Análisis de la relación entre la normatividad jurídica de la seguridad de la información en Colombia y el modelo de Sistema de Gestión de Seguridad de la Información NTC/ISO 27001*

Analysis about the relationship between legal systems, the security information in Colombia and the Information Security Management System NTC/ISO 27001

Recibido: 23 de noviembre de 2010
Revisado: 25 de mayo de 2011
Aceptado: 15 de agosto de 2011

*Daisy Sahir Navas Guzmán***
Universidad Santo Tomás e Icontec
*Edward Yecid Torres Nova****
Universidad Santo Tomás e Icontec

RESUMEN

Las tecnologías de la información contribuyen a mejorar la toma de decisiones en las organizaciones, suministrando datos con la calidad y en la cantidad que estas requieren sin embargo, el flujo de la información genera riesgos de diverso tipo: para manejar dichos riesgos se han elaborado modelos de gestión de

* Artículo de investigación.

** Correspondencia: Daisy Sahir Navas Guzmán, abogada, especialista en Derecho Administrativo, magíster en Calidad y Gestión Integral, trabaja actualmente con ECOPETROL. Correo electrónico: daisy.navas@ecopetrol.com.co

*** Edward Yecid Torres Nova, administrador y constructor arquitectónico, especialista en Gerencia de Salud, magíster en Calidad y Gestión Integral, docente de la Universidad Nacional Abierta y a Distancia; correo electrónico: edwardyecid@gmail.com

seguridad de la información como el planteado en la norma internacional ISO 27001. Por otra parte, a la alta dirección le compete tener en cuenta el marco jurídico en que se desenvuelve la organización, incluyendo las normas legales aplicables a la seguridad de la información. En este artículo se abordan cinco aspectos en los que existe relación entre la norma sobre gestión de la información y aspectos jurídicos de la legislación colombiana en materia de seguridad de la información, tales como: Seguridad en tecnologías, Datos de privacidad, Protección de los consumidores, Propiedad intelectual y Control de contenidos.

Al facilitar la comprensión y aplicación en forma integrada del marco jurídico y de la norma sobre seguridad de la información es posible mejorar el manejo de los riesgos asociados.

Palabras clave: seguridad de la información, cumplimiento legal, ISO 27001.

ABSTRACT

Colombian organizations take decisions according to the quality and quantity of information they get in different ways. On the other hand the senior management team has to take into account the legal framework. Therefore, it is relevant to create a stock list with the legal regulations that are available to the security information. Furthermore, it is favorable to use models of management system security, such as ISO 27001 that involves a chapter of legal performance. In this work, there are five features about the relationship between management and legal characteristics on legal matters about information security like: Technology security, privacy data, consumers' protection, intellectual property and control of contents. In that way, companies can recognize the legal framework and the regulation developments in order to facilitate the comprehension and the application of the same.

Keywords: Information security, legal compliance, ISO 27001.

I. INTRODUCCIÓN

En la actualidad, para llevar a cabo sus actividades la sociedad se apoya en las llamadas tecnologías de la información y la comunicación - TIC. Mediante ellas se realizan innumerables transacciones y operaciones a nivel nacional e internacional; asimismo, se comunican personas de manera eficaz, económica y veloz; sin embargo, el uso de estas tecnologías eventualmente podría derivar riesgos a quienes utilizan la redes electrónicas, las personas pueden, por ejemplo, quedar expuestas a las actuaciones de "piratas electrónicos" que roban, sabotean, comercializan, usufructúan o borran información de sus víctimas, causando perjuicios a los usuarios o dueños de la información. Camisón manifiesta que:

> La irrupción de la sociedad de la información supone innumerables ventajas para la gestión de las organizaciones, tales como la agilización del trabajo y la mejora de la productividad. Mas estas ventajas pueden ser eliminadas si la información no se protege. La seguridad de la información está amenazada por diversos riesgos, los más notorios son los provocados por los piratas y los virus informáticos cuando navegamos por Internet, que se acrecientan cuanto mayor es la organización, haciéndola más dependiente de los sistemas de información[1].

Conociendo este panorama, algunos organismos como INTERPOL ha puesto en su página de Internet una lista de chequeo que pretende inducir a las organizaciones a la prevención de ataques, con una serie de preguntas que sugestionan y hacen reflexionar sobre el tema de la seguridad de la información. Esta lista de control se enfoca en la prevención de delitos y en una serie de temas de seguridad en tecnologías de la

1 CAMISÓN, César, CRUZ, Sonia y GONZÁLEZ, Tomás. Gestión de la calidad, Madrid: Pearson Educación, 2007. p. 544.

información que son de interés de atacantes o cibercriminales. Esta "Lista de Información de seguridad y prevención de la delincuencia de la empresa"[2] es un instrumento para medir el nivel de seguridad de diferentes organizaciones, su resultado puede servir como punto de partida para observar vulnerabilidades respecto a la seguridad de la información.

En Colombia existe normatividad jurídica relacionada con la seguridad de la información: legislación doctrina, jurisprudencia, y convenios supranacionales. Las *organizaciones deben respetar la legislación* de su jurisdicción, es por ello que es útil hacer un reconocimiento de la normatividad que regula la seguridad de la información y ver su aplicabilidad en la organización.

De otro lado, expertos indican que la reglamentación colombiana en materia de seguridad de la información, al menos la que se deriva de las tecnologías de la información y la comunicación aún no es suficiente. Sobre esto, Velasco afirma:

> El desarrollo en nuestro país de normas jurídicas que respondan a los problemas que surgen del fenómeno de las TIC es mínimo. La Ley 527 de 1999 constituye uno de los pocos desarrollos importantes en este sentido. Esta situación genera un grado importante de inseguridad e incertidumbre no sólo para las organizaciones, sino para también los ciudadanos, en su condición de usuarios, consumidores y titulares de datos personales[3].

Así, mientras que Velasco menciona que la legislación no es suficiente, Cano sugiere que se fortalezca: "… se hace necesario avanzar en la formación de especialistas en derecho informático, fortalecimiento de la legislación sobre delincuencia informática y formación de especialistas en informática forense como estrategias para enfrentar la amenaza creciente del cibercrimen"[4].

Se encuentran normas de carácter técnico cuya finalidad es la gestión de la información; al respecto, la familia de las Normas ISO 27000, que se han venido desarrollando con fuerza en la última década; los Sistemas de Gestión de Seguridad de la Información - SGSI son certificables bajo el estándar ISO 27001. Según informe *The ISO Survey – 2008*[5] en el mundo se encuentran certificadas bajo este estándar 9426, en 82 países, siendo Japón el que más títulos ha conseguido, en total 4425, es decir, alrededor del 48% de los certificados. En América, se encuentra que Estados Unidos, cuenta 168 títulos, Brasil 40, México 31, Argentina 6 y Colombia 11 certificados.

En 2007, *Harvard Law School* crea el concepto *e-compliance*[6] que definen "como la gestión de los riesgos en la intersección de la ley, la tecnología y el mercado que han surgido a través y en reacción a la informatización y las redes digitales"[7]. Este texto el *e-compliance,* formula principios de aplicación legal tomando en cuenta la administración del riesgo, desde tres aspectos: el mercado, la tecnología y el derecho, acercando así las dos esferas existentes: el marco jurídico y el marco de gestión técnica.

Para las organizaciones la seguridad de la información es un tema que por representar intereses de contenido

2 INTERPOL. Lista de Información de seguridad y prevención de la delincuencia de la empresa. Disponible en: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp#top

3 VELASCO, Arean. El derecho informático y la gestión de la seguridad de la información: una perspectiva con base en la Norma ISO 27001. Barranquilla. 2008. [En línea]. Revista de Derecho. Academic Search Complete, EBSCOhost.

4 CANO, Jeimy. Seguridad informática en Colombia. Tendencias. 2008.

5 ORGANIZACIÓN MUNDIAL PARA LA ESTANDARIZACIÓN (ISO). The ISO Survey – 2008. Disponible en Internet: http://www.iso.org/iso/survey2008.pdf. Consultado 29 de agosto de 2010.

6 Urs Gasser, Haeusermann Daniel. e.compliance: Towards a Roadmap for effective Risk Management, p. 4, Harvard law school, marzo 2007.

7 Ibíd.

legal y económico, adicionales a los técnicos, no solo debe estar en manos de los ingenieros y encargados de sistemas informáticos, sino que necesita involucrar a la gerencia, que a su vez debe convocar a grupos de interés a participar activamente en la salvaguarda y uso adecuado del derecho fundamental y mayor activo: la información.

Dado lo anterior, se hace un análisis de la normalización técnica de la seguridad de la información, específicamente, la Norma ISO 27001:2005, con el ánimo de identificar puntos de referencia a la legislación aplicable a empresas colombianas. De la misma manera, se considera importante identificar las principales normas legales, sobre seguridad de la información, para el entorno colombiano.

II. METODOLOGÍA

Inicialmente se hace un reconocimiento de la legislación aplicable a la seguridad de la información, al mismo tiempo que se hace una interpretación de la norma de Sistemas de Gestión de Seguridad de la Información NTC/ISO 27001:2005.

Se tiene como referencia que a la fecha 12 organizaciones se hallaban certificadas en Colombia bajo el estándar ISO 27001. Se trató de consultar todas, sin embargo, por razones de diversa índole fue posible el contacto con expertos de cinco de estas; en lugar de ello, se logra entrevistar a siete consultores experimentados en la temática.

Certificaciones ISO 27001 en Colombia[8]

1. ComBanc S.A.
2. Etek International Holding Corp.
3. Financial Systems Company Ltda.
4. Ricoh Colombia, S.A.
5. SETECSA S.A
6. UNE EPM Telecomunicaciones. S.A E.S.P.
7. UNISYS Global Outsourcing & Infrastructure Services.

Las empresas certificadas por ICONTEC:

1. Banco de la República Compensar
2. Jaime Torres y Cía.
3. Enlace Operativo
4. Mareigua
5. Fluid Signal

Para lograr obtener información primaria se elaboraron dos cuestionarios, uno para expertos en gestión de seguridad e información y otro para conocedores jurídicos en el tema. Así las cosas, el objeto de estudio se divide en los siguientes subtemas o categorías presentadas por *Urs y Haeusermann*, en su artículo *e.compliance:*

1. Seguridad: seguridad de las tecnologías, equipos *software*, etc.
2. Datos de privacidad: relacionado con la administración de los datos privados de los clientes y trabajadores.
3. Protección de los consumidores: relacionado con la legislación de protección del consumidor.
4. Propiedad intelectual, y en especial de derecho de autor.
5. Control de contenidos sobre contenidos en línea.

8 INTERNACIONAL REGISTER OF ISMS CERTIFICATE. Disponible en http://www.iso27001certificates.com/ consultado 30 de agosto de 2010.

Una vez recopilada y analizada la información, mediante las entrevistas, se elaboran y se obtienen las relaciones entre lo jurídico y lo técnico. A continuación se presentan de manera concluyente los principales hallazgos:

Sobre privacidad

Existen herramientas tales como *software* y *hardware*, equipos de comunicaciones, metodologías especializadas y buenas prácticas, tales como, segregación de funciones, control de acceso, permisos, cifrado de datos o criptografía, procedimientos de administración de redes y servicios, mantenimiento y desarrollo de *software*, gestión de medios, revisión automática de los contenidos, entre otras. Dichas herramientas se implementan con el fin de mantener: la confidencialidad, la integridad y la disponibilidad de la información, que son los tres pilares sobre los cuales se soporta la seguridad de la información, tal como lo plantean la Norma ISO 27001 y normas jurídicas como la Circular 052 de 2007 de la Superintendencia Financiera.

En todo caso, los expertos jurídicos explican que los elementos tecnológicos especializados para proteger los datos deben acompañarse de un conjunto de medidas normativas, es decir, toda técnica, metodología o procedimiento debe estar acorde con la ley. Es probable que en un mar de normas técnicas y jurídicas, estas puedan contradecirse; en esto los encargados del área legal en las organizaciones deben poner especial atención para evitar futuros inconvenientes.

Asimismo, los expertos argumentan contundentemente que los acuerdos de confidencialidad no solamente son válidos y útiles, sino necesarios, siempre y cuando se puedan hacer cumplir y monitorear. Estos acuerdos deben ser complementados con diferentes formas de gestión.

Los juristas indican que los acuerdos de confidencialidad o elemento contractual tienen un efecto persuasivo y disuasivo, y se deben usar siempre que estén acordes con la ley y sean explicados a cada firmante, de lo cual debería quedar evidencia. La confidencialidad está en manos de las personas; en otras palabras, la seguridad de la información depende de la conciencia, formación y compromiso que tengan los individuos respecto al tema en el interior de la organización.

Sobre protección a los consumidores

A la pregunta ¿ha conocido peticiones, reclamos o quejas sobre consumidores o clientes por fuga de información sobre los mismos?, Cinco de los ocho técnicos expertos han conocido casos, los otros tres mencionan que no. En cuanto que el jurista entrevistado Andrés Guzmán, de Adalid Abogados, dice que en su organización no se han presentado, pero a su oficina llegan casos de otras organizaciones, para ser atendidos jurídicamente. Es por ello que, es importante gestionar el riesgo jurídico para evitar posibles demandas por reclamos o quejas de consumidores por fuga de información, ya que terceros pueden usar datos de manera ilegal.

Otro punto concluyente al respecto de la protección de consumidores es que no existe normatividad legal y técnica suficiente al respecto de los derechos relacionados con información de los consumidores y las obligaciones para la empresa. Dicho de otra manera, la normativa que existe es muy distante de lo que se requiere.

En la temática tratada se invita al desarrollo de una norma que compile toda la jurisprudencia de la Corte Constitucional y se redacte una norma para salvaguardar la imagen en sitios públicos, ejemplo, filmaciones de rostros de personas.

En materia de protección a consumidores, en Colombia la normatividad existente da la orientación y lineamientos alrededor de la responsabilidad que tienen los administradores de datos, lo que haría falta es un mayor y mejor cumplimiento de los mismos, articulado desde cada sector productivo del gobierno. A nivel de principios, la ley está muy arriba o trata temas muy puntuales.

Andrés Guzmán sostiene que la ley "se enfoca en el sector financiero" y favorece a la empresa privada. "En Colombia la ley no protege las bases de datos de ciudadanos, sino las de usuarios bancarios". El experto dice que los grandes vacíos están en el concepto de "banco de datos". La opinión ampliada de Guzmán se encuentra disponible en la versión electrónica del diario *La República*. "La ley existe, pero la protección de sus datos no está garantizada"[9].

Sobre propiedad intelectual

Los hallazgos a nivel general dicen que existen o se pueden desarrollar procedimientos o técnicas de seguridad tecnológica y jurídica para la protección de derechos de propiedad intelectual. Es recomendable establecer dentro de las organizaciones políticas la obligación de proteger los derechos propios y de terceros.

La protección de la propiedad intelectual en el interior de una organización se puede proteger mediante la aplicación del marco jurídico de manera estricta, es decir, a través de control legal en toda dimensión, productos y servicios, hacer uso de *software* legal, control a proveedores, patentes, compromisos contractuales e incluso dentro de los procesos de sensibilización o capacitación.

En las organizaciones deberían existir políticas o planes de transferencia de conocimiento, que son necesarias para asegurar el saber hacer; un sistema de gestión debe asegurar la transferencia del conocimiento. En materia de seguridad de la información, las personas pueden ser consideradas activos de información y, por tanto, deben hacer transferencia del conocimiento, como todo activo, es necesario hacerle *backup*.

Las organizaciones no deben depender de las personas sino del conocimiento, así pues, es necesario garantizar la trazabilidad de los procesos. La transferencia del conocimiento no se debe manejar de manera informal, deben existir obligaciones contractuales para evitar la pérdida del conocimiento.

Control de contenidos

Al respecto del tema de control de contenidos en línea, si las organizaciones tuvieran que bloquear páginas de Internet en el interior de una organización estas deberían ser páginas que no tienen que ver con la razón social de la organización, tales como: correo personal, portales distractores, redes sociales, MSN, Skype, Twitter, descarga de música, las identificadas claramente como ilegales, las antiéticas, entre otras. Solo se debe dejar lo que necesita una persona para hacer su trabajo. Sin embargo, este es un enfoque eminentemente práctico y tecnicista.

Se concluye que en principio no deben bloquearse páginas, y se argumenta que, si es para utilizar mal el tiempo, el trabajador creará formas de hacerlo con o sin servicio de Internet. Igualmente, se extrae que hay que aprender a convivir con el Internet, aprovechándolo para crear valor y no para entretenerse en cosas que no guardan relación con el trabajo.

9 VALENCIA, Juan. La ley existe, pero la protección de sus datos no está garantizada. En: Diario La República. Disponible en internet: http://www.larepublica.com.co/archivos/TENDENCIAS/2010-08-04/la-ley-existe-perola-proteccion-de-sus-datos-no-esta-garantizada_107129.php. Recuperado: 27 de agosto de 2010.

Se pueden crear y usar controles para la revisión de contenidos, lo importante es que estos se encuentren en armonía con la ley. En el mercado, hay diferentes formas tecnológicas que sirven para este fin; no obstante, es importante que los trabajadores entiendan las razones de hacer esos controles, eso genera confianza para todos. Por ello, se necesita hacer campañas de sensibilización, además de implementar otros controles. El control más reconocido son los acuerdos de confidencialidad, pero igualmente, hay más controles técnicos, jurídicos e incluso psicológicos que deben ajustarse a las necesidades de la organización.

IV. CONCLUSIONES

Se concluye que, efectivamente, el proceso de implementación de la ISO 27001 facilita el cumplimiento de las normas jurídicas relacionadas con la seguridad de la información. Se fortalece el cumplimiento, el capítulo 15 de la Norma 27001 habla del cumplimiento, aunque no se audita la ley sino la capacidad de una organización para cumplirla.

La implementación de la 27001 en opinión de uno de los entrevistados es que: "es lo único que pone orden en el cumplimiento legal". Sin embargo, un sistema de gestión de seguridad de la información, fundado bajo el enfoque ISO 27001, facilita el cumplimiento de las normas jurídicas, pero cuando se asume como una buena práctica que agrega valor, no cuando se ve como una imposición. Se concluye que, sin duda, el SGSI bajo el estándar 27001 exige revisar continuamente la matriz de regulación que debe actualizarse y aplicarse.

Por otro lado, se tiene que hay vacíos jurídicos respecto al tema de seguridad de la información. Los abogados y expertos técnicos coinciden en que en Colombia no hay legislación seria en protección de datos no financieros. Se argumenta que debería existir una legislación de seguridad de la información, no solamente para el sector financiero, sino también para otros sectores; igualmente, se menciona que falta normatividad que exija siquiera a los entes públicos a tener medidas de seguridad de la información.

Otro importante hallazgo es que no hay suficientes técnicos especializados que el mercado requiere en este momento, la industria debe formarlos, en cuanto a profesionales, la academia los está formando, sin embargo, se argumenta que cuando se titulan no consiguen empleo, probablemente porque las organizaciones en general aún no son conscientes de la importancia del tema de la seguridad de la información y por ello no se generan plazas de trabajo en esta rama. Es decir, las necesidades existen en seguridad de la información, pero no la suficiente cultura y conciencia.

V. RECOMENDACIONES

Organizaciones que manipulen información sensible deberían establecer controles que estén en armonía con la legislación vigente, se recomienda consultar a personal idóneo en el ámbito técnico y jurídico, de esta manera se logra mejorar y mantener la confidencialidad, integridad y disponibilidad de la información.

Se recomienda a organizaciones implementar modelos formales o cláusulas contractuales de manejo de confidencialidad, ya que son útiles y necesarias; sin embargo, estos arreglos deben estar acompañados de diferentes formas de gestión que apunten a garantizar la seguridad de la informacion.

Se recomienda capacitar a las personas en cuanto al tema de la confidencialidad, ya que depende de ellas mantenerla o no la seguridad de la información es parte de la formación y el compromiso que tengan los individuos, así lo manifiestan expertos juridicos y técnicos.

Es importante dar buen manejo a la información de clientes, consumidores, trabajadores y terceros, ya que este tipo de bases de datos es apetecido en el mercado; no obstante, eventuales fugas de esta información pueden acarrear sanciones para la organización que maneja estos datos.

A legisladores se les recomienda crear normas para regular sectores no financieros, y una normatividad que obligue, por lo menos, a entes públicos, a tener seguridad de la información, ya que en los últimos meses se han visto incidentes en la materia y que han afectado en general a la ciudadanía colombiana; tal es el caso, por ejemplo, de procesos electorales afectados.

Se sugiere el desarrollo de una norma que compile toda la jurisprudencia de la Corte Constitucional y se cree una norma para salvaguardar la imagen en sitios públicos, ejemplo: filmaciones de rostros de personas.

En el interior de organizaciones es importante crear políticas de propiedad intelectual, ellas de alguna manera deberían estar atadas contractualmente entre las partes.

Se recomienda crear y mantener políticas o planes de transferencia de conocimiento que son necesarios para asegurar el saber hacer, un sistema de gestión debe asegurar la transferencia del conocimiento. En materia de seguridad de la información, las personas pueden ser consideradas activos de información y por tanto deben hacer transferencia del conocimiento. La transferencia del conocimiento no se debe manipular de manera informal.

Para organizaciones que manejen información sensible se recomienda usar el modelo ISO 27001, para implementar la seguridad de la información, ya que es una manera de mantenerse al corriente de los temas jurídicos y técnicos en la materia.

VI. BIBLIOGRAFÍA

CAMISÓN, César, CRUZ, Sonia y GONZÁLEZ, Tomás. Gestión de la calidad, Madrid: Pearson Educación, 2007.

CANO, Jeimy J. Seguridad informática en Colombia: Tendencias, 2008. Edited by Foxit Reader.

DÍAZ GARCÍA, Alexánder, Derecho informático: elementos de informática jurídica. Bogotá: Leyer, 2002.

DICCIONARIO DE CIENCIAS JURÍDICAS, POLÍTICAS Y SOCIALES. Montevideo: Editorial Heliasta Manuel Ossorio, 1963.

GASSER, Urs y HAEUSERMANN, Daniel. E.compliance: Towards a Roadmap for effective Risk Management. Harvard Law School. Marzo de 2007. Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=. Recuperado el 10 de marzo de 2010.

GUTIÉRREZ GÓMEZ, María Clara. Consideraciones sobre el tratamiento jurídico del comercio electrónico. En: Internet, comercio electrónico y comunicaciones. Bogotá: Legis.

INTERNATIONAL REGISTER OF ISMS CERTIFICATE. Disponible en http://www.iso27001certificates.com/ consultado 30 de agosto de 2010.

INTERPOL. Lista Información de seguridad y prevención de la delincuencia de la empresa. Disponible en: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp#top. Recuperado el 28 de enero de 2010.

ORGANIZACIÓN MUNDIAL PARA LA ESTANDARIZACIÓN (ISO). *The ISO Survey – 2008.*

Disponible en internet: http://www.iso.org/iso/survey2008.pdf. Consultado 29 de agosto de 2010.

POLICÍA NACIONAL. Sistema de Información Estadístico Delincuencial, Contravenciones y Operativa. Periodo del reporte 01/01/2009 - 14/06/2010. Información suministrada por Grupo Investigaciones Tecnológicas de la Policía Nacional de Colombia. Cai Virtual. Correo electrónico recibido de caivirtual@correo.policia.gov.co el 6 de agosto de 2010.

VELASCO, Arean. El derecho informático y la gestión de la seguridad de la información: una perspectiva con base en la Norma ISO 27 001. En: Revista de Derecho. Academic Search Complete, EBSCO-host. [En línea]. Barranquilla, 2008.