# El sistema de información y los mecanismos de seguridad informática en la pyme

## The information system and computer security mechanisms in the SMEs

**Recibido:** 2 de febrero de 2016
**Evaluado:** 28 de abril de 2016
**Aceptado:** 17 de mayo de 2016

**Omar Javier Solano Rodríguez (Colombia)**
PhD(c) en Administración y Dirección de Empresas
Universidad del Valle
omar.solano@correounivalle.edu.co

**Domingo García Pérez de Lema (España)**
Doctor en Ciencias Económicas y Empresariales
Universidad Politécnica de Cartagena
domingo.garcia@upct.es

**Juan Jesús Bernal (Colombia)**
Doctor en Ciencias Económicas y Empresariales
Universidad Politécnica de Cartagena
juanjesus.bernal@upct.es

**Resumen**

Este trabajo muestra los resultados de una investigación en Cali (Colombia), que tuvo como propósito determinar empíricamente cómo la participación del usuario, los factores tecnológicos y la gestión organizacional contribuyen al diseño y desempeño de los controles al sistema de información (SI) de la pequeña y mediana empresa (pyme). Para ello, se realizaron 107 encuestas sobre las prácticas de planeación del SI, la dirección organizacional, el uso de herramientas tecnológicas, el diseño y desarrollo de los controles que se usan para prevenir y detectar el riesgo informático. Con el fin de contrastar estadísticamente las hipótesis planteadas, las estimaciones se realizan a partir de regresiones lineales multivariantes por mínimos cuadrados ordinarios (MCO). Los resultados obtenidos permiten inferir que a un mayor apoyo del usuario y de la administración, en la gestión y el soporte de herramientas tecnológicas, se logran mejorar los controles y se contribuye

**Summary**

This work shows the results of an investigation in Cali (Colombia), which was aimed to empirically determine the user participation, technological factors and organizational management that contribute to the design and performance of controls in the information system (IS) of small and medium enterprises (SMEs). To do this, 107 surveys were carried out to determine the (IS) practices and planning, organizational management, the use of technological tools, design and development of controls used to prevent and detect IT risks. In order to statistically compare the proposed hypotheses, estimates are made from multivariate linear regression by ordinary least squares (OLS). The results allow us to infer that by having an increased user and administrative support, management and technological tools support, these controls are able to improve and help minimize IT risks in the company. This work promotes studies on managing IT risks, administrative and technologi-

a minimizar el riesgo informático en la empresa. Este trabajo favorece los estudios sobre la administración del riesgo informático, las herramientas administrativas y tecnológicas usadas en la pyme con la intención de mejorar el sistema de control interno y su efecto respecto del desempeño, la disminución de los costos operacionales y el rendimiento del SI en la organización.

**Palabras clave:** gestión de seguridad de la información, herramientas tecnológicas, control, usuario, sistema de información.

cal tools used in SMEs with the intention of improving the internal control system and its performance effect, lower operational costs and (IS) performance in the organization.

**Keywords:** security management information technology tools, control, user information system.

# Introducción

En la pyme, el manejo de la información y la creación de políticas rigurosas de accesibilidad al sistema ha sido un tema crítico empresarial (Sindhuja, 2014). Lo es también la gestión de la seguridad en la información, las soluciones tecnológicas y su articulación con la participación del usuario (Herath y Rao, 2009). Por tanto, es necesario que la pyme desarrolle herramientas eficaces para la evaluación del riesgos (Lupu, Neagu y Minea, 2013) y cuente con una estructura congruente entre la dirección organizacional, el sistema, el usuario y la tecnología (Gheorghe, 2010), aspectos que deben agregar valor a la seguridad de la información y a reducir los riesgos informáticos. Reducir los riesgos del sistema de información (SI) en la pyme requerirá recursos tecnológicos y un modelo de gestión que logre integar el SI y la tecnología (Kumar, 2010), de tal manera que la empresa pueda prevenir, evitar, detectar o eliminar las amenazas al SI (Lupu, Neagu y Minea, 2013).

En otros aspectos del entorno, el crecimiento del comercio electrónico, los cambios impulsados por la globalización y la regulación para la seguridad de la información demandan de la pyme perfeccionar la manera de administrar los recursos de información empresarial (Gupta y Hammond, 2005). Los gerentes requieren un conocimiento amplio en seguridad de la información para garantizar la toma de decisiones sobre sistema y tecnologías de la información (Gheorghe, 2010; Parsons et al., 2014), más aún cuando el mismo usuario del SI puede poner en riesgo la organización inadvertida o deliberadamente al divulgar contraseñas o ser víctima de software malicioso o malitencionado (malware o phishing, etc.) (Parsons et al., 2014).

La presente investigación parte de los estudios realizados por Spears y Barki (2010), Spears (2007), quienes han establecido que la contribución del usuario mejora el desempeño del control e incrementa la seguridad informática. Mejorar el desempeño del control y garantizar la seguridad de la información es un aspecto relevante en las organizaciones (Spears y Barki, 2010) y dependerán de las diversas actividades de apoyo de la dirección de la empresa y de su desarrollo tecnológico (Barki y Hartwick, 2001). Otros estudios han establecido la vulnerabilidad de las empresas a los delitos informáticos, dada la carencia de recursos financieros y de la inexperiencia de la empresa para desarrollar procesos de gestión de la seguridad en la información (Gupta y Hammond, 2005).

Por tanto, la pyme debe trabajar sus limitaciones en la implementación de políticas de seguridad y determinar su relevancia sobre seguridad de tecnologías de información (TI) (Werlinger, Hawkey y Beznosov, 2009). En este proceso, los usuarios y expertos del SI tienen un papel importante en el desempeño del control (Baroudi, Olson y Ives, 1986). El usuario se ha convertido en un factor fundamental en los proyectos tecnológicos, con el fin de proyectar mejoras en el SI (DeLone y McLean, 2003), y desde una mirada organizacional, en la manera de revelar los datos y salvaguardar la información (Markus y Mao, 2004).

El objetivo de este trabajo es de tipo correlacional con enfoque cuantitativo, ya que tiene como propósito determinar empíricamente el grado de influencia que hay entre las variables gestión de la seguridad (participación del usuario y factores tecnológicos) y gestión organizativa (planificación del SI y dirección organizacional) con el desempeño del control en el SI. Las fuentes de información utilizadas fueron primarias. Por ello, la pregunta de investigación que se trata de responder es la siguiente: ¿el desempeño del control del Sí está influenciado

por la participación del usuario final y por los procesos y la gestión administrativa de la empresa? Para responder a la pregunta de investigación, se ha desarrollado un estudio empírico, recogida de datos con una encuesta a 107 directivos y usuarios de las pymes, con la proposición de cuatro hipótesis que serán testadas mediante regresiones lineales, que permiten estadísticamente inferir algunos aspectos relacionados con este tipo de organizaciones. Esta investigación contribuye a la literatura sobre la seguridad de la información, al comprobar la importancia de la participación del usuario final y de la dirección organizacional en el diseño de sistemas de control, a fin de minimizar los riesgos informáticos de la pyme colombiana.

La estructura del trabajo se divide en cuatro partes: la primera comprende el marco teórico con una revisión de la literatura sobre la seguridad de la información, la participación del usuario del Sí, la influencia de la gestión administrativa, su efecto en el desempeño del control y el planteamiento de las hipótesis; la segunda corresponde a la descripción de la metodología utilizada, donde se describe la muestra y se justifican las variables; la tercera se ha destinado al análisis de los resultados; y la última contiene las principales conclusiones obtenidas, que describen las limitaciones y las futuras líneas de investigación.

## Marco teórico y estudios empíricos

### La seguridad de la información y los factores tecnológicos como mecanismos de control

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad (Ramírez, 2012). Por esta razón, la gestión de seguridad de la información se convierte en una tarea importante y primordial para las empresas (Nazareth y Choi, 2015; Sindhuja, 2014). Labor que debe ser complementada con modelos de control y estrategia tecnológicas de TI (Gheorghe, 2010). Por consiguiente, la pyme debe garantizar una estrategia de control, siguiendo técnicas de modelos que tengan las mejores prácticas de estándares, como COSO, COBIT, ITIL, ISO 27001, 27002 e ISO 38500, entre otros. Un estándar contribuye a advertir las amenazas y los riesgos de la empresa en el SI y a promover una cultura de control y de seguridad en la información (Markelj y Bernik, 2012).

La seguridad de la información no es solo cuestión de tener nombres de usuarios y contraseñas (Von Solms y Von Solms, 2004), sino que requiere de reglamentos y diversas políticas de privacidad y protección de los datos (Susanto, Almunawar y Tuan, 2011). Además, debe apoyarse en los factores o las herramientas tecnológicas para documentar las evidencias o rastros de auditoría que dejan los delitos financieros e informáticos (Arellano y Castañeda, 2012), los cuales utilizan altos volúmenes de datos e información para evitar ser detectados (Kahan, 2006).

En un estudio empírico, Spears y Barki (2010) establecieron que el desempeño del control está asociado con la administración del riesgo del SI, el área financiera y la seguridad de la información. Por tanto, se debe estudiar un enfoque basado en el riesgo, dado que permite evaluar su efecto en el negocio (Borek, Parlikad, Woodall y Tomasella, 2014). Entretanto, la seguridad de la información en TI permite gestionar con eficacia los activos de información y

puede minimizar los riesgos que atenten contra el SI de la empresa (Broderick, 2006).

Considerando la base teórica y los estudios empíricos previos presentados, se plantea la siguiente hipótesis de investigación:

$H_1$: Las herramientas tecnológicas influyen positivamente en el desempeño del control informático de la pyme.

## El usuario final y el diseño de controles en el sistema de información.

El usuario contribuye al control a través del conjunto de actividades y tareas que desarrolla en el SI, además de participar en la evaluación del riesgo informático (Barki y Hartwick, 1994). Esa participación del usuario se convirtió en un factor importante en los proyectos tecnológicos de Sí (Spears y Barki, 2010). Asimismo, la pyme debe procurar fortalecer en el usuario una cultura de control que introduzca valores, como la confianza y la honradez (Spears, 2007), dado que desde la óptica de Chen, Dawn y Shaw (2008), el usuario puede ser el primer nivel de protección para salvaguardar la información.

Los gerentes y usuarios del SI orientarán el sistema de seguridad de la información con mecanismos de control a la medida de la empresa (Barki y Hartwick, 2001). Igualmente, deberán establecer un enfoque estructurado para la gestión de riesgos, basado en actividades integrales, con el fin de analizar los riesgos desde el nivel estratégico hasta el nivel táctico de la organización (Ross, 2008).

Los estudios empíricos han establecido que los usuarios del SI son el eslabón más débil dentro del sistema de seguridad informática (Crossler et al., 2013; Finne, 2000). Ellos inciden en la ocurrencia de errores y en el fraude electrónico (Kraemer y Carayon, 2007). Por eso, la educación y formación del usuario debe ser una prioridad para la empresa a definir mecanismos de seguridad y políticas para salvaguardar la información (Chi y Wanner, 2011; Markelj y Bernik, 2012). En una investigación sobre seguridad informática en las pymes de Singapur, Ban y Heng (1995) identifican algunos problemas que están relacionados con la sofisticación de la computadora, falta de recursos, técnicos especialistas y altos costos del *hardware* y *software* de oficina. Dificultades que unidas a la tecnología utilizada pueden influir en las expectativas de los usuarios finales (Shaw, Lee-Partidge y Ang, 2003) y crear factores de riesgo en la ejecución de los proyectos de TI (Boehm y Turner, 2005; Boehm, 1991).

Por lo anterior, considerando la base teórica y los estudios empíricos previos, se plantea la siguiente hipótesis de investigación:

$H_2$: La participación del usuario en el diseño y desarrollo de controles del SI influye positivamente en el desempeño del control informático de la pyme.

## La gestión organizativa del SI y su efecto en el desempeño del control

Gestionar la seguridad de la información requiere establecer políticas, medidas de control y de monitoreo al SI (Chang, 2013). Procesos que se deben articular a la gestión organizacional mediante actividades de planificación y dirección organizacional de la empresa (Barki y Hartwick, 1989). Las directivas de la empresa deberán centrar un

mayor esfuerzo en definir tareas que velen por la autoeficacia, el liderazgo y el apoyo a los procesos de gestión tecnológica (Petter, DeLone y McLean, 2013). La implementación de las políticas de seguridad informática deberá suponer la fijación de roles, la coordinación y revisión de procesos técnicos que ayuden a salvaguardar la información (ISO 27002). La ISO 27000 es una serie bien establecida de los estándares de seguridad de la información (Beckers, Schmidt, Küster y Faßbender, 2011)

Estos procesos integrados a las actividades de los usuarios finales del SI permiten lograr mayor efectividad en la implementación del SI y una mejora en el desempeño del control (Premkumar y King, 1992). En un estudio empírico, Kankanhalli, Teo, Tan y Wei (2003) encontraron que las empresas que brindan apoyo a las actividades de dirección y al desarrollo de los proyectos tecnológicos sus esfuerzos de prevención para minimizar el riesgo de los SI/TI son más efectivos. Por otro lado, si esos apoyos de la dirección organizacional son efectivos, los niveles de riesgos se minimizan en las inversiones de TI y en su entorno empresarial y tecnológico (Alter y Sherer, 2004). En otro estudio, se estableció que las empresas con mayor dedicación a la planificación del Sí mejoran el desempeño organizacional (Medina, García y De la Garza Ramos,, 2009). La planificación de TI como característica de los proyectos es un factor determinante para medir el efecto del SI (Petter et al., 2013) y el desempeño en el control (Byrd, Lewis y Bradley, 2006).

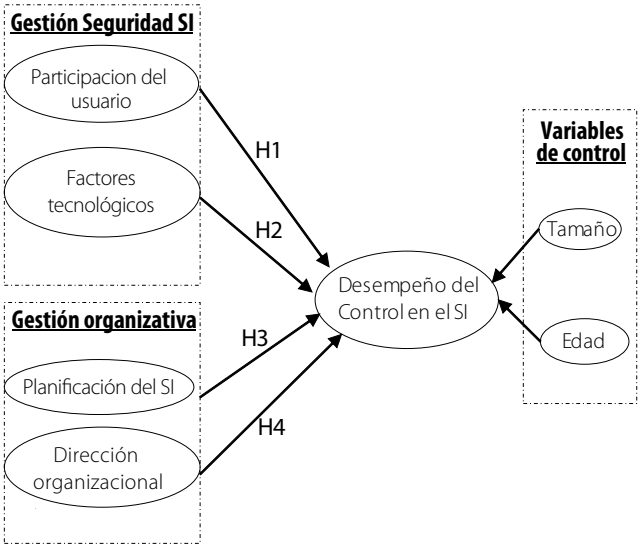
Considerando la base teórica y los estudios empíricos previos, se plantean las siguientes hipótesis de investigación:

$H_3$: La planificación del SI influye positivamente en el desempeño del control informático de la pyme.

$H_4$: La dirección organizacional influye positivamente en el desempeño del control informático de la pyme.

El modelo y las hipótesis se muestran en la figura 1.

**Figura No. 1.** Modelo teórico.



# Metodología

## Obtención de la muestra y recolección de datos

Las empresas objeto del estudio son pymes formalmente constituidas, pertenecientes a la industria, la construcción, el comercio y los servicios, y ubicadas Cali (Colombia). El tamaño muestral fue determinado para lograr que el margen de error máximo de 9.5 % para la estimación de una proporción de elementos (p = q) fuese inferior a 50 % con un nivel de confianza de 95 %. Se utilizó una muestra de 107 empresas. En la muestra se incluyen empresas denominadas pequeñas (58 %) y medianas (42 %) empresas (pymes).

Dentro de cada estrato la selección se hizo mediante un muestreo aleatorio simple. La recolección de los datos se realizó entre los meses de julio a septiembre de 2012, a través de una empresa de investigación de mercados contratada por la Universidad del Valle, dentro del proyecto de investigación denominado *Diseño de un modelo de control informático para las pymes en la ciudad de Cali*, que aparte de los riesgos y modelos informáticos, trató otras temáticas, como TIC y seguridad de la información, tecnología, calidad de la información y del uso de la información. El instrumento utilizado fue una encuesta estructurada, la cual se aplicó personalmente a los gerentes, jefes de sistemas de las empresas y usuarios del sistema de información. Para la elaboración del artículo, fue indispensable realizar los cálculos necesarios que armonizaron los pesos de la distribución en la encuesta con los reales en la población, mediante la respectiva ponderación.

## Medición de variables

*La participación del usuario final* se refiere a la intervención que tiene este en las fases de implementación del SI, el diseño y desarrollo de controles para mitigar los riesgos de seguridad al SI (Spears, 2007). Variables como el requerimiento de los usuarios, la planificación, el análisis, el diseño del SI y el control de los recursos son factores importantes de medición (Bowman, Davis y Wetherbe, 1983; King y Zmud, 1981). La participación del usuario en la implementación de la seguridad de la información y el diseño de los controles de seguridad son variables importantes (Spears y Barki, 2010). *Los factores tecnológicos* hacen referencia al efecto de la TI en la seguridad de la información. A menudo son indirectos y se ven influenciados por los factores de tipo organizacional (Petter et al., 2013). La tecnología requiere estar apoyada de prácticas de control y un mayor conocimiento de los empleados (Abu-Musa, 2006). *La planificación del SI* como característica de los proyectos de TI es un factor determinante para medir el SI (Petter et al., 2013). La planificación es importante en los requerimientos de los usuarios, el análisis y diseño de los SI y en el control de los recursos (Bowman et al., 1983; King y Zmud, 1981). Estas variables se muestran también en el estudio de Byrd et al. (2006). La planificación como herramienta de gestión debe contribuir al desarrollo de las tecnologías de la información y su alineación con las necesidades de la organización (King y Teo, 1996; Segars, Grover y Teng, 1998). También, facilita el éxito de los proyectos informáticos y mejora la calidad de los SI (Ginzberg, 1981; Grover y Lyytinen, 2015).

En cuanto a la *dirección organizacional*, centra su atención en la compatibilidad de tareas, la autoeficacia, el apoyo a los procesos de gestión (Petter et al., 2013). El apoyo a la dirección organizacional puede tener un efecto en el desempeño del control y en el éxito de la implementación del SI (Chatterjee, Grewal y Sambamurthy, 2002; Choe, 1996). Por otro lado, la variable independiente *desempeño del control* se refiere a la percepción de los usuarios con una mayor seguridad en el SI y mejores niveles de controles para mitigar los riesgos de seguridad al Sí (Spears y Barki, 2010). Las mediciones de los controles de seguridad fueron usadas por Spears y Barki (2010) y Spears (2007), quienes señalaron el grado de las deficiencias en el diseño, los errores en la ejecución del control y las eficiencias o mejoras del control al SI. Para Whitman y Mattord (2012), la planificación de la seguridad, la gestión de riesgos, la selección de la tecnología de seguridad, el monitoreo del desempeño y mantenimiento de los controles, entre otros, estarán a cargo de los directivos de seguridad. Con respecto a *las variables de control*, se consideraron dos que facilitarán el control de la información: tamaño y edad. Con respecto a la variable tamaño, esta se midió a través del número medio de empleados de 2012 en forma logarítmica. El número de empleados ha sido utilizado como medida de tamaño en este tipo de trabajos, entre otros: Bjørnenak (1997) y Merchant (1984). Sobre la variable edad, fue medida a través del número de años transcurridos desde la constitución o inicio de la actividad hasta 2012. Esta variable ha sido utilizada por Yasuda (2005) y Holmes y Nicholls (1989).

## El modelo

La ecuación 1 muestra el modelo teórico considerado para contrastar las hipótesis planteadas en este trabajo, donde $Y_i$ es la variable dependiente, que según el caso son participación del usuario, factores tecnológicos, planeación del SI, direccionamiento organizacional, y donde el desempeño del control SI es la variable independiente. Las variables de control son el tamaño y la edad de la pyme.

$$Y_i = b_0 + b_1 \text{Desempeño del Control SI}_i + b_2 \text{Tamaño}_i + b_3 \text{Edad}_i + £_i$$

## Fiabilidad y validez

En este apartado se describen las variables utilizadas y se analizan estadísticamente la robustez de los constructos, con el fin de dar validez a los resultados obtenidos. En la tabla 1 se observa la consistencia interna del constructo, con respecto a la fiabilidad del instrumento de medición se utilizó el Alfa de Cronbach. Además, se tomó la decisión de eliminar las cargas factoriales por debajo de 0.5. En este trabajo, se consideraron las siguientes variables de control: tamaño: medido a partir del número de empleados de la pyme; edad: se mide la variable continua número de años de funcionamiento de la empresa hasta la actualidad.

**Tabla No. 1.** Consistencia interna y validez de los constructos

| Variable | Indicador | Carga factorial | Alfa de Cronbach | Sig. Bartlett | KMO |
|---|---|---|---|---|---|
| Participación del usuario | Participación en la identificación del control del riesgo | 0.885 | 0.883 | 0.000 | 0.772 |
| | Participación en la seguridad del SI | 0.864 | | | |
| | Participación en proyectos tecnológicos | 0.889 | | | |
| | Participación en la ejecución de pruebas de control | 0.812 | | | |
| Factores tecnológicos | Desarrollo del software e interfaz del usuario | 0.809 | 0.708 | 0.000 | 0.637 |
| | Herramientas tecnológicas y de seguridad informática | 0.859 | | | |
| | Infraestructura tecnológica (redes-protocolos de seguridad) | 0.723 | | | |
| Planeación del SI | Control al SI | 0.738 | 0.694 | 0.000 | 0.791 |
| | Control de recursos del SI | 0.750 | | | |
| | Metodología de desarrollo | 0.746 | | | |
| | Estrategia SI/TI | 0.695 | | | |
| Dirección organizacional | Apoyo a la gestión tecnológica | 0.794 | 0.817 | 0.000 | 0.800 |
| | Apoyo y control a los procesos del SI | 0.758 | | | |
| | Apoyo a la estrategias SI | 0.848 | | | |
| | Atención a compatibilidad de tareas | 0.812 | | | |
| | Participación en proyectos tecnológicos | 0.889 | | | |
| Desempeño del control SI | Control y procedimentos de acceso al SI | 0.871 | 0.739 | 0.000 | 0.658 |
| | Segregación de funciones en el SI | 0.802 | | | |
| | Políticas de seguridad y de acceso al sistema | 0.780 | | | |

# Resultados y discusión

## Resultado descriptivo

A efectos de facilitar una mayor comprensión de los resultados, en la tabla 2 se muestran los descriptivos de las variables utilizadas en el estudio. Se puede observar que los ítems que obtienen una mayor valoración (en una escala de 1 a 5) por parte de las pymes colombianas de Cali estudiadas son "la participación en la seguridad del Sí" con una puntuación media de 4.45; la dirección organizacional apoya y controla los procesos tecnológicos, medidos por el "mejoramiento de los procesos" (4.45); la "estrategia de los SI/TI" (4.42) en la planeación del SI y la participación del usuario en proyectos tecnológicos (4.30). De forma contraria los menos valorados fueron los siguientes: la "metodología de desarrollo" (3.38); el "control de los recursos del SI" (3.56) y las "infraestructuras de TI" (3.61); y las habilidades de programadores y seguridad del SI (3.36).

**Tabla No. 2.** Descriptivo de las variables utilizadas

| Variable | Indicador | Cuestionario | Media | Desviación estándar | Min. | Máx. |
|---|---|---|---|---|---|---|
| Participación del usuario | Participación en la identificación del riesgo en el SI | Participa el usuario en identificar posibles riesgos en el ambiente informático | 4.29 | 0.765 | 1 | 5 |
| | Participación en la seguridad del SI | Se tienen en cuenta sus opiniones para el diseño del sistema de seguridad informático de la empresa | 4.45 | 0.717 | 1 | 5 |
| | Participación en proyectos tecnológicos | Se ha tenido en cuenta su participación como usuario del SI en el desarrollo de proyectos tecnológicos | 4.30 | 0.871 | 1 | 5 |
| | Participación en la ejecución de pruebas de control | Participa como usuario en las pruebas del nuevo sistema por implementar | 4.17 | 0.830 | 1 | 5 |
| Factores tecnológicos | Desarrollo del software y la interfaz del usuario | Considera que el desarrollo del proyecto de sistemas ha contribuido al desarrollo de la interfaz con las expectativas del usuario | 4.07 | 0.984 | 1 | 5 |
| | Habilidad de programadores y de seguridad del SI | La seguridad en el sistema es fiable y los programadores poseen habilidad en el manejo del software | 3.63 | 1.363 | 1 | 5 |
| | Infraestructura TI (redes-protocolos de seguridad) | La empresa tiene una infraestructura tecnológica para alcanzar los objetivos de la empresa | 3.61 | 1.203 | 1 | 5 |
| Planeación del SI | Control al SI | En la planeación de un proyecto SI, hay supervisión de los equipos y un adecuado control al SI | 30.90 | 1.027 | 1 | 5 |
| | Control de recursos del SI | Cree que la empresa planifica y ejerce control de los recursos que utilizan los usuarios del SI | 3.56 | 1.260 | 1 | 5 |
| | Metodología de desarrollo | Considera que hay metodología de desarrollo para la implementación del sistema de información | 3.38 | 1.24 | 1 | 5 |
| | Estrategia SI/TI | El SI es producto del análisis de proyectos tecnológicos a fin de apoyar las estrategias de la empresa | 4.42 | 0.630 | 2 | 5 |

| Variable | Indicador | Cuestionario | Media | Desviación estándar | Min. | Máx. |
|---|---|---|---|---|---|---|
| Dirección organizacional | Apoyo a la gestión tecnológica | Considera que la dirección de la empresa apoya la gestión en TIC con el fin de generar eficiencia y eficacia en el SI | 30.95 | 0.829 | 1 | 5 |
| | Apoyo y control a los procesos del SI | Cree que el apoyo administrativo TI contribuye al control de los procesos de los proyectos tecnológicos | 4.45 | 0.717 | 1 | 5 |
| | Apoyo a la estrategias SI | La dirección lidera acciones para apoyar los planes y objetivos del giro tecnológico de la empresa | 4.17 | 0.830 | 1 | 5 |
| | Atención a compactibilidad de tareas | La dirección organizacional presta atención y apoyo a las actividades (tareas) de los usuarios durante el ciclo del nuevo SI | 4.21 | 0.774 | 1 | 5 |
| Desempeño del control SI | Control y procedimientos de acceso al SI | El usuario en general se encuentra satisfecho con el sistema, percibe un adecuado control | 4.21 | 0.774 | 1 | 5 |
| | Segregación de funciones en el SI | Considera alta la concentración de las funciones en el SI | 30.90 | 1.027 | 1 | 5 |
| | Políticas de seguridad y de acceso al sistema | Las políticas y normas implementadas mejoran el desempeño del sistema y de los usuarios | 4.40 | 0.889 | 1 | 5 |

En la tabla 3, se describen las frecuencias de las variables relacionadas con la seguridad informática utilizadas en la encuesta.

**Tabla No. 3.** Descriptivo de frecuencias-preguntas relacionadas con la seguridad de la Información

| N.º pregunta | Pregunta del cuestionario | Frecuencia | % | % válido | % acumulado |
|---|---|---|---|---|---|
| 1 | **Los empleados de la empresa son capacitados en seguridad informática** | | | | |
| | Sí | 50.0 | 460.7 | 460.7 | 460.7 |
| | No | 56.0 | 52.3 | 52.3 | 99.1 |
| | No sabe | 1.0 | 00.9 | 00.9 | 100.0 |
| | **Total** | **107** | **100** | **100** | |

| N.º pregunta | Pregunta del cuestionario | Frecuencia | % | % válido | % acumulado |
|---|---|---|---|---|---|
| 2 | **Mencione los incidentes de seguridad informática que ha tenido la empresa** | | | | |
| | Infecciones informática | 30.0 | 28.0 | 28.0 | 28.0 |
| | Robo de datos | 59.0 | 55.1 | 55.1 | 83.2 |
| | Pérdida de información accidental | 1.0 | 00.9 | 00.9 | 84.1 |
| | No sabe | 16.0 | 15.0 | 15.0 | 99.1 |
| | **Total** | **107** | **1** | **0** | **0** |
| 3 | **Quién es notificado en caso de incidentes de seguridad** | | | | |
| | No hay una política definida a quién reportar | 7.0 | 6.5 | 6.5 | 6.5 |
| | Jefe de área o departamento | 46.0 | 43.0 | 43.0 | 49.5 |
| | Jefe de sistemas | 29.0 | 27.1 | 27.1 | 760.6 |
| | Gerente | 17.0 | 150.9 | 150.9 | 92.5 |
| | Equipo de atención de incidentes | 1.0 | 00.9 | 00.9 | 93.5 |
| | Empresa o persona que presta el servicio de outsourcing | 4.0 | 30.7 | 30.7 | 97.2 |
| | Otro | 3.0 | 20.8 | 20.8 | 100.0 |
| | **Total** | **107** | **100** | **100** | |
| 4 | **Cuál es fuente generadora de riesgo** | | | | |
| | Interna | 64.0 | 590.8 | 590.8 | 590.8 |
| | Externa | 40.0 | 37.4 | 37.4 | 97.2 |
| | Ninguna | 1.0 | 00.9 | 00.9 | 98.1 |
| | No sabe | 2.0 | 10.9 | 10.9 | 100.0 |
| | **Total** | **107** | **100** | **100** | |
| 5 | **Metodologías o modelos de gestión implementados en la empresa** | | | | |
| | ITIL | 4.0 | 30.7 | 30.7 | 30.7 |
| | COBIT | 3.0 | 20.8 | 20.8 | 6.5 |
| | Ninguno | 86.0 | 80.4 | 80.4 | 860.9 |
| | No sabe | 14.0 | 13.1 | 13.1 | 100.0 |
| | Total | 107 | 100 | 100 | |
| 6 | **Principales obstáculos para el desarrollo de la seguridad informática** | | | | |
| | Falta de apoyo directivo | 10.0 | 9.3 | 9.3 | 9.3 |
| | Falta de personal calificado | 5.0 | 4.7 | 4.7 | 14.0 |
| | Falta de recursos económicos | 20.0 | 180.7 | 180.7 | 320.7 |
| | Desconocimiento sobre seguridad informática | 27.0 | 25,2 | 25,2 | 570.9 |
| | Falta de colaboración entre las áreas | 5.0 | 4.7 | 4.7 | 620.6 |
| | Otros | 3.0 | 20.8 | 20.8 | 65,4 |
| | No tiene | 27.0 | 25,2 | 25,2 | 900.7 |
| | No sabe | 10.0 | 9.3 | 9.3 | 100.0 |
| | **Total** | **107** | **100** | **100** | |

Se puede observar que 52.3 **%** de los encuestados no son capacitados en seguridad informática; la mayor incidencia de seguridad informática ha sido el robo de datos (55.1 **%**) seguido de las infecciones por virus informático (28 **%**); la mayor fuente generadora de riesgo es de tipo interno (590.8 **%**), es decir, concebida por los mismos empleados; los principales obstáculos para el desarrollo de una efectiva seguridad informática es el desconocimiento y la falta de recursos en la pyme. Finalmente, las empresas han implementado o adoptado los siguientes modelos de control informático: ITIL (30.7 **%**), COBIT (20.8 **%**) y de los encuestados 80.4 **%** respondi**ó** que no han adoptado o implementado ningún modelo de control. No obstante, en el análisis del estudio empírico, se logra establecer que hay conciencia de la necesidad de salvaguardar la información y de la participación de los usuarios de la gestión en la seguridad del riesgo informático. Igualmente, consideran el principal obstáculo para el desarrollo de la seguridad de la información el desconocimiento del tema y la falta de recursos económicos para su inversión.

**Tabla No. 4.** Factores de efecto de las variables en la gestión de la seguridad y organizacional en el desempeño del control al SI

| | **Gestión seguridad de la informacón** | | **Gestión organizacional** | |
|---|---|---|---|---|
| | **Participación del usuario** | **Factor tecnológico** | **Planeación del SI** | **Dirección organizacional** |
| **Desempeño del control SI** | 00.740*** (11.141) | 0.477*** (50.777) | 00.635*** (8.542) | 00.850*** (16.557) |
| **Tamaño** | –0.090 (–1.365) | 0.276** (3.336) | 0.139* (10.876) | –0.062 (–1.207) |
| **Edad** | -0.068 (–1.023) | –0.057 (–00.692) | 0.174* (2.334) | –0.082 (–1594) |
| **VIF más alto** | 1.011 | 1.008 | 1.008 | 1.011 |
| **F** | 420.781 | 150.819 | 27.325 | 94.310 |
| **$R^2$ ajustado** | 0.547 | 0.301 | 0.434 | 00.729 |

Junto a cada coeficiente estandarizado, entre paréntesis, valor del estadístico t-student.
* $p \leq 0.1$; ** $p \leq 0.05$; *** $p \leq 0.01$

Para verificar las hipótesis planteadas en el trabajo de investigación empírico, se diseñaron modelos básicos de regresión, a fin de cuantificar la relación existente entre las variables analizadas. Las estimaciones se realizan a partir de regresiones lineales multivariantes por mínimos cuadrados ordinarios (MCO). Inicialmente se comprueba el factor de inflación de la varianza (VIF), a fin de descartar presencia de multicolinealidad (Diamantopoulos y Siguaw, 2006; Diamantopoulos y Winklhofer, 2001). En la tabla 3, se observan los resultados de las estimaciones realizadas del modelo, donde se examinan las relaciones entre las variables dependientes (participación del usuario, factores tecnológicos, planeación del SI, dirección organizacional) y la variable independiente: desempeño del control SI.

A continuación, se describen con mayor detalle los resultados por tipo de variable observada.

## Modelo 1: Medición de la participación del usuario

Participación del usuario$_i$ = $\beta_0$+$\beta_1$ x desempeño del control SI + $\beta_2$ x tamaño$_i$ + $\beta$3 edad$_i$ + £$_i$

La regresión (participación del usuario) muestra como resultado un coeficiente positivo y estadísticamente significativo para la variable desempeño del control SI (00.740; p ≤ 0.01). Esto indica que la pyme que logra que el usuario final participe en el diseño de requerimientos y propuesta de controles al SI se garantiza un mejor desempeño del control. Se corrobora la hipótesis $H_1$ y se confirma los resultados de Kankanhalli et al. (2003). Además, se comprueba la validez global del modelo, ya que la F tuvo un valor de 420.781 (p ≤ 0.01). Los usuarios del SI son un recurso importante para la empresa, dado que contribuye a la seguridad del SI, proporciona medidas y el conocimiento necesario para la protección de la información y de los procesos sensibles del negocio (Spears y Barki, 2010), aspectos que se deben dar en la fase de planeación del SI y su implementación.

## Modelo 2: Medición del factor tecnológico

Factor tecnológico$_i$ = $\beta_0$+$\beta_1$ x desempeño del control SI + $\beta_2$ x tamaño$_i$ + $\beta_3$ edad$_i$ + £$_i$

En la regresión (factor tecnológico) se aprecia un coeficiente positivo y estadísticamente significativo con el desempeño del control SI (0.477***). Por tanto, se acepta la hipótesis $H_2$. Es decir, las pymes que se preocupan más por tener herramientas tecnológicas tienen un efecto positivo mayor en el desempeño del control al SI. También se desprende de este análisis que un buen sistema de seguridad informático requiere una mezcla de tecnología, políticas y procedimientos (Gupta y Hammond, 2005).

## Modelo 3: Medición de la planeación del SI

Planeación del SI$_i$ = $\beta_0$+$\beta_1$ x desempeño del control SI + $\beta_2$ x tamaño$_i$ + $\beta_3$ edad$_i$ + £$_i$

En la regresión (Planeación del SI) se aprecia un coeficiente positivo y estadísticamente significativo con el desempeño del control SI (00.635***). Por tanto, se acepta la hipótesis $H_3$. Es decir, las pymes que utilizan como herramienta de gestión la planeación contribuye al desempeño del sistema y mejoramiento de los controles. Las pymes deberán tener presente que no pueden ser tan dependientes de los SI y de la seguridad del sistema con el fin de lograr ventajas estratégica (Mithas, Ramasubbu y Sambamurthy, 2011; Mithas, Tafti, Bardhan, & Goh, 2012). Además, la pyme deberá adelantar estudios que le ayuden a establecer esos mecanismos de planeación estratégica del SI, con el fin de mejorar el desempeño organizacional y de control (Gupta y Hammond, 2005).

## Modelo 4: Medición de la dirección organizacional

Dirección organizacional$_i$ = $\beta_0$+$\beta_1$ x desempeño del control SI + $\beta_2$ x tamaño$_i$ + $\beta_3$ edad$_i$ + £$_i$

Para esta relación (Dirección organizacional), se encuentra un estadístico positivo y altamente significativo (00.850; p ≤ 0.01), lo cual indica que un buen acompañamiento de las directivas contribuye a que la pyme

esté satisfecha con el cumplimiento de los objetivos de control que se adopten en el SI. Estos resultados permiten aceptar la cuarta hipótesis ($H_4$) planteada. Las pymes que cuentan con un mayor apoyo por parte de la dirección de la empresa obtienen una mayor desempeño en el SI (Petter, DeLone y McLean, 2008). La dirección de la empresa debe dar a conocer a los usuarios las políticas y los procedimientos para contribuir a una mayor seguridad de la información y evitar cierta aversión al riesgo (Parsons et al., 2014). Minimizar los riesgos del SI implica seguimiento, análisis de informes y rendición de cuenta como mecanismos de control (Gheorghe, 2010, 2011).

Al analizar de manera general los resultados del modelo planteado, es necesario resaltar que, si bien se observa la influencia positiva y altamente significativa del desempeño del control en cada una de las variables de gestión de seguridad en la información y organizacional, se debe ser prudente al extrapolar los resultados de la presente investigación, ya que los R2 ajustados no son tan representativos en las variables factor tecnológicos (0.301) y planeación del SI (0.434). No obstante, para las variables "participación del usuario" (0.547) y "dirección organizacional" (00.729), los resultados significan que un alto porcentaje de estas dos variables son explicadas por el modelo.

De igual manera es importante señalar que, en el caso del tamaño de la pyme, se encontró un efecto significativo sobre los factores tecnológicos y la planificación del SI, en relación con la edad se refleja una influencia significativa en la planeación del SI y negativa en las variables "participación del usuario", "factor tecnológico" y en la "dirección organizacional", lo cual podría indicar que, a mayor antigüedad de la empresa, mayor es el riesgo informático.

# Conclusiones

El objetivo de este trabajo fue determinar el grado de la influencia que hay entre las variables de gestión de la seguridad (participación del usuario y factores tecnológicos), la gestión organizativa (planificación del SI y dirección organizacional) y el desempeño del control en el SI, con el fin de prevenir los delitos y riesgos informáticos en la pyme colombiana. En este sentido, los principales aportes del trabajo son las siguientes:1) Las directivas de las pymes de Cali (Colombia) son conscientes de la importancia que tiene el usuario en el diseño y desarrollo de controles informáticos. 2) Es trascendental que los usuarios participen en el diseño de ciertos controles de seguridad. Los usuarios solo pueden participar en los frentes de su competencia: la seguridad a nivel de máquina, a nivel de programa fuente, a nivel de modelo de datos e incluso a nivel de parametrización puede no ser accesible a un usuario "final". 3) La pyme para contrarrestar el riesgo informático deberá tomar acciones que lleven a su mitigación, bien adoptando modelos de control existentes, bien aprovechando herramientas tecnológicas existentes. 4) Los factores y las herramientas tecnológicas influyen de manera significativa en el desempeño del control y de la organización. 5) En el estudio empírico, ni el tamaño ni la edad de la empresa aparecen como factores que inciden en la eficiencia y eficacia sobre el desempeño de los controles en la organización.

En general, las pymes tienen las mismas oportunidades de beneficiarse de las herramientas tecnológicas y de los estándares de controles establecidos, como COBIT, las ISO y los factores, que garantizan la seguridad de la información, como los definidos en la norma ISO27001 y las prácticas de seguridad en la norma ISO27002. Además,

en un plano ideal, la infraestructura tecnológica debería apoyar la estrategia de los negocios y de los SI de la empresa, dado que las nuevas tecnologías de información tienen un potente efecto en la estrategia del negocio y en los servicios que se pueden ofrecer a la pyme (Gable, Sedera y Chan, 2003; Stratman y Roth, 2002).

Los resultados obtenidos permiten inferir que el apoyo de la dirección de la empresa en la implementación del sistema mejora el control y la calidad del SI (Solano Rodríguez, García Pérez de Lema y Bernal, 2014). Además, sus indicadores de productividad, toma de decisiones y costos se verán afectados positivamente en el rendimiento de la organización (DeLone y McLean, 2003; Gable, Sedera y Chan, 2003) y el desempeño del control. También se concluye que las pymes que invierten en tecnología y tienen una mayor infraestructura tecnológica con metodologías de desarrollo de proyectos mejoran los resultados de información (Karat y Karat, 2003), optimizan el monitoreo y controlan el nivel de riesgo tecnológico a través de su infraestructura tecnológica (*hardware*, *software*) y aquellos factores que corresponden al factor humano. Riesgo tecnológico que se puede originar producto del continuo incremento de herramientas y de aplicaciones tecnológicas que no cuentan con una gestión adecuada (Ramírez, 2012).

El control de la seguridad de la información es una cualidad altamente técnica y ciertos mecanismos de seguridad no suelen ser interpretables por los usuarios (Ray, Ow y Kim, 2011), dado que las herramientas para la evaluación de riesgos informáticos son altamente sofisticados (Lupu, Neagu y Minea, 2013). La pyme necesita desarrollar la configuración de la privacidad y políticas relacionadas con el uso del sistema, como contraseñas, seguridad de datos, parches de *software* y actualizaciones, etc. (Chi y Wanner, 2011). Una política de uso aceptable de calidad tiene que establecer claramente las consecuencias de no seguir la política de seguridad de la organización (Xu, 2011).

Los estudios futuros deberían estudiar el diseño de un instrumento de control al SI, considerando la diversidad de la empresa, el sector, el tamaño y las necesidades de las pymes. Estas empresas necesitan soluciones de seguridad ajustadas al tipo de organización, factores tecnológicos y regulación del país (He, 2013). Asimismo, es importante reflexionar sobre el tipo de actividad comercial, tamaño y antigüedad de la pyme, ya que pueden ser usados para definir modelos empíricos que aporten un nuevo enfoque de control informático. Además de estudiar cómo aumentar la conciencia de los empleados para que la empresa adopte un marco de seguridad que supervise de forma proactiva y preventiva los posibles ataques y amenazas informáticas.

Finalmente, este no es un estudio concluido, si bien la evaluación de la participación del usuario y de la dirección de la empresa en la gestión de la seguridad de la información se ha venido estudiando de manera sistemática como un tema clave (Thatcher y Oliver, 2001), hay poco consenso entre investigadores sobre la mejor manera de medir el efecto de la seguridad de información en la pyme, por tanto, esta investigación es un proceso que se orientará a identificar cómo los factores de implementación y de desempeño del control pueden afectar el desarrollo de las organizaciones, aun cuando en la pyme el crecimiento de las aplicaciones de *e-business* y *e-commerce* también presentan abundantes oportunidades para el acceso no autorizado al SI (Brooks, Riley Jr y Thomas, 2005).

## Agradecimientos

Los autores agradecen el apoyo institucional a la Universidad del Valle y la Universidad Politécnica de Cartagena (España). Especialmente a la primera por la financiación del proyecto de onvestigación N.º CI8095.

## Referencias

Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information Systems*, *20*(1), 187-203.

Alter, S. y Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems*, *14*(1), 1-30.

Arellano, L. E. y Castañeda, C. M. (2012). La cadena de custodia informático-forense. *Cuaderno Activa*, *3*(3), 67-81.

Ban, L. Y. y Heng, G. M. (1995). Computer security issues in small and medium-sized enterprises. *Singapore Management Review*, *17*(1), 15-29.

Barki, H. y Hartwick, J. (1989). Rethinking the concept of user involvement. *MIS Quarterly*, 13(1), 53-63.

Barki, H. y Hartwick, J. (1994). Measuring user participation, user involvement, and user attitude. *MIS Quarterly*, *18*(1), 59-82.

Barki, H. y Hartwick, J. (2001). Interpersonal conflict and its management in information system development. *MIS Quarterly*, *25*(2), 195-228.

Baroudi, J. J., Olson, M. H. y Ives, B. (1986). An empirical study of the impact of user involvement on system usage and information satisfaction. *Communications of the ACM*, *29*(3), 232-238.

Beckers, K., Schmidt, H., Kuster, J. C. y Faßbender, S. (2011). *Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing*. Ponencia presentada en la Availability, Reliability and Security (ARES), 2011 Sixth International Conference on.

Bjørnenak, T. (1997). Diffusion and accounting: The case of ABC in Norway. *Management Accounting Research*, *8*(1), 3-17.

Boehm, B. (1991). Software risk management: principles and practices. *IEEE Software*, *8*(1), 32-41.

Boehm, B. y Turner, R. (2005). Management challenges to implementing agile processes in traditional development organizations. *IEEE Software*, *22*(5), 30-39.

Borek, A., Parlikad, A. K., Woodall, P. y Tomasella, M. (2014). A risk based model for quantifying the impact of information quality. *Computers in Industry*, *65*(2), 354-366.

Bowman, B., Davis, G. y Wetherbe, J. (1983). Three stage model of MIS planning. *Information & Management*, *6*(1), 11-25.

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26-31.

Brooks, R. C., Riley Jr, R. A. y Thomas, J. (2005). Detecting and preventing the financing of terrorist activities: A role for government accountants. *The Journal of Government Financial Management*, *54*(1), 12-18.

Byrd, T. A., Lewis, B. R. y Bradley, R. V. (2006). IS infrastructure: The influence of senior IT leadership and strategic information systems planning. *Journal of Computer Information Systems*, *47*(1), 101-113.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. y Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

Chang, H. (2013). Is ISMS for financial organizations effective on their business? *Mathematical and Computer Modelling*, *58*(1), 79-84.

Chatterjee, D., Grewal, R. y Sambamurthy, V. (2002). Shaping up for e-commerce: institutional enablers of the organizational assimilation of web technologies. Mis Quarterly, 26(2), 65-89.

Chen, C. C., Dawn Medlin, B. y Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), 360-376.

Chi, M. y Wanner, R. (2011). Security policy and social media use. Recuperado de http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749

Choe, J. M. (1996). The relationships among performance of accounting information systems, influence factors, and evolution level of information systems. Journal of Management Information Systems, 12(4), 215-239.

Delone, W. H. y McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. Journal of Management Information Systems, 19(4), 9-30.

Diamantopoulos, A. y Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. British Journal of Management, 17(4), 263-282.

Diamantopoulos, A. y Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. Journal of Marketing Research, 38(2), 269-277.

Finne, T. (2000). Information systems risk management: Key concepts and business processes. Computers & Security, 19(3), 234-242.

Gable, G., Sedera, D. y Chan, T. (2003). Enterprise systems success: a measurement model. ICIS 2003 Proceedings. Paper 48. Recuperado de http://aisel.aisnet.org/icis2003/48/?utm_source = aisel.aisnet.org %2Ficis2003 %2F48&utm_medium = PDF&utm_campaign = PDFCoverPages

Gheorghe, M. (2010). Audit Methodology for IT Governance. Informatica Economica, 14(1), 32. -42.

Gheorghe, M. (2011). Risk Management in IT Governance Framework. *Economia. Seria Management*, *14*(2), 545-552.

Ginzberg, M. J. (1981). Key recurrent issues in the MIS implementation process. *MIS Quarterly*, *5*(2), 47-59.

Grover, V. y Lyytinen, K. (2015). New state of play in information systems research: The push to the edges. *MIS Quarterly*, *39*(2), 271-296.

Gupta, A. y Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297-310.

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, *21*(5), 381-400.

Herath, T. y Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Holmes, S. y Nicholls, D. (1989). Modelling the accounting information requirements of small businesses. *Accounting and Business Research*, *19*(74), 143-150.

Kahan, S. (2006). Sherlock Holmes enters accounting: Dramatic increase in fraud brings more CPA sleuths into the industry. *Accounting Today*, *20*(8).

Kankanhalli, A., Teo, H. H., Tan, B. C. y Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139-154.

Karat, J. y Karat, C. M. (2003). The evolution of user-centered focus in the human-computer interaction field. *IBM Systems Journal*, *42*(4), 532-541.

King, W. R. y Teo, T. S. (1996). Key dimensions of facilitators and inhibitors for the strategic use of information technology. Journal of Management Information Systems, 12(4), 35-53.

King, W. R. y Zmud, R. W. (1981). Managing information systems: Policy planning, strategic planning and operational planning. ICIS 1981 Proceedings. Paper 16. Recuperado de http://aisel.aisnet.org/icis1981/16/?utm_source = aisel.aisnet.org %2Ficis1981 %2F16&utm_medium = PDF&utm_campaign = PDFCoverPages

Kraemer, S. y Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2), 143-154.

Kumar, M. (2010). Risk management practices in global manufacturing investment (Tesis de doctorado, University of Cambridge, Cambridge, Reino Unido).

Lupu, M., Neagu, L. y Minea, V. (2013). Internal audit, risk detection tool for contemporary crisis. Internal Auditing & Risk Management, 8(2), 149-158.

Markelj, B. y Bernik, I. (2012). Mobile devices and corporate data security. International Journal of Education and Information Technologies, 6(1), 97-104.

Markus, M. L. y Mao, J. Y. (2004). Participation in development and implementation-updating an old, tired concept for today's IS contexts. Journal of the Association for Information Systems, 5(11-12), 14-544.

Medina Quintero, J. M., García Pedroche, E. y De la Garza Ramos, M. I. (2009). Influencia de los factores de implementación en la calidad de los sistemas de información para la satisfacción del usuario. Journal of Information Systems and Technology Management, 6(1), 25-44.

Merchant, K. A. (1984). Influences on departmental budgeting: An empirical examination of a contingency model. Accounting, Organizations and Society, 9(3), 291-307.

Mithas, S., Ramasubbu, N. y Sambamurthy, V. (2011). How information management capability influences firm performance. MIS Quarterly, 35(1), 237.

Mithas, S., Tafti, A. R., Bardhan, I. y Goh, J. M. (2012). Information technology and firm profitability: mechanisms and empirical evidence. MIS Quarterly, 36(1), 205-224.

Nazareth, D. L. y Choi, J. (2015). A system dynamics model for information security management. Information & Management, 52(1), 123-134.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. y Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

Petter, S., DeLone, W. y McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. European Journal Of Information Systems, 17(3), 236-263.

Petter, S., DeLone, W. y McLean, E. (2013). Information systems success: The quest for the independent variables. Journal of Management Information Systems, 29(4), 7-62.

Premkumar, G. y King, W. R. (1992). An empirical assessment of information systems planning and the role of information systems in organizations. Journal of Management Information Systems, 9(2), 99-125.

Ramírez, C. A. (2012). Riesgo tecnológico y su efecto para las organizaciones, parte I. Seguridad cultura de prevención para TI, 14. 12-17. Recuperado de http://revista.seguridad.unam.mx/sites/revista.seguridad.

unam.mx/files/revistas/pdf/SeguridadNum14.pdf

Ray, S., Ow, T. y Kim, S. S. (2011). Security assurance: How online service providers can influence security control perceptions and gain trust. Decision Sciences, 42(2), 391-412.

Ross, R. (2008). Managing risk from information systems: An organizational perspective. Gaithersberg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Segars, A. H., Grover, V. y Teng, J. T. (1998). Strategic information systems planning: Planning system dimensions, internal coalignment, and implications for planning effectiveness. Decision Sciences, 29(2), 303-341.

Shaw, N., Lee-Partidge, J.-E. y Ang, J. S. K. (2003). Understanding the hidden dissatisfaction of users toward end-user computing. Journal of End User Computing, 15(2), 1-22.

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance. Information Management & Computer Security, 22(5), 450-473.

Solano Rodríguez, O. J., García Pérez de Lema, D. y Bernal García, J. J. (2014). Influencia de la implementación del sistema de información sobre el rendimiento en pequeñas y medianas empresas: un estudio empírico en Colombia. Cuadernos de Administración, 30(52), 31-43.

Spears, J. L. (2007). End users' contribution to information security policy effectiveness. Ponencia presentada en la 6th Annual Security Conference, Las Vegas, NV. Recuperado de http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/17.pdf

Spears, J. L. y Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.

Stratman, J. K. y Roth, A. V. (2002). Enterprise resource planning (ERP) competence constructs: two-stage multi-item scale development and validation. Decision Sciences, 33(4), 601-628.

Susanto, H., Almunawar, M. N. y Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences, 11(5), 23-29.

Thatcher, M. E. y Oliver, J. R. (2001). The impact of technology investments on a firm's production efficiency, product quality, and productivity. Journal of Management Information Systems, 18(2), 17-45.

Von Solms, B. y Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Werlinger, R., Hawkey, K. y Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), 4-19.

Whitman, M. y Mattord, H. (2012). *Principles of information security*. Boston, USA: Cengage Learning.

Da Xu, L. (2011). Enterprise systems: state-of-the-art and future trends. *IEEE transactions on industrial informatics*, *7*(4), 630-640.

Yasuda, T. (2005). Firm growth, size, age and behavior in Japanese manufacturing. *Small Business Economics*, *24*(1), 1-15.