REGLAMENTO SOBRE SEGURIDAD

INFORMATICA

TITULO I

OBJETIVOS Y ALCANCE

ARTICULO 1: El presente Reglamento tiene por objeto establecer los principios, criterios y requerimientos de Seguridad Informática que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, siendo el Jefe máximo de cada entidad el responsable del cumplimiento de todo lo que en él se dispone .

ARTICULO 2: A los efectos de este Reglamento se entenderá por Seguridad Informática, el conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información.

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, sociedades y asociaciones económicas que se constituyan conforme a la Ley, (en lo adelante entidad), siendo de obligatorio cumplimiento por todas las personas que participen en el uso, aplicación, explotación y mantenimiento de las tecnologías de información.

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

TITULO II

ESTABLECIMIENTO DE LAS MEDIDAS ADMINISTRATIVAS SOBRE LA SEGURIDAD INFORMATICA.

CAPITULO I

POLITICAS Y PLANES DE SEGURIDAD INFORMATICA Y DE CONTINGENCIA

Sección 1

Políticas sobre Seguridad Informática.

ARTICULO 5: Cada administración adecuará la política, que establecerá en su entidad acorde a las regulaciones que rijan sobre la seguridad de la información que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, determinará los tipos de información y recursos para su protección, y creará y establecerá los mecanismos de control para garantizar el cumplimiento de las regulaciones previstas en este Reglamento.

ARTICULO 6: 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 7: El Plan de Seguridad Informática se instituye como una exigencia para todas las entidades, en el cual deben reflejar las políticas, estructura de gestión y el sistema de medidas, para la Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidad realizados. El máximo dirigente de cada entidad garantizará , según corresponda a la actividad informática que se desarrolle, que se elabore, ponga en vigor, cumpla y actualice periódicamente.

ARTICULO 8: El Plan de Seguridad Informática y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia entidad.

Sección 3

Plan de Contingencia para la Seguridad Informática.

ARTICULO 9: 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 10: El Plan de Contingencia para la Seguridad Informática, contendrá las medidas 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.

ARTICULO 11: El Plan de Contingencia y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia entidad.

CAPITULO II

SEGURIDAD FISICA

Sección 1

Requerimientos de protección física en áreas vitales.

ARTICULO 12: ***Se consideran áreas vitales aquellas donde se procese, intercambie, reproduzca y conserve información clasificada a través de las tecnologías de información , 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 servicios, 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 técnica de protección a las tecnologías de información, 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

Requerimientos de protección física en áreas reservadas.

ARTICULO 15: Se consideran áreas reservadas aquellas donde la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información sea sensible para la entidad y se aplicarán las normas de protección establecidas de acuerdo a las características de cada lugar.

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

Sección 3

Requerimientos de protección física a los soportes.

ARTICULO 17: 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 para su protección y conservación.

ARTICULO 18: Los soportes pertenecientes a una entidad, cuando contengan información clasificada o sensible, serán controlados ,debiendo reflejar los datos de control en los soportes removibles que lo

permitan, señalizándolos de forma clara y visible, con la categoría de clasificación de la información de mas alto valor contenida en los mismos.

ARTICULO 19: Para utilizar soportes de propiedad personal o de otra entidad, será necesario contar con la autorización del jefe administrativo del lugar, aplicándose los controles establecidos en los casos en que la información contenida en los mismos sea clasificada o sensible.

ARTICULO 20: Cuando 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 su protección. Una vez concluido su uso, se efectuará la destrucción 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 los soportes, se destruirá físicamente una vez concluida su utilización, mediante el uso de desmagnetizadores y sobreescrituras (al menos cinco escrituras) u otros mecanismos que permitan su destrucción.

ARTICULO 23: La entrada y salida de soportes contentivos de información no clasificada, 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: Los requerimientos para la seguridad técnica o lógica, que se establecen en este Capítulo, serán de implementación a nivel de software y hardware y estarán en correspondencia directa con las políticas y modelos de seguridad que para la información se determinen en cada entidad.

ARTICULO 25: A las tecnologías de información en que se procese, intercambie, reproduzca y conserve información clasificada o sensible, se les implementarán mecanismos para identificar y autenticar los usuarios.

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 de información utilizando sistemas de protección criptográfica diseñados y producidos por entidades debidamente certificadas por el Ministerio del Interior.

ARTICULO 28: A partir de la promulgación 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, según corresponda. En los casos de los documentos o bases de datos con distintos niveles de clasificación se marcarán con 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 clasificación 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; y***

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 intencionada o fortuitas, de acuerdo a la clasificación o importancia de la información que protegen.

ARTICULO 32: En dependencia de las características técnicas de los equipos se aplicarán detectores automatizados de violaciones, que permitan conocer y neutralizar las acciones que constituyan un riesgo para la confidencialidad, integridad y disponibilidad de la información.

ARTICULO 33: En las tecnologías de información en que se procese información clasificada o sensible, se aplicarán mecanismos de protección que controlen el acceso a través de los dispositivos de soportes removibles.

TITULO III

SEGURIDAD DE OPERACIONES

CAPITULO I

GENERALIDADES

ARTICULO 34: Toda entidad tiene que mantener identificadas las tecnologías de información que posean, en aquellos casos que sean utilizadas para procesar información clasificada.

ARTICULO 35: La reparación o mantenimiento de los equipos destinados al procesamiento de información clasificada se realizará una vez borrada físicamente la información. Cuando 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 dicha información.

ARTICULO 36: Cuando las tecnologías de información 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 está obligado a borrar físicamente la información clasificada que en ella se contenga.

ARTICULO 37: Se prohibe la utilización, distribución o comercialización de herramientas de Seguridad Informática que no cuenten con la aprobación del órgano correspondiente del Ministerio del Interior, sin perjuicio de las autorizaciones que puedan conceder otros organismos.

ARTICULO 38: 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.

CAPITULO II

DESIGNACION Y FUNCIONES DEL RESPONSABLE DE LA SEGURIDAD INFORMATICA.

Sección 1

Designación

ARTICULO 39: Las entidades que operen con tecnologías de información, en dependencia de sus características y necesidades designarán, a una persona con la experiencia y confiabilidad suficiente para ser Responsable de la Seguridad Informática.

ARTICULO 40: Cuando las características propias de la entidad y el volumen y dispersión de las tecnologías de información instaladas, así lo aconsejen, se podrá designar más de un responsable para la atención de la Seguridad Informática en las diferentes áreas de trabajo.

Sección 2

Funciones

ARTICULO 41: Son funciones del Responsable de Seguridad Informática en cada entidad las siguientes:

a) ser responsable de la aplicación y mantenimiento de los planes de seguridad informática y de contingencia;

b) comunicar al Jefe administrativo de su área cuando en ella no se posean los productos de seguridad informática actualizados y certificados, de acuerdo a las normas recogidas en el presente Reglamento, y a las condiciones de trabajo del área;

c) 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, con el fin de determinar las causas y condiciones que propician violaciones en el uso y conservación de estos sistemas y en la información que se procese en ellos;

d) ***proponer y controlar la capacitación del personal vinculado a esta actividad, con el objetivo de contribuir al conocimiento y cumplimiento de las medidas establecidas en el Plan de Seguridad Informática y en este Reglamento; y***

e) ***analizar periódicamente los registros de auditorías a la Seguridad Informática.***

CAPITULO III

TRABAJO EN REDES

Sección 1

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

ARTICULO 42: Se prohibe la conexión de las máquinas donde se procese información clasificada a las redes de datos de alcance global.

ARTICULO 43: Son de obligatoria implementación los mecanismos de seguridad de los cuales están provistas 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 44: Quien detecte indicios de difusión de mensajes contrarios al interés social, la moral y las buenas costumbres, la integridad o seguridad del Estado, debe comunicarlo al Administrador de la red y este al Titular de la misma.

Sección 2

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

ARTICULO 45: Toda red de computadoras deberá contar para su operación con la existencia de un Administrador que tendrá entre sus funciones básicas:

a) ***velar por la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red;***

b) ***velar porque la misma sea utilizada para los fines que fue creada;***

c) activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de acciones nocivas que se identifiquen; y

d) contar con un mecanismo de coordinación y aviso con el resto de las redes nacionales y el Ministerio del Interior, que permita actuar de conjunto ante la ocurrencia de violaciones.

TITULO IV

PRESTACION DE SERVICIOS DE SEGURIDAD INFORMATICA A TERCEROS.

ARTICULO 46: Solo estarán autorizadas a brindar servicios de Seguridad Informática a terceros aquellas entidades que cuenten con el correspondiente certificado de autorización emitido por el Ministerio del Interior sin perjuicio de las que puedan conceder otros organismos.

ARTICULO 47: Los criterios a tener en cuenta para emitir el certificado de autorización para prestar servicios de Seguridad Informática son los siguientes:

a) nivel técnico - profesional 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 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 de Seguridad Informática, que utilicen estén debidamente certificados por los órganos correspondientes del Ministerio del Interior sin perjuicio de los certificados que puedan conceder otros organismos facultados para ello; y***

g) ***que el capital sea enteramente nacional y el personal designado para brindar los servicios sea ciudadano cubano y resida de forma permanente en el país.***

TITULO V

SALIDA AL EXTERIOR DE LAS TECNOLOGIAS DE INFORMACION Y SUS SOPORTES.

ARTICULO 48: El traslado al extranjero de tecnologías de información contentivas de información clasificada, solo será autorizado de acuerdo con lo establecido en la legislación vigente.

ARTICULO 49: La persona responsabilizada con el control de la información clasificada, en coordinación con el Responsable de

Seguridad Informática, comprobará si las tecnologías de información y sus soportes que se trasladen al extranjero, contienen solo la información que se autoriza para ello, así como que estén libres de virus informáticos.

TITULO VI

ENFRENTAMIENTO A LAS VIOLACIONES DETECTADAS EN EL FUNCIONAMIENTO Y USO DE LAS TECNOLOGIAS DE INFORMACION

ARTICULO 50: El Responsable de Seguridad Informática, ante posibles violaciones de las medidas de protección establecidas en este Reglamento informará de inmediato al Jefe de la entidad o en quien este delegue, y se creará una comisión encargada de realizar las investigaciones necesarias y comunicarlo al órgano correspondiente del Ministerio del Interior.

ARTICULO 51: La comisión encargada de realizar las investigaciones ante la detección de violaciones, estará integrada por el Responsable de Seguridad Informática y dos personas más que cuenten con los conocimientos técnicos e informativos del área donde se hayan producido, siempre que no estén implicados en las mismas, con el fin de esclarecer lo ocurrido y precisar los responsables.