Ciencias de la Información ISSN: 0864-4659 Vol. 48, No. 3, septiembre-diciembre, pp. 41- 47, 2017

La protección de la información. Una visión desde las entidades educativas cubanas

The protection of the information. A vision from the cuban educational entities

Osmany Aguilera Almaguer
Edilberto de Jesús Pérez Alí Osmán
Rolando Rivero Cuesta

La protección de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, de forma tal que garantice su confidencialidad, integridad y disponibilidad.El presente trabajo tiene como objetivo ofrecer una alternativa que favorezca la protección de la información que se procese, intercambie, reproduzca o conserve a través de las tecnologías de la información en correspondencia con las funciones propias del trabajo para el que han sido destinadas.Ello permite el ajuste de las medidas de seguridad en correspondencia con la caracterización y organización de estas tecnologías en grupos o clases.

***Palabras clave**: datos, protección de la información, entidades educativas, tecnologías informáticas*

RESUMEN

ABSTRACT

The protection of the information depends on a group of administrative, organizational, physical, technical or logical, legal and educational measures, with an integral focus and in system, in such way that guarantees its confidentiality, integrity and readiness. The present work has as objective to offer an alternative that favors the protection of the information that is processed, exchange, reproduce or conserve through the technologies of the information in correspondence with the functions characteristic of the work for which have been assigned. It allows it the adjustment of the measures of security in correspondence with the characterization and organization of these technologies in groups or classes.

***Keywords**: data, protection of the information, educational entities, informatics technologies*

Introducción

El desarrollo constante y en ascenso de las tecnologías informáticas (TI), hace de ellas un factor a tener en cuenta para el desempeño profesional en cualquier área. La esfera educacional no escapa a este fenómeno contemporáneo. En nuestro país se han invertido cuantiosos recursos para llevar a cabo un programa de informatización de la sociedad, que ha permitido dotar de estas a todas los centros docentes del país.

La introducción de la informática en la educación está encaminada a preparar a las nuevas generaciones con la finalidad de que puedan utilizar de forma creadora y ética las bondades que ofrece el empleo de estas tecnologías en la solución de problemas de su contexto profesional o social, y puedan enfrentar el flujo creciente de información contradictoria que se genera y difunde continuamente a través de estas tecnologías informáticas, por lo que forma parte de su formación integral. Por ello, en las instituciones educativas cubanas, las TI se pueden encontrar en la docencia, en la elaboración de software, en la investigación, en la dirección o como soporte para brindar diversos servicios donde la información puede estar impresa, almacenada electrónicamente, trasmitida por correo o por medios electrónicos. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma

debería ser siempre protegida adecuadamente.

El recurso que hoy se considera más importante es la información. Para alcanzar un objetivo es preciso acceder a la información pertinente para llegar a tomar las decisiones adecuadas. Esto es especialmente importante en ambientes cada vez más interconectados. Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades.

La protección de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, de forma tal que garantice su confidencialidad, integridad y disponibilidad.

El presente trabajo tiene como objetivo ofrecer una alternativa que favorezca la protección de la información que se procese, intercambie, reproduzca o conserve a través de las TI en correspondencia con las funciones propias del trabajo para el que estas tecnologías han sido destinadas.

Métodos utilizados

Para elaborar el trabajo se emplearon los métodos de análisis y síntesis, inducción-deducción y la revisión de documentos, los cuales permitieron la elaboración de los indicadores para la caracterización de las tecnologías informáticas y su agrupación en clases, así como el método sistémico-estructural funcional para establecer cada una de las clases y su relación con los niveles de seguridad.

Resultados

La información tratada en las entidades educativas se ha convertido en el eslabón esencial para el desarrollo económico y social de las mismas, yaque la información es un bien más de su activo y, en muchos casos, prioritario sobre los restantes.

Dato e Información (diferencias y dependencias)

Estos dos elementos serán herramientas prioritarias para estudiar el tratamiento que las organizaciones dan a la información. Por ello, resulta necesario acotar y precisar qué se entiende por cada uno de esos conceptos.

Se considera dato, como la unidad mínima con la que se compone la información, los datos no tienen significado sin un contexto, y guarda relación con el espacio y el tiempo, es decir, el ciclo de vida de estos datos en un espacio y tiempo determinado, por lo que los datos son acaecidos físicos (pequeñas parcelas o trozos de la realidad), susceptibles de transportar cierta información. Poseen una naturaleza material y pueden ser considerados como soporte físico de la información, por ser acaecimientos físicos, son sencillos de capturar, estructurar, cuantificar o transferir, la expresión dato es sinónimo de señal. Los datos son la materia prima de la información.

Por su parte la información, es el conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento. Es el resultado de procesar o transformar los datos.

En las entidades educativas los datos se pueden procesar o transformar a través de las TI en función de las clases, la elaboración de software, la investigación, la dirección del proceso docente educativo o de brindar diversos servicios a trabajadores y estudiantes y por tanto la información es relevante en relación con el contexto.

Es por ello que el conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, para garantizar la protección de la información (en lo adelante seguridad de la información) deben estar en correspondencia con la importancia que tiene la información para la entidad educativa,y no se corra el riesgo de que estas medidas sean insuficientes para proteger la información o que sean impracticables por ser molestas o costosas.

Según ACISSI (2011), hoy en día no existe duda de que se está en una nueva era caracterizada porel uso masivo de la información, que adicionalmente ha acarreado mucha másrelevancia que en anteriores épocas, debido a lo cual es fundamental dentro de las organizaciones el poder detectar las vulnerabilidades del sistemade información para contrarrestar las amenazas y riesgos por el gran número de usuarios con potencial de ataque, que no tan solo se centran en el ambiente que se ubica fuera de la organización, sino también en los usuarios comunesque trabajan y son una gran amenaza a la seguridad si no se tienen políticasclaras de acceso a la información.

Lograr que la seguridad de la información se corresponda con la importancia de los bienes a proteger y de los riesgos a que están sometidos es el principal dilema que enfrentan las entidades educacionales, como se declara en el artículo 4 del Reglamento de Seguridad para las Tecnologías de la Información del Ministerio de la Informática y las Comunicaciones (Resolución Ministerial 127 del 2007), aplicablea todos los Órganos y Organismos de la Administración Central del Estado y sus dependencias; otras entidades estatales; empresas mixtas; sociedades y asociaciones económicas que posean o utilicen, en interés propio o de un tercero, tecnologías de la información.

¿Cómo resolver estacontradicción?

El análisis de las principales normas, guías, modelos, estándares y metodologías existentes en la bibliografía sobre seguridad de la información coinciden en que para garantizar la protección de la información es necesario establecer medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas estrechamente interrelacionadas pero con un carácter muy general, dejando a la entidades la adecuación de las mismas en correspondencia con sus objetivos.

Para poder contextualizar las normas, guías, modelo, estándares y metodologías existentes en el ámbito internacional a las entidades educativas cubanas fue necesario establecer un criterio que nos permitiera ajustar el conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas para garantizar la seguridad de la información que se procesa, intercambia, reproduzca o conserva a través de las tecnologías de información.

El análisis y valoración de la bibliografía relacionada con el tema, la aplicación de varios instrumentos empíricos como entrevistas y el análisis de riesgo y la experiencia de los autores como especialistas de seguridad informática condujeron a establecer como criterio la caracterización de la tecnología de la información y como

indicadores para la caracterización de la información que se procesa, según sus funciones y el cargo del usuario que la trabaja.

¿Por qué caracterizar las TI?

Según el artículo 4, del mencionado reglamento de seguridad para las TI, cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un sistema de seguridad informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos: minimizar los riesgos sobre los sistemas informáticos, y garantizar la continuidad de los procesos informáticos.

Para Aldegani, G. (2003),el objetivo de la seguridad informática será mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), control y autenticidad de la información manejada por computadora.

Rodao, J. (2004), define a la seguridad informática como: «El conjunto de procedimientos que nos permite que nuestros datos de hoy puedan ser utilizados mañana sin ninguna merma de calidad en los mismos. Por ello, la seguridad abarca muchos temas aparentemente dispares como el mantenimiento regular de los equipos, la ocultación de datos, la protección de los mismos con claves de acceso y más».

Sin embargo, Areitio J. (2008), asegura que la seguridad Informática no solo debe encargarse de los posibles fallos desaprensivos, sino que también debe tener en cuenta lo errores que sepudieran generar por el mal funcionamiento del hardware, así como prevenir acciones involuntarias que puedan afectar la seguridad de la información que seencuentre contenida en los sistemas. La seguridad informática también ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares a tener una aplicación de dimensiones inimaginables ycrecientes que incluyen transacciones financieras, acuerdos contractuales, información personal, archivos médicos, negocios por internet y más.

En el propio Reglamento de Seguridad para las Tecnologías de la Información del Ministerio de la Informática y las Comunicaciones (Resolución Ministerial 127 del 2007: 21) se declara que un sistema de seguridad informática es el: «Conjunto de medios humanos, técnicos y administrativos, que de manera interrelacionada garantizan diferentes grados de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados».

En esta definición se subrayan dos elementos que orientaron nuestro análisis, el primero se relaciona con «garantizar diferentes grados de seguridad informática» y el segundo con la «importancia de los bienes a proteger».

En el último caso se refiere a que la información se procesa, intercambia, reproduce o conserva en las tecnologías de la información disponibles en las entidades educativas,y que las mismas se pueden encontrar en laboratorios, en departamentos docentes, en departamentos encargados de la creación de software educativos, en departamentos económicos, en centros de estudio y de investigación, en los nodos de comunicación brindando los servicios de conectividad, navegación o correo electrónico, en la dirección de cada uno de los procesos de la entidad, por tanto, existen tecnologías que requieren de una atención especial por su importancia para la gestión de la entidad.

Por otro lado, la protección de la información en cada escenario no debe ser igual, así por ejemplo, los laboratorios al ser empleados para la impartición de clases la información que se maneja por profesores y estudiantes debe estar relacionada con el contenido de las asignaturas que por ende no producen daños o riesgos para el funcionamiento de la entidad. La situación seria distinta en los nodos de comunicación pues laobtención dedatos de un usuario como la contraseña puede provocar el acceso o divulgación no autorizada de la información y ocasionar daños o riesgos para el funcionamiento de la entidad.

Es por ello que la caracterización de las TI de la entidad atendiendo a los indicadores previstos permite seleccionar los elementos que las tipifican y distinguen de las demás tecnologías, esto facilitasu organización y la aplicación de diversos niveles de seguridad informática.

¿Cómo caracterizar las TI?

Como se ha mencionado, el recursos más importantes de toda institución es la información sin embargo en muchos casos esta no se valora adecuadamente debido a su intangibilidad de ahí que establecer suvalor es algo totalmente relativo, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

En esta dirección, varios son las propuestas que se pueden encontrar, así por ejemplo en el Decreto Ley 199 de 1999 se declara que la información puede ser «clasificada» cuando contiene datos o informaciones cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para el Estado o para su desarrollo político, militar, económico, científico, técnico, cultural, social o de cualquier otro tipo; «limitada» cuando su importancia para el objeto social de la entidad no resulta conveniente su difusión pública y debe limitarse su acceso a personas determinadas y «ordinaria»: cuando su conocimiento o divulgación no autorizada no produce daños o riesgos para el funcionamiento de la entidad.

Clasificación necesaria pero no suficiente cuando se habla del tratamiento de la información en los sistemas informáticos que se encuentran ubicados en los diversos escenarios que existen en las entidades educativas.

La norma cubana ISO/IEC 27001:2007 declara tres elementos a tener en cuenta, ellos son:

a) Confidencialidad, cualidad deseable en la información que se caracteriza por exigir que la misma sea revelada sólo a los usuarios autorizados, en la forma y tiempo determinado.

   Telin, P. (2006), asevera que la confidencialidad se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

b) Integridad, cualidad deseable en la

información que se caracteriza porque ésta solo pueda ser modificada por personal autorizado, (incluye la creación y borrado de la información).

Para los autores del presente trabajo, la integridad se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, deforma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, esdecir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

c) Disponibilidad, cualidad deseable en la información que se caracteriza por exigir que la misma se encuentre asequible y utilizable en el momento y forma que requieran los usuarios autorizados.

Baeta, J. (s/f), plantea que la disponibilidad se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar lapermanencia del sistema informático, en condiciones de actividad adecuadaspara que los usuarios accedan a los datos con la frecuencia y dedicación querequieran, este principio es importante en sistemas informáticos cuyoscompromiso con el usuario, es prestar servicio permanente.

Otros autores como De Lara, N. (2007: 6) le incluyen otros dos principios:

• Autenticidad, cualidad deseable en la información que se caracteriza por exigir que la misma sea válida y utilizable en tiempo, forma y distribución.

• Trazabilidad, cualidad deseable en la información que se caracteriza por asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento, así como quién ha accedido a los datos.

A partir de las consecuencias que tendría para la entidad el incumplimiento de alguno de los elementos antes señalados, estos pueden ser evaluado en las categorías de: ALTO, MEDIO y. BÁSICO a partir del criterio de:

d) Confidencialidad: se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

e) Integridad: se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

f) Autenticidad: se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica y en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas.

g) Disponibilidad: se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita y en función de las consecuencias que tendría el que una persona autorizada no pudiera usar al servicio cuando lo necesita.

h) Trazabilidad: se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información y en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio

¿Para qué caracterizar las TI?

Como se mencionó, el proceso de caracterización de las TI de la entidad permite seleccionar los elementos que las tipifican y distinguen de las demás tecnologías, y facilitando su organización en grupos o clases y la adecuación de las medidas de seguridad para proteger la información en correspondencia con dicha organización.

Considerando la información que las TI procesan y el cargo o función del usuario que la trabaja se agruparon en las siguientes clases:

Clase A: Constituye el nivel de seguridad válido más alto. A esta clase pertenecen aquellos sistemas informáticoscuya salida de funcionamiento afectaría el trabajo de las áreas y de la conexión de la entidad con el exterior, es decir afectaría el procesamiento, envío y recepción desde la entidad y hacia la entidad de información.

Clase B: Constituye el segundo nivel de seguridad. A esta clase pertenecen aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información clasificada o se encargan de su correcto funcionamiento.

Esta clase se subdivide en dos:

• B1: aquellos sistemas informáticos que se encargan de la configuración y correcto funcionamiento de las máquinas de la clase anterior o cuya salida de funcionamiento afectaría el trabajo de un área específica.

• B2: pertenecen aquellos sistemas informáticos encargados de procesar, intercambiar, reproducir o conservar información clasificada.

Clase C: Constituye el tercer nivel de seguridad. A esta clase pertenecen aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información limitada.

Esta clase se subdivide en tres:

• C1: aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información que solo es del conocimiento del consejo de dirección ampliado de la entidad.

• C2: aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información que solo es del conocimiento del consejo de dirección ampliado de la entidad o manejan información relacionada con proyectos de investigación.

• C3: aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información relacionada con la dirección del proceso de enseñanza aprendizaje de la entidad.

Clase D: Constituye el cuarto nivel de seguridad. A esta clase pertenecen aquellos sistemas informáticos que procesan, intercambian, reproducen o conservan información contable y financiera.

Clase E: Constituye el quinto nivel de seguridad. A esta clase pertenecen aquellos sistemas informáticosque procesan, intercambian, reproducen o conservan información ordinaria.

Clase F: Constituye el nivel más bajo de seguridad. A esta clase pertenecen los sistemas informáticos personales.

Así, las medidas de seguridad a aplicar a cada clase se personalizan garantizando diferentes grados de seguridad, aunque cada clase contiene las medidas de la clase que le precede. En la tabla 1 se puede apreciar la relación entre las clases y la categoría que debe alcanzar los indicadores propuestos.

Por lo general a los sistemas informáticos que se agrupan en las clases A y B les corresponden un nivel de seguridad alto siendo la clase A la más alta de las dos. Por su parte los sistemas informáticos que se encuentran agrupados en las clases C y D les corresponden el nivel de seguridad medio, con la diferencia que las tecnologías informáticas de la clase D se encuentran interconectadas en una red privada. Por último están los sistemas informáticos agrupados en las clases E y F en el que la clase E es la más importante por pertenecer a la entidad.

Lo antes planteado se puede observar en la figura 1 que aparece a continuación, en la que se empleó los colores para resaltar el nivel de seguridad al que pertenece cada una de las clases.

Con la caracterización de las tecnologías informáticas, se procederá a establecer las medidas de seguridad para cada uno de los niveles, hay que tener presente que en las medidas a implantar se requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y las facilidades para el usuario, está claro que a mayor seguridad en un sistema informático, su operatividad es menor.

Una revisión de las normas cubanas ISO/IEC 27001:2007e ISO/IEC 17799: 2007, del Reglamento de Seguridad para las Tecnologías de la Información del Ministerio de Informática y las Comunicaciones (Resolución Ministerial 127/2007), del Reglamento de Seguridad Informática en la Actividad Educacional del MINED (Resolución Ministerial176/

Tabla 1. Relación entre las clases y los indicadores a evaluar (Fuente: elaboración propia)

		CLASES								
		A	**B1**	**B2**	**C1**	**C2**	**C3**	**D**	**E**	**F**
Confidencialidad	Nivel Alto	X								
	Nivel Medio		X	X	X	X		X		
	Nivel Básico						X			
	Sin Valorar								X	X
Integridad	Nivel Alto	X	X	X						
	Nivel Medio				X	X		X		
	Nivel Básico						X			
	Sin Valorar								X	X
Autenticidad	Nivel Alto	X	X					X		
	Nivel Medio			X	X					
	Nivel Básico					X	X		X	X
	Sin Valorar									
Disponibilidad	Nivel Alto	X								
	Nivel Medio		X	X				X		
	Nivel Básico				X	X	X		X	
	Sin Valorar									X
Trazabilidad	Nivel Alto	X	X	X	X			X		
	Nivel Medio					X				
	Nivel Básico						X			
	Sin Valorar								X	X

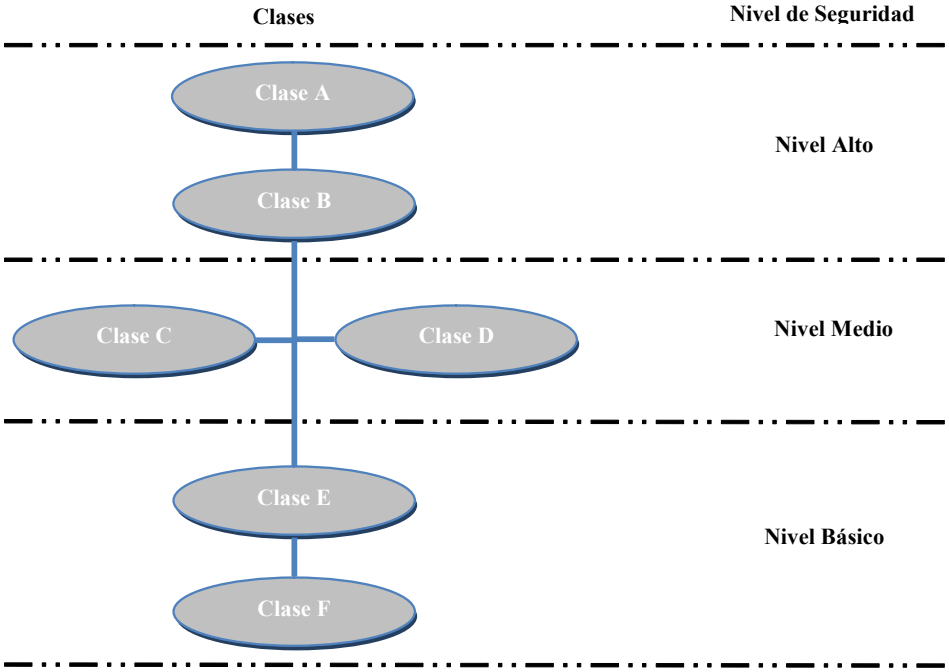

Figura 1. *Relación entre las clases y los niveles de seguridad (Fuente: elaboración propia)*

2007) permitió, desde un enfoque integral y en sistema, delimitar las medidas de seguridad a implantar.

Estas medidas de seguridad se subdividen en:

a) Medidas administrativas y organizativas: consiste en la aplicación de procedimientos de control, como medidas de prevención y contramedidas dirigidas a minimizar riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos.

b) Medidas de seguridad física y ambiental: consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a recursos e información, implementados para proteger el hardware y los medios de almacenamiento de datos o con el fin de controlar los efectos de la naturaleza.

c) Medidas de seguridad técnica o lógicas: consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita que accedan a ellos las personas autorizadas para hacerlos.

d) Medidas legales: consiste en la aplicación de medidas de carácter preventivo e inmediato a aplicar frente a cualquier violación en que incurran los usuarios de los sistemas informáticos referente a lo que se estipula como prohibiciones y obligaciones del usuario.

e) Medidas educativas: consiste en la aplicación de medidas de carácter preventivo dirigidas a la preparación del personal de la entidad sobre las medidas y procedimientos establecidos vinculados con la seguridad de las tecnologías de la información vital para el desempeño de su trabajo.

Por ello, cada nivel de seguridad estará compuesto por un conjunto de medidas físicas y ambientales, técnicas o lógicas, administrativas y de organización, legales y educativas muy interrelacionadas entre sí y que dependen de la caracterización de las tecnologías informáticas de la entidad.

En la figura 2 se observa la relación entre la caracterización de las TI y las medidas de seguridad para garantizar el nivel de seguridad que exige la información a proteger.

Claro está que la seguridad de la información no es un producto, sino un proceso continuo que debe ser controlado, gestionado y monitorizado en el que la caracterización de las TI juega un importante papel dentro de la gestión global de la seguridad de la información en la entidad educativa.

Por ello se asume el modelo de procesos «Planificar-Hacer-Verificar-Actuar» (PHVA), que se aplica para estructurar todos los procesos del sistema de gestión de la seguridad de la información adoptado por la norma cubana ISO/IEC 27001: 2007 y que hace énfasis en la importancia de:

a) comprender los requisitos de seguridad de la información, la necesidad de establecer la política y objetivos en relación con ellaasí como la de caracterización de las tecnologías de la información;

b) implementar y operar controles para manejar los riesgos de seguridad de la información enla entidad educativa a partir de los niveles de seguridad declarados;

c) realizar el seguimiento y revisión del desempeño y eficacia del sistema de gestión de la seguridad de la información; y

d) la mejora continua basada en la medición de objetivos.

Conclusiones

En las entidades educativas cubanas, la información que se procesa, almacena electrónicamente, se trasmite por correo o por medios electrónicos debe ser protegida adecuadamente. La protección de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, educativas y legales, con un enfoque integral y en sistema, de forma tal que garantice su integridad confidencialidad, y disponibilidad. Es por ello, que la caracterización y organización de las tecnologías informáticas encargadas de procesar dicha información permite ajustar estas medidas en correspondencia con la clase en la que se ubica dicha tecnología y por tanto favorece los procesos que se desarrollan en cada una de las entidades educativas.

Referencias

ACISSI(2011). Seguridad Informática. Ediciones ENI, Primera edición,Barcelona – España.

Aldegani, G. (2003). Seguridad Informática. MP Ediciones. Argentina.

Areitio J.(2008). Seguridad de la información. Editorial Paraninfo,Primera Edición, Madrid-España.

Atelin, P. (2006). Redes Informáticas. Ediciones ENI, Primera Edición,Barcelona-España.

Baeta, J. (s/f). Seguridad Informática. [Versión electrónica] Disponible en:http://es.scribd.com/doc/95069532/Seguridad-Informatica

Consejo de Estado (1999). Decreto Ley 199/99 Seguridad y Protección de la Información Oficial. La

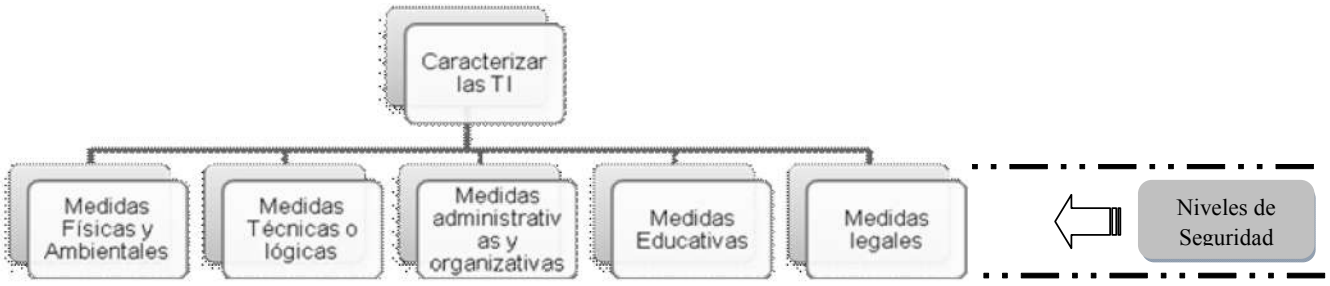

Figura 2. *Relación entre la caracterización de las TI y las medidas de seguridad según los niveles de seguridad (Fuente: elaboración propia)*

Habana, Cuba.

De Lara Guerrero, N. (2007). Guía de Seguridad de la Información para Administración Local y PYMES.

Ministerio de Educación (2007). Resolución Ministerial No. 176/*2007* Reglamento de Seguridad para las Tecnologías de la Información en la actividad educacional. La Habana, Cuba: MINED.

Ministerio de la Informática y las Comunicaciones (2007). Resolución Ministerial No. 127/2007. Reglamento de Seguridad para las Tecnologías de la Información. La Habana, Cuba: MIC.

Norma Cubana ISO/IEC 17799: 2007 (2007). Tecnología de la información – Código de buenas prácticas para la gestión de la seguridad de la información (ISO/IEC 17799: 2005, IDT). La Habana, Cuba: Oficina Nacional de Normalización.

Norma Cubana ISO/IEC 27001: 2007 (2007). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos (ISO/IEC 27001: 2005, IDT). La Habana, Cuba: Oficina Nacional de Normalización.

Rodao, J.(2006). Piratas cibernéticos, Cyberware, Seguridad informática e Internet. Editorial Alfaomega Ra-Ma, Madrid-España.

Recibido: 21 de marzo de 2017
Aprobado en su forma definitiva: 14 de julio de 2017

Osmany Aguilera Almaguer
Universidad de Holguín, Cuba
Correo-e.: oaguilera@uho.edu.cu

Edilberto de Jesús Pérez Alí Osmán
Universidad de Holguín, Cuba
Correo-e.: edilbertop@uho.edu.cu

Rolando Rivero Cuesta
Universidad de Holguín, Cuba
Correo-e.: rolando@uho.edu.cu