

Un SGSI Genera Valor cuando una Organización se adapta a nuevas Leyes como la 1581 de Protección de Datos Personales

Rojas Garzón, Leidy Diana y Martínez Meléndez, Juan Carlos.
{dianaroga, jcmelendez}@gmail.com
Universidad Piloto de Colombia

Resumen— Este artículo expresa una opinión de los autores, acerca de la generación de valor que puede proporcionar un SGSI cuando una Organización requiere adaptarse a nuevas reglamentaciones, como lo es la reciente Ley de protección de datos personales en Colombia. En este documento se tratan conceptos de un SGSI, aspectos relevantes de la Ley 1581 de Octubre del año 2012 y el Decreto 1377 de Junio de 2013. Este documento aplica para Compañías de cualquier tamaño, donde este tipo de normatividades exige un cambio en la seguridad de la información de la misma.

Abstract— This article expresses an opinion of the authors, about the creation of value that can provide an SGSI when an organization needs to adapt to new regulations, such as the recent law on personal data protection in Colombia. In this paper should address an SGSI concepts, relevant aspects of the 1581 Act October of 2012 and Decree 1377 of June 2013. This document applies to companies of any size, where this type of normativities requires a change in the information security of the same

Índice de Términos—SGSI, ISO, Leyes, Organización.

I. INTRODUCCIÓN

Las empresas deben dejar de concentrarse en ser las mejores, sino en ser únicas, de acuerdo a un artículo de Harvard Business Review. En tiempos tan competitivos como los actuales, algunas marcas logran sobresalir en el mercado por algún elemento que las hace diferentes, no por intentar copiar los modelos de negocio ya existentes que obviamente no generarán los mismos resultados (en la mayoría de los casos resulta algo mucho más deficiente con respecto al original).

“Ser el mejor no debe ser la competencia”, afirma Joan Magretta en este texto, “lo que es lo mejor

para unos, no lo es para otros”¹. Entonces, ¿dónde está la clave? La respuesta puede parecer sencilla: en la creación de estrategias efectivas para cautivar todos los días a los clientes nuevos y a los que ya te compran y ofrecerles un valor extra que los haga seguir apostando por tus productos o servicios. Existen diversas maneras de **generar valor en una compañía**, ya sea por medio del marketing, de sus recursos humanos, de un nuevo diseño, de la exclusividad o de la atención al cliente, entre otras.

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

¹ Remanencia de Datos. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>

² Ley 1581 Protección de datos personales

II. SGSI – ISO 27001

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran

III. LEY 1581 COMO NORMATIVIDAD DE REFERENCIA

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y

garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Con esta ley se busca cumplir los siguientes aspectos de la información, son los principales principios del tratamiento de la información:

- Legalidad: El Tratamiento es una actividad reglada por lo tanto debe sujetarse a lo establecido en ella y en las demás disposiciones.
- Finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.
- Libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular.
- Veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Transparencia: En el Tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- Acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos Personales, de las disposiciones de la presente ley y la Constitución.
- Seguridad: Los Datos Personales deben Tratarse con las medidas técnicas, humanas y administrativas para dar seguridad a los registros de las bases de Datos Personales.
- Confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

Artículo 5

¹ Remanencia de Datos. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>

² Ley 1581 Protección de datos personales

Datos Sensibles: Se define aquellos que afecten la intimidad del titular cuyo uso indebido puede generar su discriminación, tales aquellos que releven el origen radical o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derecho humanos o que promueva intereses de cualquier político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Se crean dos actores principales en el manejo de la información que realizan el tratamiento de datos personales el Responsable y el Encargado del tratamiento, el primero será la persona que, por sí o con asocio con otros decida sobre la base de datos y el Encargado es toda persona que, por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Deberes de los responsables del tratamiento:

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Exigir al encargado del tratamiento, en todo momento, el respecto de las condiciones de seguridad y privacidad de la información del titular.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley, y en especial, para la atención de consultas y reclamos.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de los titulares.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso².

IV. ASPECTOS CLAVES DEL DECRETO 1377

El pasado 27 de junio DE 2013 se aprobó el Decreto 1377 “Donde Se reglamenta parcialmente la Ley 1581 de 2012”, es un paso con la protección

de la información que Colombia da, adoptando un régimen jurídico de protección de datos estar a la vanguardia a nivel iberoamericano e internacional. El Decreto tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros:

- 1). El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).
- 2). Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.
- 3). Determinación de canal electrónico y físico para recibir las autorizaciones.
- 4). Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).
- 5). Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión.

Para datos recolectados a partir de la expedición del **Decreto 1377** se necesita:

- 1). Aviso de Privacidad (que se puede hacer estratégicamente en el mismo formato de autorización de la captura).
- 2). Definir o crear un área o sujeto responsable de la protección de la información personal, según el tamaño empresarial del cliente (es decir aquí opera el criterio de responsabilidad demostrada consagrado en los arts. 26 y 27 del Decreto 1377).

¹ Remanencia de Datos. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>

² Ley 1581 Protección de datos personales

- 3). Establecer cláusulas para transmisiones y transferencias de datos (si estas aplican).
- 4). Definir o conocer cuáles son los grupos de interés del cliente.
- 5). Definir las finalidades y los tratamientos genéricos en cada grupo de interés, pues esto se debe indicar en la política de tratamiento y en el formato de autorización.

Las empresas Colombianas no pueden ver la protección de datos como una norma ajena, deben empezar a preocuparse cuáles serán los mecanismos a implementar, la protección de datos debe verse cada día más como parte de su negocio es una actualidad global organizacional que debe estar lineada en su política de seguridad.

El artículo 27 del Reglamento 1377 establece que los responsables de los tratamientos deberán garantizar la estructura administrativa dentro de la organización que vele por el completo cumplimiento de la ley 1581, el cual compromete al Gobierno de la Organización, en el proyecto de adecuación será necesaria la colaboración de todas las áreas y departamentos que traten datos personales, colaboración que debe ser manejada desde las altas gerencias como norma de implementación en la seguridad de la información.

V. CRECIMIENTO DE IMPLEMENTACIONES DE SGSI

Es muy importante conocer el crecimiento que está teniendo el uso de SGSI en las Organizaciones, ya que esto refleja la situación actual, y como cada día las nuevas leyes, normas y/o regulaciones obligan a las Compañías a optar por certificaciones como lo es la ISO 27001.

Cada año ISO realiza una encuesta para identificar las compañías certificadas por año, en los resultados del año 2012 podemos encontrar las cifras reportadas en la siguiente tabla.

TABLA I
The ISO Survey of Management System Standard Certifications – 2012

Standard	Number of certificates in 2012	Number of certificates in 2011	Evolution	Evolution in %
ISO 9001	1 101 272	1 079 647	21 625	2%
ISO 14001	285 844	261 957	23 887	9%
ISO 50001	1 981	459	1 522	332%
ISO 27001	19 577	17 355	2 222	13%
ISO 22000	23 231	19 351	3 880	20%
ISO/TS 16949	50 071	47 512	2 559	5%
ISO 13485	22 237	19 849	2 388	12%
TOTAL	1 504 213	1 446 130	58 083	4%

ISO / IEC 27001:2005 establece los requisitos para los sistemas de gestión de seguridad de la información. A finales de diciembre de 2012, al menos 19 577 ISO / IEC 27001:2005 fueron certificados, un crecimiento del 13% (2 222), se habían emitido en 103 países y economías, tres más que en el año anterior. Los tres primeros países en cuanto al número total de certificados emitidos fueron Japón, el Reino Unido y la India, mientras que los tres primeros para el crecimiento en el número de certificados en 2012 eran Rumania, Japón y China.

En Colombia está creciendo el número de organizaciones que están implementando un SGSI, las nuevas leyes vigentes, como lo es la 1581 ha disparado un interés por buscar certificaciones como la ISO 27001. Para las compañías que tienen experiencia o un grado de madurez en estos temas, desarrollan con mayor rapidez las nuevas políticas al interior de estas, que cumplen con lo establecido en la Ley.

VI. SGSI COMO GENERADOR DE VALOR

El SGSI en las organizaciones debe verse como una herramienta para ayudar a la ejecución y cumplimiento de la protección de datos apoyando con procesos construidos dentro del mismo como un manual interno de políticas y procedimientos para cumplir con la Ley sobre protección de datos.

La adecuación a la Ley 1581, debe verse como una oportunidad de buscar los beneficios que puede producir en la organización este proceso no solo es verse como cumplir con la Ley, como es la

¹ Remanencia de Datos. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>

² Ley 1581 Protección de datos personales

obtención de un mejor conocimiento de los tratamientos y detectar las mejoras, incorporar mejores prácticas en Seguridad. Seguramente el mayor aporte que esta ley dejará es que cada Organización mejorará la relación y los procesos con las personas sobre las cuales trata sus datos y garantizarles la privacidad y sus derechos de Habeas Data.

Elaborar las políticas del tratamiento de la información y suministrarlas al registro nacional de bases de datos, el cual está a cargo de la Superintendencia de Industria y Comercio, detectando las mejoras, incorporar mejores prácticas en Seguridad Informática y Gestión Documental.

VII. CONCLUSIONES

Al adoptar un SGSI en cualquier organización, brinda una protección al activo más importante de cualquier compañía que es la información. Cuando se tiene que cumplir nuevas regulaciones en términos de seguridad, el modelo actual muestra sus bondades y genera ese valor que las compañías no ven al momento de invertir. El famoso ROI se puede evidenciar en la eficiencia, mejores tiempos de respuestas y cumplimiento de las leyes locales para aportar crecimiento y mejores prácticas a un país.

La ley 1581 establece madurez en la relación de la seguridad de la información en el país, el sistema de manejo de la información consiente de la necesidad de adoptar medidas establece un buen inicio con estas regulaciones que se pone al nivel internacional. Cada vez el auge de la información y el uso continuo de la misma requiere que las empresas se preocupen por mantener la seguridad de la información esto ayuda a ver importantes beneficios en las Organizaciones y en los dueños de la información.

REFERENCIAS

- [1] ITU-T Recommendation X.805 – “Security architecture for systems providing end-to-end communications” (alineada con iso/iec 18028 –2). <http://www.itu.int/rec/T-REC-X.805-200310-I/en> (octubre de 2009)
- [2] ISO/IEC 27000 “Information technology - Security techniques - Information security management systems - Overview and vocabulary”
- [3] ISO/IEC 27000 “Information technology - Security techniques - Information security management systems - Overview and vocabulary”
- [4] UNIT - ISO/IEC 27001:2005. “Tecnología de la información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos”.
- [5] TMForum. “Business Process Framework (eTOM v. 8.0)”. <http://www.tmforum.org/browse.aspx?catID=1647> (octubre de 2009)
- [6] Joan Magretta, “Stop Competing to Be the Best”, Noviembre 30 de 2011, Harvard Business Review. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>
- [7] ISO 27001 Portal en español. <http://www.iso27000.es/iso27000.html>
- [8] Carozo E., Freire G., Martínez G., “Análisis del Sistema de Gestión de Seguridad de la Información de ANTEL”, ANTEL.
- [9] María Eugenia Corti. “Análisis y automatización de la implantación de SGSI en Empresas Uruguayas”. Tesis de maestría, Universidad de la República, Facultad de Ingeniería, 2006.

Autores

Leidy Diana Rojas Garzón

Juan Carlos Martínez Meléndez

Ingenieros de Sistemas, en proceso final de obtener el título de la Especialización de Seguridad Informática en la Universidad Piloto de Colombia.

¹ Remanencia de Datos. <http://blogs.hbr.org/2011/11/stop-competing-to-be-the-best/>

² Ley 1581 Protección de datos personales