Sistemas de seguridad de la información, factor diferencial para la competividad empresarial en pymes de la región Caribe*

Information security systems, differential factor for business competitiveness in smes of the Caribbean region

Hugo Hernández Palma[1]
David Martínez Sierra[2]

* Artículo resultado de investigación en los sistemas de seguridad de la información, factor diferencial para la competitividad empresarial en pymes de la región Caribe. Trabajo de aula en la asignatura Sistemas integrados de gestión del programa maestría en Ingeniería Industrial Universidad Simón Bolívar.

1 Ingeniero Industrial, Especialista en Estudios Pedagógicos, Especialista en Diseño y Evaluación de Proyectos, Magíster en Sistema de Gestión. Docente Programa de Administración de Empresas Universidad del Atlántico.
Email: hugoghernandezpalma@gmail.com

2 Ingeniero Industrial, Magíster en Ingeniería Industrial, Docente Universidad Simón Bolívar.
Email: dmartinez@unisimonbolivar.edu.co.

RESUMEN

La realidad económica que demanda la globalización exige que toda organización se oriente en conseguir un nivel de óptima competencia; lo anterior hace pertinente pensar en la institución de un adecuado sistema de gestión de la seguridad informática (SGSI). Esta necesidad promueve el cumplimiento de unos parámetros esenciales que faciliten la toma de decisiones oportunas y que permitan elevar los niveles de seguridad al interior de cualquier tipo de organización. Con el presente artículo se busca analizar los diferentes conceptos y percepciones que se deben tener en cuenta para la puesta en marcha, seguimiento y mejoramiento de los SGSI. Se revisarán las bases fundamentales para establecer políticas organizacionales de seguridad que faciliten la identificación de los riesgos informáticos y, por ende, programar planes de acción para aminorar su impacto. Posteriormente se propondrán las medidas preventivas y correctivas como mecanismos de control, y finalmente se observará la situación actual, de los SGSI en las Pymes de la región Caribe.

Palabras clave: políticas de seguridad, información, medios digitales, controles, riesgos.

ABSTRACT

The economic reality demanded by globalization, requires that every organization is oriented towards achieving a level of optimal competition, this makes it pertinent to think of the institution of an adequate computer security management system (ISMS). This need promotes the fulfillment of essential parameters that facilitate the making of timely decisions and that allow to raise the levels of security within any type of organization. This article aims to analyze the different concepts and perceptions that must be taken into account for the implementation, monitoring and improvement of ISMS. The fundamental bases will be revised

to establish organizational security policies that facilitate the identification of computer risks and, therefore, to plan action plans to mitigate their impact. Subsequently, the preventive and corrective measures will be proposed as control mechanisms, and finally the current situation of the ISMS in the SME's of the Caribbean region will be observed.

Keywords: security policies, information, digital media, controls, risks.

INTRODUCCIÓN

Actualmente, generar valor en el ámbito empresarial es un factor primordial para toda organización. Las oportunidades de negocio que brinda la economía dinámica y globalizada hacen necesario que las empresas conduzcan sus esfuerzos con nuevas herramientas tecnológicas y, por consiguiente, se debe tener en cuenta, en igualdad de condiciones, los beneficios y también los riesgos.

Lo precedente sugiere a toda corporación la inserción de políticas renovadas al direccionamiento estratégico de cada entidad, y es lo que hoy se conoce como: sistema de gestión de seguridad para la información (SGSI). Lograr los instrumentos necesarios para la identificación de los riesgos y peligros a los que puede estar expuesta la información empresarial brinda a cada organización, la tranquilidad para cuidar y preservar su patrimonio más valioso, generando así efectos colaterales positivos como mejora en la gestión con las partes interesadas en todo el proceso (Fernández, 2010, p.35).

Hoy día se han podido conocer los avances más notorios en tecnología, sus aplicaciones y alcances. La información se origina, transforma y comunica con base en plataformas virtuales que dependen de los

desarrollos y avances que a diario se incorporan a los procesos productivos. Para obtener competitividad y alta participación en los mercados, es necesario salvaguardar la información que se genera en todos los procesos internos, ya que en esta información, se fundamenta la infraestructura organizacional que, si bien es de tipo digital, significa para toda organización un activo prioritario y notable para el desarrollo a corto, mediano y largo plazo (Perafán, 2014).

Paralelo a los avances tecnológicos, muchas empresas siguen viendo la inversión en esta área como algo innecesario o de bajo impacto en los resultados empresariales. Sin embargo, la experiencia y seguimiento de cifras a nivel mundial muestra que la no adopción de los SGSI puede impactar a toda empresa con sobrecostos, afectación de la imagen corporativa, reprocesos y pérdida de información diferencial (datos financieros y otros).

De acuerdo a las premisas citadas, y tomando en cuenta que actualmente el desarrollo tecnológico es protagonista en el desarrollo empresarial tanto nacional como internacional, se desarrollará a continuación una revisión detallada que destaque la importancia de incluir en la planeación estratégica de toda empresa los SGSI como factor diferencial para el crecimiento, posicionamiento y consolidación de las organizaciones en los diferentes ámbitos de competencia.

A nivel empresarial es importante la incorporación de herramientas que estén acorde a los modelos y estándares actuales; para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información, que en un futuro será la base para implementar el sistema de gestión de seguridad de la información (SGSI), que permitirá mantener un modelo de negocio estable logrando un valor agregado y posicionamiento a nivel regional (Perafán, 2014).

Según Parra & Porras (2007), desde el enfoque empresarial, un sistema de información es la columna vertebral. En el país existen diversos riesgos a los que normalmente se está expuesto por diferentes factores externos, ya sea por la falta de estándares de seguridad o políticas al interior de las empresas. Para garantizar que la seguridad de la información sea gestionada correctamente se debe identificar, inicialmente, su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- 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.

Las empresas que se acojan y cumplan estos estándares dentro de sus operaciones serán reconocidas como actores seguros y tendrán ciertos beneficios en la reducción de sus operaciones, ahorro de tiempos y procesos más seguros, derivados de la manipulación de la información.

SITUACIÓN ACTUAL DE LA SEGURIDAD INFORMÁTICA EN COLOMBIA

Son muchas las fuentes que se pueden tomar en cuenta para realizar un diagnóstico de la situación actual de los SGSI en Colombia; sin embargo, la reciente Encuesta Nacional de Seguridad Informática realizada en el país por la Asociación Colombiana de Ingenieros de Sistemas, la cual incluyó información de todos los sectores productivos y contó de manera adicional con organizaciones especializadas en seguridad, aporta mucha información sobre los diferentes riesgos, amenazas y

ataques informáticos que de forma reiterada se presentan en el país, y sugiere las causas que se estiman relevantes para el tema (Almanza, 2016).

De manera local, el gobierno colombiano viene trabajando en diferentes programas desde el ministerio de las TIC, estimulando las prácticas que incentiven la protección total del proceso desde su punto de inicio hasta el final, esto con el fin de contar con un sistema integral de protección, que comprenda medidas de seguridad adoptadas, coordinadas y enlazadas entre ellas.

La velocidad en el tiempo de respuesta en los negocios, es de vital importancia; por esta razón, se debe tener la capacidad de reaccionar rápidamente (Niebles, Hernández & Cardona, 2016), para lo cual es necesario invertir en una red de información que permita rápido acceso, información veraz y concisa. De acuerdo a lo anterior, en el mercado existen ofertas atractivas a bajos costos que ayudan a las empresas para implementar un sistema de información certificado.

RIESGOS INFORMÁTICOS

Con la globalización y expansión del desarrollo tecnológico, y la masificación del internet, las empresas han adoptado gran variedad de soluciones informáticas con la finalidad de facilitar y agilizar los procesos al interior de cada organización. En la medida en que la tecnología se ha hecho cotidiana, se han dinamizado muchos de los procesos que se consideran vitales al interior de las empresas, pero al mismo tiempo, se han evidenciado los riesgos o peligros que estos avances pueden generar para la operación de todo ente. Lo anterior, plantea la necesidad de tener herramientas que permitan la identificación, gestión y erradicación de los riesgos informáticos (Cano, 2006).

Al hablar de riesgos, se puede afirmar que ninguna empresa, por más que invierta en la gestión tecnológica, está exenta de sufrir amenazas o fallas asociadas a los peligros de la red. De esta realidad se origina la necesidad de orientar esfuerzos y recursos a la investigación, puesta en marcha e innovación de mecanismos de control y protección (Dutra, 2008).

TIPOLOGÍA DE LOS RIESGOS INFORMÁTICOS

Para lograr la identificación oportuna de los riesgos, todas las organizaciones deben contar con instrumentos adecuados y ajustados a las necesidades propias y particulares de acuerdo a su actividad: comercial, industrial o de servicios (Fernández, 2010). Los riesgos pueden ser identificados y clasificados básicamente en dos grandes grupos que son: riesgos externos y riesgos internos.

Riesgos externos. Como su nombre lo sugiere, son aquellos cuyo origen se da fuera del ente productivo, y son usualmente conocidos como *malwares*, gusanos, virus o *spam*. Normalmente estos riesgos son producto de la mala fe de personas dedicadas a estropear las actividades productivas, exempleados insatisfechos o competidores desleales. Por ser una amenaza poco predecible, requiere de un plan de acción en constante renovación y actualización.

Riesgos internos. En este apartado se hace referencia a los peligros generados dentro de la misma organización y que son resultado de la operación de los empleados o usuarios, quienes en un momento determinado, por omisión, intención o descuido, pueden generar situaciones de impacto y falla, que representan para la empresa sobrecostos, demoras y traumas. Estos peligros normalmente se originan por el uso indebido, con o sin intención, de recursos como el internet, equipos o datos.

Ambos tipos de riesgos demandan un trabajo constante y de innovación permanente que brinde un escenario de control y seguimiento, pues solo así se podrá lograr un entorno de seguridad que fomente el sano desarrollo de cualquier tipo de operación empresarial (Baquerizo, 2016).

MODELO DE SEGURIDAD DE LA INFORMACIÓN

Para la gestión de la seguridad de la información es habitual establecer o adoptar un modelo, partiendo de la información como activo central. En este modelo se identificarán tanto los principios básicos que determinan la necesidad del nivel de seguridad en información, como los actores que afectan a su estado, tanto positivamente como negativamente (Momphotes & Alzate, 2014).

Existen varios modelos para estimar el estado de la seguridad de la información; sin embargo, el más extendido está basado en los principios básicos de Confidencialidad, Integridad y Disponibilidad que se detallarán en los apartados siguientes (Barraño, 2016).

Confidencialidad: este principio permite asegurar que los individuos solamente tienen acceso a los recursos e información a los que están explícitamente autorizados. Por ejemplo, una transacción de tarjeta de crédito en internet, requiere que el número de tarjeta de crédito sea transmitida desde el comprador al comerciante, y el comerciante del establecimiento a una red de procesamiento de transacciones. Si una parte no autorizada obtiene el número de la tarjeta de algún modo, se habrá producido una violación de la confidencialidad (Guindel, 2010).

Integridad: este componente garantizará que la información del sistema estará disponible tal y como se almacenó, y que se controla cualquier modificación no autorizada. La violación de integridad se presenta

cuando un empleado, programa o proceso (por accidente o con intencionalidad) modifica o borra los datos importantes que son parte de la información; así mismo, hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La comprobación de integridad de un mensaje se puede obtener mediante distintos métodos, uno de los más habituales suele realizarse mediante la obtención de un conjunto de datos auxiliares que permiten la comprobación de la integridad, como puede ser la firma digital (Freitas, 2009).

Disponibilidad: este lineamiento facilitará que los recursos de los activos de información, y la información como tal, se encontrarán disponibles cuando sean necesarios para una entidad autorizada. En el caso de los sistemas utilizados para almacenar y procesar la información, los controles de seguridad deben asegurar la disponibilidad de la información, los propios sistemas y los canales de comunicación, evitando interrupciones del servicio debido a incidentes causados por factores diversos como cortes de energía, fallos de *hardware*, *software* malicioso, actualizaciones del sistema… etc. (Velásquez, 2003).

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA

A continuación se evocan algunos juicios encontrados con respecto a la gestión del riesgo en la seguridad informática; parte de ellos, de documentos respaldados por organismos reconocidos por su labor investigativa y sus aportes a las tecnologías de la información y comunicaciones (TIC).

La presencia de amenazas que comprometen el sistema, deben ser analizadas y a su vez evaluadas las probabilidades, de que una amenaza aproveche esas vulnerabilidades. Eugene Howard Spafford, profesor de la Universidad de Purdue, ubicada en Indiana, Estados Unidos, dijo:

"El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón, y sellado en una habitación con guardias armados. E incluso así, tengo mis dudas". La gestión del riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Para comprender aún mejor la gestión del riesgo, se hace claridad de los siguientes conceptos:

a) Activo: como en los aspectos contables existe el activo y el pasivo, la información ahora posee un valor importante, y por eso se lo considera un activo. Si un alumno posee el trabajo final de grado y no posee un *backup* o resguardo en otro dispositivo, ese activo corre un serio riesgo de sufrir algún daño irrecuperable.
b) Amenaza: todo aquello que pueda provocar un daño a nuestro activo. Por ejemplo, si un virus corrompe el ordenador en donde el alumno tiene su trabajo final, no podrá acceder al momento de presentarlo y tal vez lo pierda.
c) Vulnerabilidad: son las inseguridades que posee el activo, tanto por problemas tecnológicos, como problemas de procedimientos. Está demostrado que la gran mayoría de pérdidas de activos son por falta de procedimientos o desconocimiento. El alumno no ha realizado copias de su trabajo en otros medios.
d) Riesgo: es la probabilidad de que una amenaza aproveche una vulnerabilidad. Siguiendo el caso del ejemplo, se supone que el equipo no posee una descarga a tierra, y en una noche tormentosa el equipo sufra una descarga y se queme el disco (Dutra, 2008).

Un proceso de gestión de riesgo va a permitir a la organización entender cuál es su situación de seguridad actual, le va a facilitar tomar decisiones adecuadas para mitigar los riesgos; también evaluar qué medidas se implementan a largo y corto plazo, y al final precisará si

las decisiones fueron las correctas (North, 2003). Enrique Dutra, Consultor de IT & Seguridad, certificado en seguridad de Windows desde el 2005, durante los últimos seis años por Microsoft; afirma que en la gestión de riesgos se involucran cuatro estadios:

a) Situación actual: un análisis de la situación de seguridad de la compañía para entender cómo se están tratando los activos, qué niveles de seguridad existen, qué leyes se están cumpliendo y cuáles no. Es lo que se denomina la foto. En esta etapa, suelen llevarse a la práctica los clásicos "test de vulnerabilidad" o "test de penetración". Los mismos, deben ser rigurosos y muy bien planificados, ya que muchas veces, hay profesionales que, con el afán de demostrar todos sus conocimientos de intrusión, provocan caídas de servicios que ponen en riesgo a la compañía a nivel funcional.
b) Definir pasos a seguir: con base en un informe detallado de la situación actual, un comité formado por los responsables de sistemas, RRHH, legales y la gerencia, deberán definir cuáles son los pasos a seguir para atacar el riesgo.
c) Implementación: con base en las decisiones tomadas se implementan las normas, procedimientos, actualizaciones y ajustes que sean requeridos y que fueron aprobados por el comité. La misma debe ser rigurosamente planificada, ya que hay puntos que deben ser tenidos en cuenta para no impactar en los procesos de negocios.
d) Monitorear: analizar el éxito de las implementaciones llevadas a cabo, verificar qué desvíos surgieron y planificar un nuevo análisis en un período acorde en la compañía. Los factores críticos de éxito para que el proceso de la gestión de riesgos cumpla los objetivos establecidos, requieren de apoyo incondicional de la gerencia desde el inicio y durante todo el proceso; involucrar a todo el capital intelectual de la organización con participación activa y compromiso

hacia la seguridad de la informática; conocer los procesos críticos de negocio de la organización y qué activos intervienen: implementar los cambios sugeridos que permitan mitigar los riesgos; dar a conocer a toda la organización el proceso de la gestión de riesgo (Dutra, 2008).

Adicionalmente se resalta la importancia de la alta gerencia en la gestión del riesgo: la práctica ha demostrado que la función y los riesgos de las TIC a menudo no son bien comprendidos por las principales partes interesadas de una organización, entre ellos los miembros de la junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de las TIC para alcanzar los objetivos estratégicos; en consecuencia, deberían ser los responsables de la gestión de los riesgos (Dutra, 2008). Sin una clara comprensión de la función y de los riesgos asociados a las TIC, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos. Estos no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de las TIC, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos (Hernández, 2011). Por consiguiente, son responsables de la gestión de los riesgos asociados. La gestión eficaz de los riesgos promueve la mejora continua y es una parte de las actividades diarias.

En el tema de gestión de riesgos no todo está dicho; es un proceso que evoluciona constantemente y de forma rápida, paralelo a las nuevas TIC. Para finalizar con los principios de la gestión del riesgo, es pertinente concluir con las estrategias más utilizadas para reducir (mitigar) el riesgo:

a) Evitar riesgos: se debe salir de las actividades o de las condiciones que dan lugar a riesgo, eliminar la causa raíz; se puede aplicar cuando no hay otra respuesta adecuada.
b) Reducción de riesgos/mitigación: corresponde a las medidas tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto. Al aplicar los controles sobre las causas del riesgo se reduce la frecuencia o su materialización futura. La eficacia de esta estrategia se puede medir por medio de los indicadores establecidos en los planes de control.
c) Riesgo compartido/transferencia: transferencia o distribución de una parte del riesgo; las técnicas más comunes son los seguros y la subcontratación. Sin embargo, el riesgo no se transfiere por completo al subcontratista o aseguradora, la empresa sigue asumiendo parte del riesgo y además se expone a otros riesgos relacionados con la subcontratación o aseguramiento.
d) Aceptación del riesgo: no se toman medidas relativas con un riesgo particular, y la pérdida es aceptada cuando se produce, esto es diferente de ignorar el riesgo. En ocasiones se considera aceptar el riesgo cuando mitigarlo resulta más costoso que el mismo impacto que este pueda producir a la organización (Fernández, 2010).

METODOLOGÍA

Tomando como base un estudio cuantitativo, se aplicó una encuesta a 50 empresarios de la región Caribe, con la finalidad de indagar sobre la aceptación y uso del concepto de tecnologías para la seguridad de la información. Se definió este tipo de análisis ya que permite evaluar, predecir y estimar, las concepciones de los empresarios frente a los SGSI. En palabras de Jurado (2011), la medición cuantitativa, permite profundizar en aspectos de la realidad de un sector, comunidad o sociedad.

Con este instrumento se buscó identificar los aspectos más sobresalientes o de mayor interés por parte de los empresarios, para posteriormente postular recomendaciones para la gestión empresarial basada en la seguridad de la información. La encuesta se diseñó con preguntas cerradas y de selección múltiple para facilitar la recolección de la información y la interacción con los empresarios. Los interrogantes en su orden aparecen a continuación, con una gráfica ilustrativa que facilita el análisis de cada cuestión. La muestra se determinó de manera no probabilística con fines especiales, ya que el objetivo principal es recoger la impresión de un determinado sector frente a una posición en particular (Jurado, 2011).

RESULTADOS

Pregunta 1. ¿Es importante salvaguardar la información de su empresa, para el desarrollo normal de sus actividades?

Para el 85 % de las pymes, lograr mantener a salvo la información de su negocio es un factor vital, puesto que esto garantiza que sus secretos, particularidades y componentes competitivos, permanezcan lejos de agentes externos, que puedan impactar en la operación normal. Este indicador reitera lo expuesto por algunos autores, quienes expresan que la información es una fuente dinamizadora de todo el marco empresarial, y pondera los aspectos sustanciales para fomentar un crecimiento a futuro (Almanza, 2016).

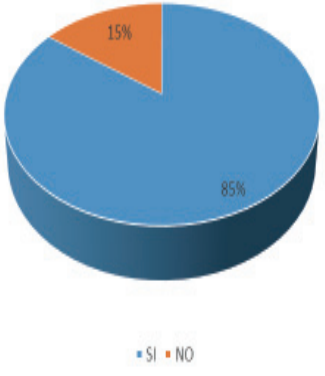

Figura 1. Importancia de la Seguridad de la Información Empresarial
Fuente: Elaboración Propia, 2016.

Pregunta 2. ¿Cuáles son las principales ventajas competitivas del buen manejo de la información?

Para el 55 % de los empresarios la ventaja más palpable se consolida en la innovación, ya que al tener la información completamente alejada del medio exterior, es posible sacar al mercado, productos o servicios ajustados a los requerimientos de un público que demanda creatividad y nuevas propuestas. Esta posición guarda concordancia, con las teorías recientes que muestran cómo al innovar se pueden procrear escenarios de desempeño que potencian la calidad y buenas prácticas en cualquier tipo de negocio (Niebles, Hernández & Cardona, 2016).

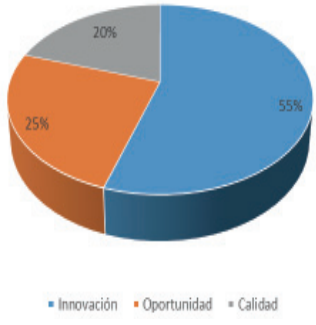

Figura 2. Ventajas de la seguridad de la información
Fuente: Elaboración Propia, 2016.

Pregunta 3. ¿Cómo maneja y custodia la información vital para su empresa en la actualidad?

Este apartado permite apreciar el enorme rezago que existe al interior de las pymes, en cuanto a la actualización e implementación de las TIC. Solo el 25 % de los empresarios maneja recursos digitales y un 10 % mecanismos combinados. Lo anterior hace importante fomentar la capacitación

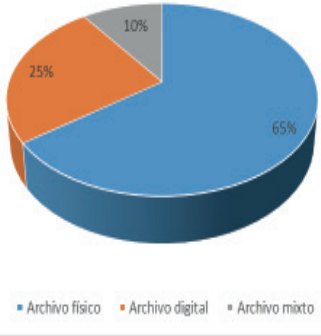

Figura 3. Mecanismos de Seguridad para la Información
Fuente: Elaboración propia, 2016.

a los líderes responsables de estas áreas, ya que al tener la información en un 65 % en archivos solo físicos, la exposición y vulnerabilidad es demasiado alta. Lo expuesto motiva la adopción de nuevas teorías de direccionamiento estratégico y genera la necesidad de cambiar los mecanismos actuales; solo así se podrá contar con herramientas necesarias al interior de los sectores productivos y de servicios (Parra & Porras, 2007).

Pregunta 4. ¿Qué espera de un sistema de seguridad para el manejo de la información?

Ante el cuestionamiento de las expectativas o resultados esperados por parte de los empresarios, se encuentra que el 35 % aspira a que estos procesos sumen y no resten, es decir, que dinamicen la operación cotidiana; un 34 % que agilicen; y un 31 %, que estos mecanismos puedan ajustarse a sus presupuestos para inversiones. Los SGSI, vienen siendo adoptados en muchos países como un mecanismo de competencia y, por tanto, una consecuencia directa es el desarrollo económico integral que permite, alcanzar tanto las metas financieras, como aquellas relacionadas con el mercado y sus exigencias (Freitas, 2009).

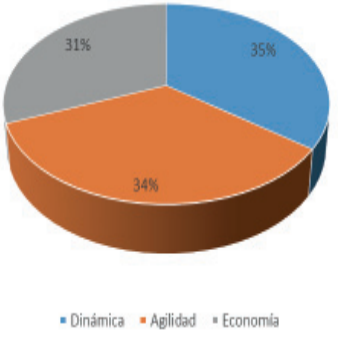

Figura 4. Expectativas frente a los SGSI
Fuente: Elaboración Propia, 2016.

CONCLUSIONES

Los Sistemas de Gestión de Seguridad de la Información (SGSI), fueron diseñados para proteger las tareas relacionadas con la gestión y admi-

nistración de datos a través de diferentes medios, y las acciones relacionadas con ello. La implementación con SGSI nos permite identificar los procesos necesarios, aplicar controles, cumplir con los objetivos de una organización, además de mejorar dentro del mercado competitivo. Cabe recalcar que estas métricas de ayuda no se cumplirían si no está involucrada la dirección.

Hoy día es importante contar con estrategias y medios que permitan la sensibilización del SGSI permanentemente, con los usuarios y colaboradores, ya que ellos son los responsables del uso adecuado de la información. Las mejoras al SGSI pueden posibilitar niveles de madurez fijados por la organización.

Un SGSI conlleva a cambios de procesos y estructuras, pero hace que la innovación, competitividad y dinamización, se incorporen como activos intangibles de las organizaciones, facilitando su crecimiento y proyectando su posicionamiento al interior de un mercado globalizado.

REFERENCIAS BIBLIOGRÁFICAS

Almanza, A. (2016). "Tendencias 2016 - Encuesta nacional de seguridad informática". *Revista Sistemas, 139*.

Barraño, G. (2016). Revisión de la Seguridad en la Implementación de Servicios sobre IPv6. *INGE CUC, 12*(1), 86-93.

Baquerizo, A. (2016). Análisis de la Seguridad en los Sistemas de e-Gobierno mediante el Problema SAT. *INGE CUC, 12*(1), 73-79.

Cano, J. J. (2006). Asociación Colombiana de Ingenieros de Sistemas. *Revista SISTEMAS, Asociación Colombiana de Ingenieros de Sistemas (ACIS), 96*. Recuperado el 03 de 2012, de Inseguridad Informática y Computación Anti-Forense: Dos Conceptos Emergentes en Seguridad de la Información: www.acis.org.co

Dutra, E. (2008). Gestión de Riesgo en Procesos de Negocios. *Revista Hakin, 9*(33), 55-65.

Fernández, L. A. (2010). *La Gestión del Riesgo Operacional de la teoría a su aplicación*. México: Limusa - Noriega Editores.

Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 6*(1), 43-55.

Guindel, E. (2010). Calidad y seguridad de la información y auditoría informática. Madrid: Universidad Carlos III.

Hernández, H. (2011). La gestión empresarial, un enfoque del siglo XX, desde las teorías administrativas científica, funcional, burocrática y de relaciones humanas. *Revista Escenarios, 9*(1), 38-51.

Jurado, Y. (2011). *Metodología de la investigación*. (5ta. Reimpresión). México: Esfinge.

Momphotes. L. F & Álzate, A. (2014). *Prototipo para la auditoria de sistema de gestión seguridad de la información (SGSI)*. Pereira.

Niebles, W., Hernández, H. & Cardona, D. (2016). Gestión tecnológica del conocimiento: herramienta moderna para la gerencia de instituciones educativas. *Revista de Investigación e Innovación, 7*(1), 25-36.

North, K. (2003). "Organización basada en Conocimiento (La Cuarta Dimensión)". Documentación facilitada en el Taller "Estado del Capital Intelectual" del Foro del Conocimiento Intellectus. Madrid, vol. 1. 15-35.

Parra, C. & Porras D. (2007) "Las amenazas informáticas: Peligro latente para las organizaciones actuales". *Gerencia tecnológica Informática, 6*(16), 85-97.

Perafán, J. (2014). "Análisis de Riesgos de la Seguridad de la información para la Institución Universitaria Colegio Mayor del Cauca, M.C.

Velásquez, L. (2003). *Estudio del alcance de la implantación de tecnologías de la información, como apoyo al mejoramiento de los procesos*. Bogotá.

Cómo citar este capítulo:
Hernández Palma, H. y Martínez Sierra, D. (2017). Sistemas de seguridad de la información, factor diferencial para la competividad empresarial en pymes de la región Caribe. En E. De la Hoz Granadillo, D. Martínez Sierra, E. Orozco Acosta, R. De la Hoz Reyes, J. C. Herrera Vega, H. Hernández Palma, . . . L. E. Ortiz Ospino, D. Martínez Sierra, H. Hernández Palma, & R. De la Hoz Reyes (Comp.), *Estudios de competitividad y análisis empresarial en la región Caribe* (pp.91-108). Barranquilla: Ediciones Universidad Simón Bolívar.