Revista Ciencia & Tecnología

No. 18, 30 de abril de 2018
ISSN impreso: 1390 - 6321

La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar

Information security: A crucial aspect that every company in the 21st century must manage

MSc, Roxana Patricia Cedeño Villacís[1]
rcedenov@hotmail.com

Recibido: 1/12/2017, Aceptado: 1/02/2018

RESUMEN
Este trabajo de investigación ha sido orientado a vislumbrar desde la revisión literaria, los aspectos cruciales que debe considerar la empresa para salvaguardar su información a través de la aplicación de normativas internacionales más reconocidas como son ISO/IEC 27001, ITIL y Cobit, con el fin de que la empresa pueda alcanzar su meta de disminuir las amenazas y vulnerabilidades, sean estas de origen interno o externo. Al inicio del artículo, se enfoca en presentar la conceptualización de seguridad de la información, riesgo, amenaza y vulnerabilidad; además, aborda brevemente una explicación de las 3 normativas mencionadas anteriormente y hace hincapié de la preocupación de los empresarios para los ataques que están afectando a las organizaciones; luego, se explica una metodología propuesta en relación de aspectos que debe considerar para la implementación de la seguridad de la información. En la última parte la Autora señala las conclusiones y recomendaciones. El presente documento, es producto de la revisión literaria obtenida de fuentes secundarias.

Palabras clave: Seguridad de la información, empresa del siglo XXI, vulnerabilidad, amenaza, riesgo

ABSTRACT
This research work has been oriented to envision, from the literary review, the crucial aspects that the company must consider safeguarding its information through the application of more recognized international regulations such as ISO / IEC 27001, ITIL and Cobit, in order to that the company can achieve its goal of reducing threats and vulnerabilities, whether internal or external. At the beginning of the article, it focuses on presenting the conceptualization of information security, risk, threat and vulnerability. In addition, it briefly addresses an explanation of the 3 regulations mentioned above and emphasizes the concern of entrepreneurs for the attacks that

[1] Universidad Técnica Particular de Loja. Ecuador

are affecting organizations; then, a proposed methodology is explained in relation to aspects that must be considered for the implementation of information security. In the last part, the Author points out the conclusions and recommendations. This document is the product of literary review obtained from secondary sources.

Keywords: Information security, 21st century enterprise, vulnerability, threat, risk

Introducción

Con la llegada del siglo XXI, los empresarios empezaron a preocuparse cada vez más por la automatización de sus procesos y por conseguir herramientas informáticas que les permitan obtener resultados de manera más ágil para su toma de decisiones. Además, observaron que el tratamiento de su información mediante aplicaciones informáticas era un mecanismo ideal para obtener una respuesta con mayor precisión en las acciones a emprender para su competitividad.

Las empresas con el tiempo se hicieron cada vez más tecnificadas; por lo que, sus Directivos empezaron a sentir temores y preocupaciones por los posibles riesgos que conlleva el uso de la tecnología, y la dependencia como tal a estas herramientas y aplicaciones informáticas; y el pensar, que su información esté en bases de datos que de alguna u otra manera pudieren verse amenazados o vulnerables ante situaciones externas o por aquellas que internamente el personal técnico no atendiere de manera oportuna.

En ese sentido, las preocupaciones latentes ante los posibles riesgos relacionados con la tecnología de información han permitido a organismos internacionales la generación de normas y recomendaciones para que las empresas lo pongan en práctica; esto, con el fin de disminuir las brechas que pudieren afectarle a futuro. En este trabajo de investigación, se mencionará algunas normas y modelos muy útiles para que las empresas puedan aplicarlo.

El presente documento, tiene como objetivo proveer el empresario de las directrices generales para que gestione la seguridad de la información en su organización. El impacto esperado del mismo es estimular a los directores y/o Gerentes a precautelar el bien más preciado de su empresa, que es la información.

Ha sido desarrollado bajo el enfoque cualitativo a través de documentación extraída de fuentes secundarias provenientes de artículos científicos, tesis, sitios web de empresas consultoras y periódicos. En este escrito, se utilizó la investigación descriptiva.

Desarrollo

Según [1] la información es el activo más valioso de una organización; y, por lo tanto, es necesario implementar técnicas cada vez más sofisticadas para protegerla. Para [2] la seguridad de información está relacionada con "la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio".

Para [3] el concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. En cambio, la seguridad de información se encarga de la protección de la información

de la empresa.

Refiere [4] que los servicios de tecnologías de la información son cada vez más complejos, produciendo afectaciones en el tiempo y en los costos; todo en función, de obtener una mayor eficiencia empresarial, que a la larga se hace más difícil de administrar.

Todo este proceso relacionado con la TI, hace que se derive en situaciones de amenazas y vulnerabilidades; entiéndase por amenaza a la situación o evento en la que el sistema se encuentre en posible peligro y genere como consecuencia un daño; la vulnerabilidad, es aquella debilidad que puede tener el sistema y que puede convertirse a futuro en amenaza. Por ejemplo, un terremoto es una amenaza latente para los sistemas informáticos, y la vulnerabilidad puede ser que el Centro de datos se encuentre ubicado en una zona altamente sísmica.

Otro factor fundamental que debe conocer la empresa, son los riesgos; al riesgo se lo define como la probabilidad de que un evento pueda ocurrir. Estos riesgos pueden tener diferentes tipologías, algunos autores han clasificado a los riesgos en físicos, químicos, biológicos, ergonómicos y psicosociales; otros, refieren además de los anteriores, a los riesgos tecnológicos, riesgos naturales y riesgos financieros. Para poder atender y remediar aquellos eventos de riesgos que pudiere presentarse en la empresa, es necesario que, dentro de la misma, se implemente políticas y procedimientos que aseguren una pronta y prolija atención a aquellas amenazas y vulnerabilidades que afecten la seguridad de la información. En la actualidad, existen modelos, estándares y normativas que ayudan a las organizaciones con las directrices a seguir para una buena práctica de gestión de la seguridad de la información y el análisis de los riesgos que incurren en este ámbito; entre ellos, se encuentra la norma ISO/IEC 27001, ITIL y COBIT.

Normativas Internacionales
ISO/IEC 27001
ISO 27001 como es comúnmente conocido, es una normativa internacional emitida por la Organización Internacionalización de normalización, con el propósito de describir los lineamientos que toda organización debiera efectuar para poder implementar un sistema de gestión de seguridad de la información.

El sistema de gestión de seguridad de la información (SGSI) es un modelo estratégico diseñado para toda organización que requiere establecer, crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información [5]. Hay que recalcar que esta normativa, le permitirá a toda organización que cumpla con sus lineamientos, obtener la certificación internacional. Este lineamiento, describe una serie de requerimientos que de manera general se presenta en la tabla 1.

La última versión de ISO/IEC 27001, es la 2013, la cual ha incluido cambios desde su versión 2005 referente a su estructura de 8 a 10 requisitos o cláusulas, también incorpora conceptos de la normativa ISO 31000 de Gestión de Riesgo; otro elemento, es que se eliminan los anexos B y C por ende ya no se hace explícito el uso del modelo PDCA (Plan-Do-Check-Act); y su anexo A, es modificado variando sus dominios, objetivos de control y controles.

Tabla 1. Etapas para implementar el SGSI

ISO/IEC 27001:2005	ISO/IEC 27001:2013
4. El sistema de gestión de seguridad de la información	4.Conocimiento de la organización y su contexto
5. Responsabilidad de la Dirección	5. Liderazgo
6. Auditorías internas SGSI	6. Planificación
7. Revisión de la gestión SGSI	7. Soporte
8. Mejora del SGSI	8. Operaciones
-	9. Evaluación del desempeño
-	10. Mejora

Fuente: Elaboración propia a partir de la ISO/IEC 27001 2005 y 2013

ITIL

Sus siglas provienen de biblioteca de infraestructura de tecnologías de información (ITIL), mismo que nació por la necesidad de incorporar en las organizaciones servicios de TI con altos estándares de calidad que soporten el cumplimiento de dichos objetivos [6].

ITIL se ha convertido en uno de los estándares con mejores prácticas de Gestión de Servicios de TI integradas bajo el enfoque de procesos. Entre los beneficios más significativos está la mejora en la satisfacción del cliente ya que los proveedores de TI saben y entregan lo que se espera de ellos, mayor flexibilidad para el negocio a través de un entendimiento mejorado del soporte de TI, flexibilidad y adaptabilidad mejoradas en los servicios de TI que soportan los procesos del negocio, beneficios de negocio ocasionados por sistemas mejorados en términos de la seguridad, precisión, velocidad y disponibilidad según los niveles de servicio acordados [7]. Cabe indicar además que esta normativa también permite a las organizaciones obtener la certificación internacional.

El modelo de ITIL consiste en la estrategia, el diseño, la transición, la operación y la mejora continua del servicio de TI, tal como se muestra en el grafico 1. En la actualidad, la última versión de ITIL es la 3.0.

Figura 1. Ciclo de vida ITIL

Fuente: http://www.bitcompany.biz/que-es-itil-cursos/

COBIT
El modelo COBIT (Control Objectives for In-formation and related Technology) es el marco aceptado internacionalmente de buenas prácticas para el control de la información TI y los riesgos que conllevan. COBIT se usa para implementar el gobierno de TI y mejorar los controles de TI. De igual manera, contiene objetivos de control, directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez [8].

La implementación de COBIT se hace a través de un sistema de control interno o también llamado marco de trabajo en el que debe vincularse con los requerimientos del negocio, donde además es necesario identificar los recursos de TI, y por supuesto definir los objetivos de control. Actualmente la versión de Cobit que está vigente es la 5. Sus principios que tienen una visión holística buscan satisfacer las necesidades de los interesados y que el marco de trabajo cubra a toda a la organización, en la figura 2 se puede apreciar sus principios.

Figura 2. Principios de Cobit

Fuente: Cobit 5

Preocupación de los Empresarios
Los empresarios han ido notando que, con la adquisición de mayor tecnología de información, también ha ido aumentando las vulnerabilidades y amenazas en sus organizaciones. Cada día, se conoce por la prensa de un nuevo ataque a empresa.

Las estadísticas refieren [9] que los daños causados por los delitos cibernéticos lleguen a 6 billones de dólares en el mundo en 2021, siendo su afectación la destrucción de datos, dinero robado, pérdida de productividad, fraude, eliminación de datos, sistemas hackeados y daño reputacional.

La empresa internacional Kapersky manifestó que en Latinoamérica se presentan 12 ataques por segundo, provocado por software malicioso; siendo Brasil el país con el porcentaje más alto [10], cifras realmente alarmantes.

Panda Security, en su sitio web menciona que el 91% de las pymes españolas sufren diariamente ataques informáticos y que sus orígenes provienen de web poco seguras, descargas de aplicaciones de internet y de virus recibidos por correo electrónico [11].

Estas recientes estadísticas demuestran que las empresas tienen una evidente exposición al riesgo, porque no han logrado detectar sus vulnerabilidades y amenazas, las mismas que a corto, mediano o largo plazo pudieren comprometer el activo más importante que es la información. ¿Pero qué origina todo esto?

Existen diferentes orígenes de ataques que se dan a las empresas, pudiendo ser externas o internas; lo interesante es que la mayoría de estos ataques provienen de colaboradores o empleados de la organización. Las estadísticas reflejan que los ataques en Latinoamérica se dan en un 38% proveniente por exempleados [12].

En definitiva, es claro que las empresas que aún no han logrado implementar un sistema de gestión o control interno para la seguridad de información, difícilmente podrán lograr prevenir los ataques, y peor aún tener una respuesta inmediata frente a esta situación, porque no han sido capaces de desarrollar políticas y procedimientos preventivos y correctivos ante los incidentes de seguridad.

Método y Resultados

Metodología para implementar la seguridad de la información

La autora, presenta la siguiente metodología de trabajo para que sirva como guía para la implementación de un sistema o control interno para la seguridad de la información en cualquier tipo de empresa, sea pública, privada, comercial, industrial, etc. En la figura 3 se observa los pasos a seguir.

1. Evaluar la situación actual de TI. En la actualidad, es raro encontrar una empresa u organización que no cuente con su departamento de tecnología de información o también llamado área de sistemas. Las empresas por pequeñas que estas sean cuentan con uno o varios colaboradores que se hacen cargo de dar soporte, mantenimiento preventivo y correctivo, programación y administración de base de datos. Estas que he mencionado, corresponden a gestiones primarias y relevantes en toda organización.

En ese sentido, lo primero que debe efectuar el Empresario, es solicitar un inventario existente de software, hardware, comunicaciones, personal, manuales, con el fin de determinar y conocer en primera instancia la situación real de TI.

2. Determinar la normativa. Según la necesidad de la empresa, sea en mejorar su nivel de servicios, calidad, mayor control de los riesgos o implementar todo un sistema de gestión, deberá escoger la normativa. Es necesario conversar previamente con el personal de TI, mantener reuniones de trabajo para escoger cuál de las

normativas sean ISO 27001, Cobit o ITIL sea más útil para los propósitos y objetivos del negocio. Cualquiera que seleccione, tiene el componente de seguridad y gestión de riesgos, que es vital administrar y controlar en la actualidad.

3. Seleccionar al experto. Probablemente, el personal de TI no ha tenido experiencia en temas relacionados con la implementación de todo un sistema de gestión de seguridad de la información; en esos casos, es necesario recurrir a un experto. En la actualidad, existen consultoras de prestigio que dominan este tema, evalúe y cotice, seleccionando al final la que mejor se ajuste en presupuesto y servicio.

Otro factor, que también debe evaluar el Empresario, es convertir a su personal de TI en experto, con cursos y capacitación continua en temas relacionados a la seguridad de información. En el mercado, existen preparaciones con certificaciones incluidas donde logran especializar al personal de TI en seguridad de la información. Es una opción viable y más económica que la contratación de una consultora.

Figura 3. Metodología para implementar la seguridad de la información
Fuente: Elaboración propia

4. Aplicar la normativa. El proceso más largo y duro, es arrancar con la implementación de la normativa, todo en pos de lograr la disponibilidad, confidencialidad e integridad de la información. Durante esta etapa, la organización deberá efectuar cambios en sus políticas y procedimientos, adquirir nuevas herramientas para mejorar su seguridad, deberá además identificar, analizar y evaluar sus riesgos, será necesario efectuar periódicamente auditorías internas al sistema de seguridad de la información, y será necesario crear una unidad de Seguridad de la información, la cual deber ser independiente del área de Sistemas, pues así lo recomiendan las buenas prácticas.

5. Obtener la certificación. Una vez alcanzado todos los objetivos requeridos en el sistema de gestión, el experto deberá notificar a la organización que ésta se encuentra lista para obtener la certificación. En esta fase, se deberá contratar a una empresa certificadora, que no es la misma consultora experta que colaboró con la aplicación de la normativa. El proceso para obtener la certificación consistirá en una auditoría, el tiempo de duración dependerá del tamaño de la empresa.

Conclusiones

Para el desarrollo de este trabajo de investigación, se identificaron algunas definiciones para la seguridad de información, amenazas, vulnerabilidades y riesgos. También se abordó las normativas internacionales más reconocidas en el ámbito de la seguridad de la información como son las ISO/IEC 27001, ITIL y Cobit.

En cuanto a las preocupaciones de los empresarios, a través de cifras estadísticas se hicieron resaltar los ataques que actualmente se están dando a las empresas, sus orígenes y la importancia del por qué es necesario implementar un sistema de gestión o control interno para la seguridad de la información.

Se explicó una metodología propuesta por la Autora de 5 pasos, con el fin de que sirva como mecanismo para iniciar la gestión y el control del activo más importante que es la información.

Se recomienda a las empresas que aprovechen los avances en el tema de la seguridad de la información, ya que la misma se encuentra normada como buena práctica; por lo que, si aún no ha realizado acciones en pos de disminuir las amenazas y vulnerabilidades, entonces ya es el momento de hacerlo.

Este siglo XXI, ha traído consigo la creación de delincuentes denominados cibercriminales, quienes dedican su tiempo para atacar a empresas vulnerables, y aprovecharse de la información sustraída de manera ilegal, para hacer mal uso de ella.

Considere, que gran parte de los ataques a las empresas provienen de exempleados; en virtud de ello, es muy importante fortalecer los procedimientos de salida del personal y la eliminación de los accesos físicos y lógicos. En muchas ocasiones, esto queda a un lado, o simplemente por no existir una política institucional, el personal no sabe cómo gestionarlo. Es ahí, donde el contar con un sistema de control o sistema de gestión de seguridad de la información, se hace imprescindible.

El implementar un sistema de seguridad de la información es vital para la supervivencia de la empresa del siglo XXI; y, por tanto, debe ser considerado en todo plan estratégico organizacional; así como también, es importante contar con una unidad especializada en la seguridad de la información al interior del negocio.

Referencias bibliográficas

[1] A. Angarita, C. Tabares y J. Ríos, Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento, Entre Ciencia e Ingeniería, 2015.

[2] L. Gómez y A. Andrés, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR, 2012.

[3] E. Domínguez, N. Paladines y C. Flores, Ética y seguridad informática en el sector de la salud pública en el siglo XXI, *Revista científica Dominio de las ciencias*, 2016.

[4] Gestión de los servicios de tecnología de información: Modelo de aporte de valor basado en ITIL e ISO/IEC 20000, El profesional de la información, 2013.

[5] ISO/IEC, Estándar Internacional ISO/IEC 27001, 2005 y 2013.

[6] J. Palacios, J. Rodríguez y C. García, Modelo de gestión de servicio ITIL para E-

learning, Bogotá: *Revista Educación en Ingeniería*, 2017.

[7] Y. Medina y D. Rico, Modelo de gestión de servicios para la universidad de Pamplona: ITIL, Scientia et Technica, 2008.

[8] V. Montaño, La gestión de la seguridad de la información según Cobti, ITIL e ISO 27000, *Revista Pensamiento Americano*, 2011.

[9] IT now, «Revista IT Now» [En línea]. Available: https://revistaitnow.com/las15-principales-estadisticas-2017/. [Último acceso: 21 11 2017].

[10] BBC, «BBC mundo,» [En línea]. Available: http://www.bbc.com/mundo/noticias- 37286420. [Último acceso: 21 11 2017].

[11] Panda, «Panda Security,» [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/pymesataques- informáticos/. [Último acceso: 21 11 2017].

[12] Welive security, «welive security» [En línea]. Available: https://www.welivesecurity.com/la-es/2014/10/06/incidentes-de-seguridadcrecen-2014/. [Último acceso: 21 11 2017].