eventos.

VIII.4 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.

VIII.5 Prohibir la conexión de las máquinas donde se procese información clasificada a redes con conectividad al exterior de la Entidad.

VIII.6 Instalar en las redes que prevean conexiones desde o hacia el exterior 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.

VIII.7 Implementar mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda, en las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos.

VIII.8 Las Entidades que coloquen información en servidores, en el territorio nacional o en el extranjero, para su acceso público desde otros sitios, establecerán las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con los intereses de la propia Entidad y del país.

VIII.9 Tomar las medidas que correspondan por parte de las Entidades, a fin de evitar que los servidores destinados a conexiones externas de una red sean instalados en las mismas máquinas en que se instalen los servidores destinados para el uso interno de dicha red.

VIII.10 Comunicar a las instancias pertinentes cuando se detecten indicios de difusión de mensajes contrarios al interés social, la moral y las buenas costumbres, la integridad o seguridad del Estado.

IX Empleo de los servicios en redes externas

IX.1 Los servicios que ofrecen las redes de datos mediante una conexión externa solo se utilizarán en interés de cada Entidad. La asignación de cuentas para el empleo de los diferentes servicios será aprobada en todos los casos por la Dirección de la Entidad sobre la base de las necesidades requeridas para el funcionamiento de la misma.

IX.2 El acceso a cualquier tipo de servicio de Internet a partir de otro servicio (por ejemplo acceder al E-Mail desde el Web) tiene que responder a la Política que establezca cada Entidad al respecto y bajo ningún concepto a los intereses o iniciativa personal de un trabajador.

IX.3 Ningún trabajador tiene derecho a establecer una cuenta de correo en servidores que se encuentran en el exterior y brindan estos servicios de forma gratuita. Si de manera excepcional por no haber otra alternativa, surgiera esta necesidad de manera puntual, tiene que ser aprobada previamente por el Director de la entidad, 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.

IX.4 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 mensajes a través del mismo.

IX.5 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.

IX.6 Se prohibe la generación de cartas en cadena y el envío de mensajes de correo a más de 15 destinatarios. De requerirse excepcionalmente el envío de un mensaje a más destinatarios que los señalados, tendrá que ser autorizado por el Director de la Entidad.

IX.7 La suscripción a cualquier tipo de lista de correo electrónico y del empleo de servicios de conversación en tiempo real (chat) y de voz sobre Internet, será autorizada en todos los casos por la Dirección de cada Entidad en correspondencia con los intereses de la misma.

IX.8 Las Entidades con redes destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas están en la obligación de cumplir, haciendo referencia a los mismos en los correspondientes contratos, los aspectos siguientes:

a) a) Establecer las medidas y procedimientos de Seguridad Informática que garanticen la protección de los servicios a brindar y los intereses de seguridad de las Entidades que los reciben.
b) b) Dar a conocer a las Entidades que solicitan estos servicios los requerimientos de Seguridad Informática que deben cumplir en correspondencia con las políticas de seguridad establecidas en la red que los brinda.

X Tratamiento de la información oficial.

X.1 En las tecnologías de información en que se autorice procesar información clasificada o limitada, se cumplirán los siguientes requisitos:

a) a) Se ubicarán en áreas vitales o reservadas según corresponda.
b) b) Se aplicarán las medidas de protección previstas para este tipo de información.
c) c) Si se conserva información clasificada en los discos duros se aplicarán mecanismos de seguridad que controlen el acceso a esta información, considerando entre ellos el control de los dispositivos de soportes removibles y la utilización de sistemas criptográficos autorizados por el Ministerio del Interior.

X.2 Todas las aplicaciones destinadas al procesamiento de información clasificada o limitada, cumplirán los requisitos siguientes:

a) a) Poseer los mecanismos de control de acceso que por características propias de la gestión de la Entidad, sean necesarios aplicar, partiendo del nivel de clasificación de la información que procesan;
b) b) Prever la posibilidad de asignar en pantalla y en cada hoja de salida por la impresora, la categoría de clasificación de la información según corresponda. En los casos de documentos o bases de datos con distintos niveles de clasificación se marcarán con la categoría de clasificación de mayor nivel contenida en los mismos.
c) c) Registrar todas las operaciones principales, realizadas en el tratamiento de bases de datos.

X.3 En aquellos lugares donde se procesa o maneja información clasificada o limitada, se extremarán las medidas de precaución, como por ejemplo, el control de acceso a los locales y a las tecnologías informáticas, la destrucción física de esta información una vez concluido su uso, la utilización de técnicas criptográficas para el caso de intercambio de información clasificada a través de las tecnologías informáticas, entre otras.

X.4 Prohibir la transmisión de información oficial clasificada sin protección criptográfica. Los sistemas de protección criptográfica que se utilicen serán los autorizados por el Ministerio del Interior.

X.5 Establecer por parte de las Entidades las medidas y procedimientos para garantizar que los mantenimientos de los equipos, soportes y datos, se realicen en presencia y bajo la supervisión de personal responsable y que en caso de traslado de algún equipo fuera de la Entidad la información contenida en él sea protegida.

X.6 La reparación o mantenimiento de los equipos destinados al procesamiento de información clasificada o limitada se realizará una vez borrada físicamente la información que contienen, previa certificación del Responsable de Seguridad Informática.

X.7 Todos los soportes que contengan información clasificada serán controlados y conservados en la oficina de control de la información clasificada o en el área responsabilizada, según lo establecido en cada entidad. Dicha información se destruirá una vez concluida su utilización mediante el uso de desmagnetizadores y sobre escrituras físicas (al menos 5) u otros mecanismos que permitan su destrucción (formateo).

X.8 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.

X.9 Cuando se autorice a que se procese o conserve información oficial clasificada en soportes de otra Entidad, los mismos serán controlados con las medidas establecidas para su protección. Una vez concluido su uso, se efectuará la destrucción de la información.

X.10 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.

X.11 El traslado al extranjero de tecnologías de información contentivas de información clasificada, en los casos en que se autorice, se realizará según lo establecido en el Reglamento sobre Seguridad y Protección de la Información Oficial para este tipo de información.

X.13 Cada Entidad establecerá los procedimientos que garanticen la comprobación de que las tecnologías de información y los soportes que se trasladen al extranjero, no contengan información clasificada o limitada y solo la que se autorice.

XI Recuperación ante Contingencias

XI.1 Establecer por parte de las Entidades la estrategia a seguir ante cualquier contingencia que pueda producirse en correspondencia con la importancia de los activos de información y recursos informáticos que posean y las posibles alternativas a emplear para garantizar los servicios.

XI.2 Establecida la estrategia, cada Entidad dispondrá las medidas y procedimientos que correspondan con el fin de garantizar la continuidad, restablecimiento o recuperación de los procesos informáticos, ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro, el normal desarrollo de los mismos.

XI.3 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 para ello.

XII Tratamiento de Incidentes y violaciones de Seguridad Informática

XII.1 Establecer por parte de las Entidades los procedimientos para el tratamiento de incidentes y violaciones de Seguridad Informática, definiendo los pasos a seguir para garantizar una correcta evaluación de lo que ha ocurrido, a quien, como y cuando debe ser reportado, la respuesta adecuada, los aspectos relacionados con su documentación y las acciones a seguir una vez restablecida la situación inicial.

XII.2 Ante cualquier incidente que afecte la Seguridad Informática, se designará una comisión encargada de realizar las investigaciones necesarias, con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y establecer la conducta a seguir.

XIII Registros.

XIII.1 Habilitar un Libro de Incidencias sobre la Seguridad Informática por áreas donde se recojan todos aquellos hechos relevantes en este sentido: roturas, mantenimientos, traslados, aparición de virus, uso de las tecnologías informáticas por personal ajeno a la entidad, entre otros.

XIII.2 Registrar y controlar en cada entidad los soportes de información que contengan las salvas de las copias de programas y sistemas.

XIII.3 Mantener actualizado el inventario de las tecnologías informáticas que posea cada entidad.

XIII.4 Establecer para cada área el software autorizado a permanecer en la misma.

Adicionalmente cada entidad establecerá cuantos registros estime conveniente para lograr el control de sus recursos y el cumplimiento de las medidas de seguridad informáticas establecidas.