GESTIÓN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN ISO 17799

*JUAN CASTILLO MAZA**
E-mail: jcastillom@unmsm.edu.pe

INTRODUCCIÓN

La humanidad vive actualmente en una sociedad dominada por el conocimiento y la información, necesita sistematizar un modelo de gestión que garantice la seguridad de la información, para dar acceso a todo aquello que sea necesario para el proceso de toma de decisiones en las empresas y todo tipo de corporaciones. Producto del proceso de globalización, internacionalización y mundialización, gerentes de seguridad de empresas líderes, han trabajado y producido en conjunto, la normatividad relacionada con la seguridad de las informaciones que estuviese sujeta a auditoría y a la vez reconocida globalmente.

La información, es un conjunto de datos que dentro de un contexto dado tiene un significado para alguien[1]. Por lo que se debe considerar diferente que dato, por cuanto éste, se refiere a la materia prima para la producción de información.

Un sistema de información, es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio[2]. Componentes interrelacionados que capturan, almacenan, procesan y distribuyen la información para apoyar la toma de decisiones, el control, análisis y visión en una institución.

La seguridad, se refiere a las políticas, procedimientos y medidas técnicas usadas para evitar un acceso no autorizado, alteración, robo o daños físicos a los sistemas de información[3]. La seguridad puede promoverse mediante un conjunto de técnicas y herramientas para salvaguardar el hardware, software, las redes de telecomunicaciones y de datos.

Se asume que las normas de seguridad, apoyarán los esfuerzos de los gerentes de tecnología de la información, en el sentido que facilitará la toma de decisiones de compra, incrementará la cooperación entre los múltiples departamentos por ser la seguridad, el interés que ayudará a consolidar éste como prioridad empresarial.

En este contexto, desde la publicación, por parte de la Organización Internacional de Normas Técnicas (*ISO, International Organization for Standarization*) en el año 2000, la norma ISO 17799 surge como la regla técnica de seguridad de la información, reconocida a nivel mundial. ISO 17799 se define como "Un conjunto de normas, que incluye las prácticas exitosas de seguridad de la información".

ANTECEDENTES

Por más de un siglo, el Instituto Británico de Normas Técnicas (*BSI, British Standar Institute*) y la Organización Internacional de Normas Técnicas (*ISO, International Organization for*

* *Licenciado en Administración por la Universidad Nacional de Trujillo. Magíster en Economía por la UNMSM. Profesor Principal de la UNMSM. Director de la Unidad de Investigación de la Facultad de Ciencias Administrativas de la UNMSM. Profesor de Post Grado en la UNMSM, UNFV, UNE, UNASAM, UNSCH. Director de la* Revista de Investigación Gestión en el Tercer Milenio.

Standarization) han brindado parámetros globales a las técnicas de operación, fabricación y desempeño. Sólo faltaba que BSI e ISO establezcan una norma técnica para la seguridad de la información.

En el año de 1995, el *British Standar Institute* publicó la primera norma técnica de seguridad, BS 7799, redactada con el fin de abarcar los asuntos de seguridad relacionados con el *e-comerce*. En ese año, dificultades como el problema informático del año 2000 (Y2K) y la Unión Económica y Monetaria (EMU) prevalecieron sobre otros. Para empeorar las cosas, la norma BS 7799 se consideraba inflexible por lo que no tuvo gran acogida. No se presentó la norma técnica en el momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces.

En el año de 1999, el *British Standar Institute* intenta publicar nuevamente la segunda versión de la norma BS 7799, una versión ampliada de la primera; esta edición sufrió muchos mejoramientos y perfeccionamientos en relación a la versión inicial. A partir de ese momento la *International Organization for Standarization* se percató de estos cambios y comenzó a trabajar en la revisión de la norma técnica BS 7799.

En diciembre del año 2000, la Organización Internacional de Normas Técnicas (*ISO International Organization for Standarization*) acogió y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. Paralelamente, adoptó un medio formal de acreditación y certificación para cumplir con la norma técnica. Los problemas informáticos del año 2000 (Y2K) y la Unión Económica y Monetaria (EMU) y otros similares se habían solucionado o reducido y la calidad total de la norma técnica había mejorado considerablemente. La adopción por la *ISO International Organization for Standarization* de la Parte 1 –los criterios de la norma técnica– de BS 7799 recibió gran aceptación por parte del sector internacional y fue en este momento que un grupo de normas técnicas de seguridad tuvo amplio reconocimiento.

MARCO DE LAS RECOMENDACIONES

La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy en día es un compendio de recomendaciones y prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para ser flexible y nunca indujo a las personas que la cumplían para que prefirieran una seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

La flexibilidad e imprecisión de la norma ISO 17799 es deliberado por cuanto es difícil concebir una norma que funcione en una variedad de entornos de tecnología de la información y ser capaz de desarrollarse con el cambiante mundo de la tecnología. La norma ISO 17799 sencillamente ofrece un conjunto de reglas a un sector donde no existían.

LAS ÁREAS DE CONTROL DE LA NORMA ISO 17799

La estructura de la normatividad de gestión en seguridad de sistemas de información, norma ISO 17799, queda especificada en 10 componentes, que incluyen: política de seguridad, organización de la seguridad, control y clasificación de los recursos de información, seguridad de personal, seguridad física y ambiental, manejo de las comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, manejo de la continuidad empresarial, así como el cumplimiento.

VENTAJAS DE LA NORMA ISO 17799

Las más relevantes serían:

- Protección de los bienes de la empresa (información y actividades)
- Protección de la información en las comunicaciones y software
- Protección ante accesos malintencionados
- Prevenir alteraciones en las comunicaciones entre organizaciones
- Procesamiento seguro de la información

BENEFICIOS DE LA NORMA TÉCNICA ISO 17799

Una empresa certificada con la norma técnica ISO 17799 puede ganar frente a sus competidores no certificados. Si un cliente potencial tiene que escoger entre empresas diferentes y la seguridad es un aspecto trascendente, por lo general optará por la certificada. Además una empresa certificada tendrá en cuenta lo siguiente:

- Mayor seguridad en la empresa
- Planeación y manejo de la seguridad más efectivos

- Alianzas comerciales y *e-commerce* más seguros
- Mayor confianza en el cliente
- Auditorías de seguridad más precisas y confiables
- Menor responsabilidad civil.

CONCLUSIONES

a. En plena era del conocimiento, las informaciones se constituyen en el principal capital de las organizaciones y empresas; su administración no tendrá valor sin la seguridad que le permita una relativa privacidad y exclusividad.

b. De acuerdo a estadísticas, la seguridad en la mayoría de las empresas consiste en acciones correctivas; la norma ISO 17799 propicia las bases hacia un giro preventivo.

c. La aplicación de la norma ISO 17799 a una empresa deberá realizarse dentro de un proceso; se evalúa inicialmente la posición actual de la organización y posteriormente identificando los cambios que se necesita para cumplir con la norma; en suma, la planificación e implementación.

Notas

1 Daniel Cohen & Enrique Asín. *Sistemas de informacion para los negocios Un enfoque de toma de decisiones.* Ed. McGraw-Hill, México 2000, p. 3.

2 Ibídem, p. 4.

3 Kenneth C. Laudon & Jane P. Laudon. *Administracion de Los Sistemas de Informacion, Organización y Tecnología,* Ed. Prentice Hall Hispanoamericana, S.A., México 1996, p. 708.

BIBLIOGRAFÍA

Cohen Daniel y Asín Enrique. *Sistemas de Información para los Negocios. Un Enfoque de Toma de Decisiones*. Editorial McGraw-Hill, México 2000.

Laudon Kenneth C. y Laudon Jane P. *Administración de los Sistemas de Información, Organización y Tecnología*. Editorial Prentice Hall Hispanoamericana, S.A., México 1996.

http://www.compumentor.org/y2k/workbook/y2k_espanol.html

http://www.monografias.com/trabajos/ano2000/ano2000.shtml

http://www.iaf.es/publicaciones/nautilus005.pdf