

# Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia)<sup>1</sup>

*Security of information systems in SMEs in Santiago de Cali (Colombia)*

*A segurança dos sistemas de informação nas PME em Santiago de Cali (Colômbia)*

**Sandra Cristina Riascos Erazo**

Doctorado en Ingeniería Informática. Docente, Facultad de Ciencias de la Administración, Universidad del Valle – Colombia.

sandra.riascos@correounivalle.edu.co

**Adriana Aguilera Castro**

Magíster en Ciencias de la Organización, Universidad del Valle – Colombia. Docente, Facultad de Ciencias de la Administración, Universidad del Valle – Colombia.

adriana.aguilera@correounivalle.edu.co

**Gloria Patricia Ávila Fajardo**

Magíster en Ciencias de la Organización, Universidad del Valle – Colombia. Profesora Asistente Universidad del Valle – Colombia

gloria.avila@correounivalle.edu.co

---

Fecha de recepción: Mayo 15 del 2014

Fecha de aceptación: Junio 10 del 2014

## Resumen

La estrategia de utilizar los Sistemas de información para generar oportunidades competitivas en las Pymes está bastante difundida en la actualidad; la estrategia requiere que las organizaciones implementen mecanismos de seguridad que permitan proteger la información como su principal activo. Este artículo tiene como objetivo principal analizar el nivel de seguridad de los sistemas de información en 96 Pymes de la ciudad de Santiago de Cali (Colombia). Para tal efecto se estimaron tres variables: Confiabilidad, Disponibilidad e Integridad, obteniéndose como principal resultado que las Pymes tienen un nivel medio de seguridad en sus sistemas de información, esto se ve reflejado en la favorabilidad de tener bases de datos integradas, políticas de seguridad, disponibilidad de la información y copias de seguridad de la información.

## Palabras clave

Sistemas de información, seguridad, Pymes

## Abstract

The strategy of using information systems to generate competitive opportunities in SMEs is quite widespread today; this strategy requires organizations to implement security

1. Este artículo es producto del proyecto de investigación CI 8096: *Aplicación del modelo de evaluación de la efectividad de las TIC en procesos organizacionales en las Pymes de Santiago de Cali – Colombia*. Financiado por la Universidad del Valle – Colombia, en la Convocatoria Interna 2010

*Cómo citar:* Riascos Erazo, Sandra Cristina; Aguilera Castro, Adriana; Ávila Fajardo, Gloria Patricia. (2014). Seguridad de los sistemas de información en las pymes de Santiago de Cali (Colombia). *Libre Empresa*. Enero - Junio, 107-118.

mechanisms designed to protect the information as the main asset of organizations. This article's main objective is to analyze the level of security you have information systems in 96 SMEs in the city Santiago de Cali (Colombia), for this purpose three variables were estimated: Reliability, Availability and Integrity, obtained as main result that SMEs have an average level of security in information systems, this reflected in favorability to have integrated databases, security policies, availability of information and backup information.

## Keywords

Information systems, security, SMEs

## Resumo

A estratégia de usar os sistemas de informação para gerar oportunidades de concorrência nas PME, é bastante difundida hoje; estratégia exige que as organizações implementem mecanismos de segurança destinadas a proteger as informações como o seu principal trunfo. O principal objetivo deste artigo é analisar o nível de segurança dos sistemas de informação em 96 PME, na cidade de Santiago de Cali (Colômbia). Confiabilidade, disponibilidade e integridade, obtendo como resultado principal que as PME têm um nível médio de segurança em sistemas de informação, o que se reflecte na favorabilidade das bases de dados tendo integrado, políticas de segurança: Para este fim três variáveis foram estimados , a disponibilidade de informações e cópias de segurança da informação.

## Palavras-chave

Sistemas de informação de segurança, as PME

## 1. Introducción y antecedentes teóricos

Es evidente que las organizaciones en la actualidad y en el futuro tienen un elemento importante que incluyen en el desarrollo de todas sus actividades empresariales, ese elemento, lo constituyen las Tecnologías de la Comunicación y la Información (en adelante TIC). El análisis estratégico de la utilización de los sistemas de información en beneficio de las organizaciones es fundamental para alcanzar un alto grado de eficacia de estas tecnologías en los procesos administrativos.

Las encuestas realizadas para recolectar la información necesaria para desarrollar a cabo la investigación de la que se deriva este artículo, permiten tener una visión amplia de la opinión de los ejecutores de proyectos de tecnología y de las personas encargadas de la gestión de los sistemas de información en las Pymes de Santiago de Cali (Colombia). Este artículo presenta los resultados y principales conclusiones de los indicadores que conforman la seguridad en los sistemas de información utilizados en las organizaciones objeto de estudio.

El artículo se estructura de la siguiente forma: primero un acercamiento teórico al concepto de sistemas de información y seguridad de los sistemas de información; luego se presentan la metodología; los resultados, y por último, las conclusiones.

### 1.1 Sistemas de información

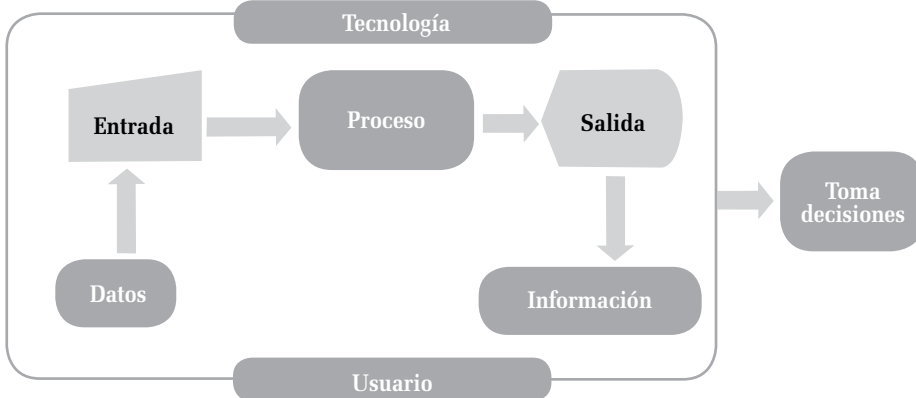
Antes de abordar los aspectos teóricos relacionados con los sistemas de información, es imprescindible hablar sobre la Teoría General de Sistemas, idea desarrollada por L. Von Bertalanffy en 1930, que sin lugar a dudas fundamenta aspectos clave en el desarrollo de las organizaciones y la administración. La Teoría General de Sistemas (TGS) se distingue por su perspectiva integradora, donde se considera importante la interacción y los conjuntos que brotan a partir de ella (Instituto Nacional de Estadística e Informática, 1994). Por ello, desde esta teoría se puede evidenciar un aporte importante al concepto y la visión de los sistemas de información.

Dichos sistemas se pueden definir como un conjunto de elementos interrelacionados (entre los que podemos considerar los distintos medios técnicos, las personas y los procedimientos) cuyo cometido es capturar datos, almacenarlos y transformarlos adecuadamente y distribuir la información obtenida mediante todo este proceso (Riascos, 2008).

El objetivo fundamental es apoyar y mejorar las operaciones normales de la empresa, así como satisfacer las necesidades de información para la resolución de problemas y la toma de decisiones por parte de la alta gerencia.

Los sistemas de información constituyen un conjunto de datos adquiridos en un proceso de entrada que son transformados en información y deben ser entregados a través de mecanismos de salida al usuario para su correspondiente toma de decisiones; la transformación de los datos en información requiere la utilización de la tecnología que permita que el proceso se realice de forma efectiva (Figura 1).

**Figura 1.** Sistema de información



**Fuente:** Riascos (2008)

Para Sieber, Valor y Porta (2006), la visión más intuitiva del SI de una empresa se obtiene simplemente observando cómo fluye la información dentro de la misma y entre ella y su entorno. Algunos flujos de información son claramente observables porque se corresponden con flujos físicos. Imaginemos, por ejemplo, el pedido de un cliente que llega a una empresa; alguien del departamento de ventas lo registra y envía una copia al almacén para que pueda ser servido (probablemente después de confirmar que el cliente en cuestión tenga crédito); en el almacén se comprueba que exista stock disponible y, en caso afirmativo, se asigna al

pedido, se adjunta el albarán correspondiente y se remite una copia a facturación, donde se prepara la factura de acuerdo con las condiciones pactadas con el cliente.

## 1.2 Estructura del sistema de información

Los sistemas de información requieren de una estructura funcional para lograr su objetivo, cada componente tiene una función específica que le permite interactuar con los demás componentes, diversos autores coinciden en los componentes básicos que debe tener un sistema de información; Whitten, Bentley y Barlow (2003) proponen un modelo basado en cinco bloques elementales para definir un sistema de información: personas, actividades, datos, redes y tecnología.

Bloque “Personas”: hace referencia a los propietarios del sistema (entendidos como tales aquellas personas que patrocinan y promueven el desarrollo de los sistemas de información), los usuarios (directivos ejecutivos, directivos medios, jefes de equipo, personal administrativo...), los diseñadores y los constructores.

Bloque “Datos”: se refiere a la “materia prima” empleada para crear información útil, se considera la mínima expresión de la información.

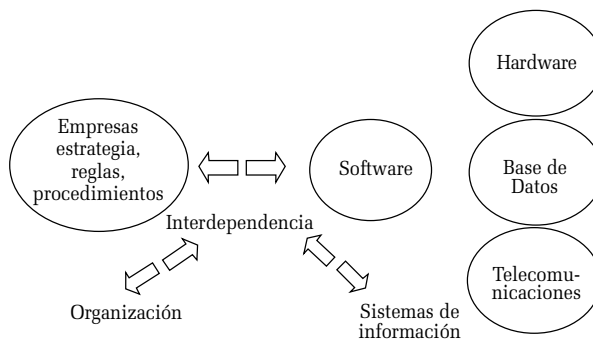
Bloque “Actividades”: se incluyen las actividades (procesos) que se llevan a cabo en la empresa y las gestiones de proceso de datos y generación de información que sirven de soporte a las primeras.

Bloque “Redes”: se analiza la descentralización de la empresa y la distribución de los restantes bloques elementales en los lugares más útiles (centros de producción, oficinas, delegaciones...), así como la comunicación y coordinación entre dichos lugares.

Bloque “Tecnología” hace referencia tanto al hardware como al software que sirven de apoyo a los restantes bloques integrantes del sistema de información.

La interrelación entre los componentes de un sistema de información permite a las organizaciones modernas mantener la sinergia de la información en función del propósito del sistema, lo cual se refleja en la disponibilidad oportuna, especialmente en los procesos que implican la toma de decisiones de la alta gerencia. En la Figura 2 se observa la articulación entre los componentes del sistema y los objetivos de la organización.

**Figura 2.** Interrelación entre los componentes del sistema de información



**Fuente:** Laudon y Laudon (1998)

### 1.3 Características de los sistemas de información

La importancia que tienen los sistemas de información en la organización implica que estos satisfagan algunas características importantes como por ejemplo:

**Calidad:** la norma ISO 9126 o series 25000, hace referencia al conjunto de propiedades y características de un producto o servicio que le permiten satisfacer necesidades establecidas o implícitas del usuario. La calidad se encuentra apoyada por la valoración de diferentes aspectos como: la funcionalidad, la fiabilidad, la usabilidad, la eficiencia, la mantenibilidad y la portabilidad.

**Funcionalidad:** hace referencia, según la norma ISO 9126 al conjunto de atributos referidos a la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son aquellas que ejecutan unos requerimientos o satisfacen unas necesidades implícitas; es decir, el cumplimiento de las funciones que requiere el usuario.

**Efectividad:** es la medida del impacto de la gestión, tanto en el logro de los resultados, como en el manejo de los recursos utilizados y disponibles (Vidal, 2004). Se puede decir que la efectividad es la suma entre los resultados obtenidos por la eficiencia y la eficacia de la tecnología informática y de la comunicación.

**Seguridad:** es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. El objetivo es proteger la misión de la organización, teniendo en cuenta las diferentes dimensiones de la seguridad.

**Integridad:** mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente el correcto desempeño de las funciones de una organización.

**Confidencialidad:** que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, que puede minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

**Eficacia:** Sieber, Valor y Porta (2006) comentan una serie de características que se deben cumplir para que un sistema de información sea eficaz:

- La estructura y funciones del sistema de información de una empresa deben ser coherentes con su estrategia en cada momento.
- La planificación y el diseño de un sistema de información deben servir a los objetivos estratégicos de la empresa, por lo que tienen que ser consensuados entre los expertos de sistemas de información y el resto de la organización.
- El sistema de información tiene que planificarse, diseñar e implantar de forma que guarde un equilibrio con el resto de sistemas integrantes de la infraestructura organizativa.

- El sistema de información debe gestionarse desde una perspectiva amplia, contando con la implicación y el compromiso de la alta dirección de la empresa.

#### 1.4 Seguridad de los sistemas de información

Hace referencia a un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas (Ramió, 2006); para la valoración de esta actividad se considerará la norma ISO 17799 (ISO, 2002) y autores como Castillo y otros (Castillo, Caldera, Losavio, & Matteo, 2006)

**Indicador de disponibilidad:** Hace referencia a salvaguardar los recursos necesarios y capacidades asociadas (COBIT 1998, 2001); además la disponibilidad es el grado en el cual las TIC permanecen operables sin la presencia de fallos, y por tanto se relaciona con los procesos no interrumpidos del procesamiento de información (Rakiting, 1997); (Lodensteijn, 2000). Según Galin (2004) las métricas de este indicador distinguen tres aspectos principales: disponibilidad total, disponibilidad vital e indisponibilidad total.

**Indicador de confiabilidad:** Se refiere a la provisión de información apropiada para los procesos administrativos, con el fin de operar la entidad en perfecto estado. Así mismo, como la protección de información sensible contra divulgaciones no autorizadas (COBIT, 1998, 2001). También se puede definir como el conjunto de atributos que respaldan la capacidad del software para mantener un desempeño en ciertas condiciones y en un período (ISO 9126).

**Indicador de integridad:** Es un aspecto que complementa la confiabilidad de las TIC. Ribagorda (1997) comenta que el mantenimiento de la integridad, junto con el de la confidencialidad y la disponibilidad, constituye el objetivo de la seguridad de la información. El COBIT (1998, 2001) define integridad como la precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio. En general, González (2001) señala que la integridad se refiere a los resultados fiables, completos, puntuales y exactos de las aplicaciones.

## 2. Metodología

Las Pymes registradas ante la Cámara de Comercio de Santiago de Cali – Colombia, a noviembre de 2011 son 7.376, de ese total el 80% corresponde a empresas pequeñas y el 20% a empresas medianas. Según el método de Muestreo Aleatorio Estratificado con un nivel de confianza del 95%, un margen de error del 10%, una proporción del 50%, se obtuvo que el tamaño adecuado de la muestra para la investigación en las Pymes de Santiago de Cali era de 96 empresas, de las cuales en correspondencia con la información anterior se debían estudiar 77 pequeñas y 19 medianas.

Con el objeto de evitar pérdida en el nivel de confianza por errores al recolectar la información, o por información no suministrada, se consideró una proporción esperada de pérdida de datos del 10%, lo que dio como resultado un tamaño de muestra de 106 empresas, repartidas en 85 empresas pequeñas y 21 empresas medianas. Dadas las dificultades propias en la recolección de información en un proyecto de investigación, la muestra real quedó distribuida en 76 empresas pequeñas y 30 empresas medianas, lo que no afecta el nivel de confianza propuesto.

Las técnicas utilizadas para la recolección de la información en las organizaciones objeto de estudio fueron las entrevistas y las encuestas aplicadas al personal administrativo y de soporte tecnológico.

Dentro de la investigación se estableció una metodología fundamentada en las siguientes cuatro fases:

<b>Fase I</b>	<b>Contextualización</b> , relacionado con el reconocimiento del entorno tanto interno como externo de la organización que permita establecer las condiciones sobre las cuales se plantea el contexto tecnológico. <b>Planeación</b> , un procedimiento donde se deben definir puntualmente los objetivos, el alcance de la evaluación, las actividades y recursos necesarios para ejecutar la evaluación propuesta.
<b>Fase II</b>	Dentro del proceso de evaluación es importante obtener la mayor cantidad de información posible, que permita efectuar un análisis objetivo de la situación a evaluar y por tanto, establecer unos juicios de valor coherentes con la realidad evidenciada
<b>Fase III</b>	Después de tener la información necesaria se efectúa el análisis pertinente, de acuerdo con los parámetros de evaluación definidos en el modelo de Riascos (2008); para esta actividad fue necesario utilizar software de análisis como Statistical Package for the Social Sciences (SPSS).
<b>Fase IV</b>	Conclusiones alrededor del tema de la evaluación de la seguridad de los sistemas de información en las Pymes de Santiago de Cali – Colombia.

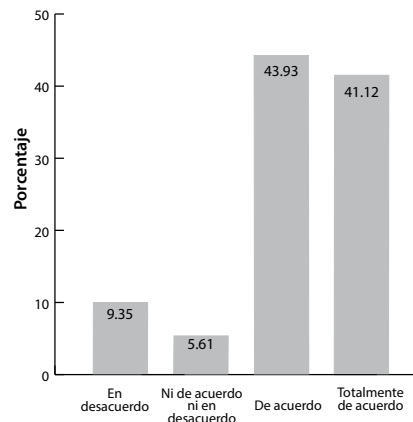
### 3. Resultados

El promedio de antigüedad de las empresas en la muestra es de 24.7 años, con un nivel de dispersión respecto a la media de 17.24 años, lo que indica un alto grado de variabilidad en la antigüedad de las empresas encuestadas (69.8%); esto se puede evidenciar al encontrar empresas con 2 años de antigüedad, así como otras que presentan 102 años. Cabe destacar que el 75% de las empresas de la muestra, cuentan con una antigüedad inferior a 35 años, lo cual indica que la gran mayoría de empresas encuestadas se encuentran en edades tempranas y medias de operación.

#### 3.1 Aspectos generales de seguridad en las Pymes

##### ¿Existen reglamentos (políticas y normas) para la utilización del software o programas en su empresa?

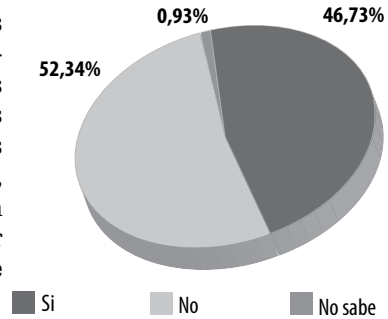
En la Gráfica 1 se puede observar que el 85.05% del total de la muestra está de acuerdo con que existen reglamentos para la utilización del software. Estas empresas han implantado políticas, normas y buenas prácticas que salvaguarden la seguridad de su información, sistemas de información (SI) y los recursos tecnológicos, beneficiándose al hacer mejor uso de las tecnologías de la información (TI) en función de los (SI) de la empresa.



**Gráfica 1.** ¿Existen reglamentos para la utilización del software?

**¿Los empleados de su empresa son capacitados en seguridad informática (prevención y protección de datos y/o equipos)?**

El 46.73% del total de la muestra respondió que sus empleados están capacitados en seguridad informática. Esto permite que los usuarios realicen mejores prácticas de seguridad física y lógica enmarcadas sobre la misma. También en los temas relacionados con delitos, legislación, amenazas, factores de riesgo, incidentes y políticas de seguridad, entre otros. Toda la apropiación de conocimiento que puedan tener y sea aplicado, permitirá obtener un alto nivel de seguridad informática (Gráfica 2).

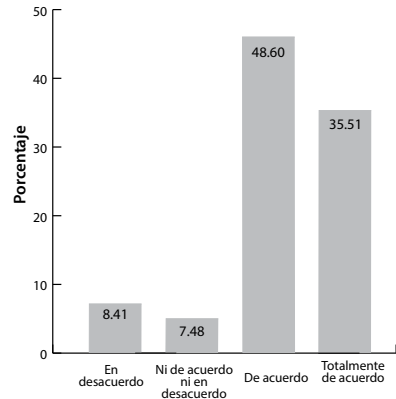


**Gráfica 2.** ¿Los empleados de su empresa son capacitados en seguridad informática?

**Seguridad: Integridad**

**¿Las bases de datos están integradas y disponibles para todos los procesos de información que requieren las áreas administrativas en su empresa?**

El 84.11% del total de la muestra están de acuerdo en que las bases de datos están integradas y disponibles para todos los procesos de información (Gráfica 3). Por lo tanto, se puede decir que se cumple con los requerimientos mínimos de seguridad de la información como la confidencialidad, la integridad y la disponibilidad. Así mismo, se puede pensar que criterios de calidad como la efectividad, la eficiencia y la confiabilidad prevalecen sobre el desarrollo de los mismos y en la información producida.



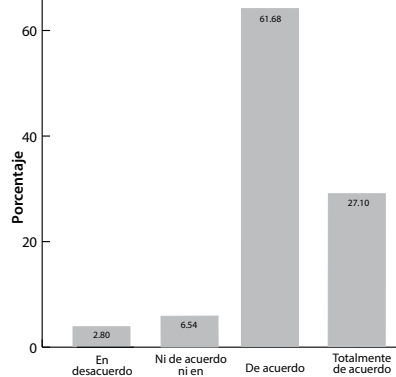
**Gráfica 3.** Bases de datos están integradas y disponibles para todos los procesos de información que requieren las áreas administrativas

En términos generales, la característica de integridad se evidencia con una tendencia a la aceptación por parte de las Pymes consultadas.

**Seguridad: Disponibilidad**

**¿Los informes del sistema son generados y entregados oportunamente?**

En la Gráfica 4 se evidencia que el 90.65% total de la muestra está de acuerdo en que los informes del sistema son generados y entregados oportunamente. Es decir, que los sistemas de información (SI), en conjunto con las tecnologías de la información (TI), funcionan óptimamente y generan información de calidad o en consecuencia efectiva, pertinente, entregada oportunamente, correcta y consistente.

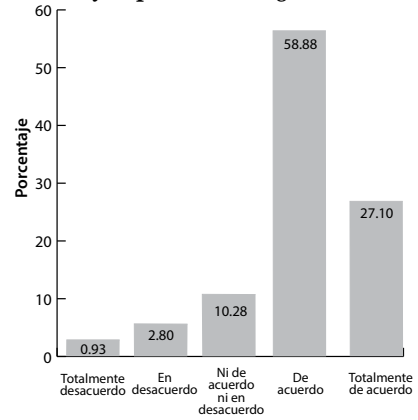


**Gráfica 4.** ¿Los informes del sistema son generados y entregados oportunamente?



**¿Las formas para ingresar los datos al sistema, son fáciles y rápidas de diligenciar?**

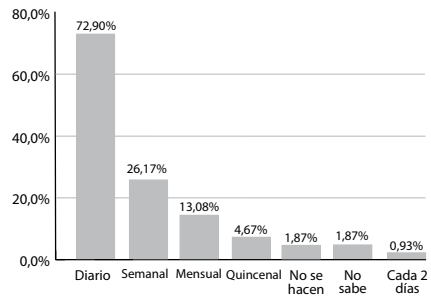
El 85.98% del total de la muestra de empresas consultadas, están de acuerdo con que las formas para ingresar los datos al sistema son fáciles (sencillas) y rápidas de diligenciar. Esto indica que los diseños de formularios para la entrada de datos con las tecnologías de información (TI) implantadas son amigables, y fáciles de entender. Por lo tanto, los usuarios se demoran poco tiempo en ingresar o actualizar los datos en el sistema. El 3.73% están en desacuerdo, tal vez porque los usuarios no tienen las competencias para hacer buen uso de los programas, falta mayor inducción o en definitiva el ingreso de los datos en demasiado extenso y dificultoso (Gráfica 5).



**Gráfica 5.** ¿Las formas como se ingresan los datos al sistema son fáciles y rápidas de diligenciar?

**¿Cada cuánto se hacen las copias de seguridad o backup de los datos en su empresa?**

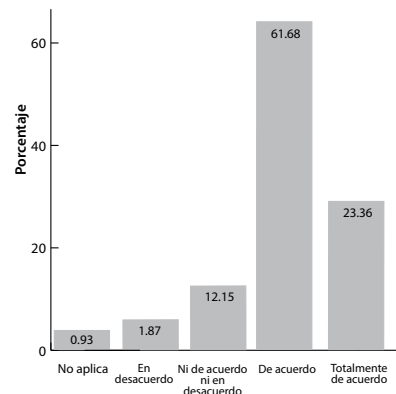
En el 72.90% de los casos se hacen copias de seguridad todos los días (Gráfica 6). Un resultado muy positivo porque se aseguran de tener un amplio respaldo de los datos para restaurarlos después de una eventual pérdida de los mismos, o consultas especiales por fechas específicas. El 26.17% lo hacen semanalmente, una práctica de alto riesgo porque están expuestos a repetir trabajos de varios días anteriores, cuando se presente la necesidad de restaurar y adicionalmente la pérdida de tiempo al enfrentar retrasos en los procesos de información inmediatos por atender.



**Gráfica 6.** Frecuencia de backup de los datos

**¿El software o programas en su empresa presentan fallas técnicas muy pocas veces?**

El 85.04% del total de la muestra están de acuerdo con que los programas presentan fallas técnicas muy pocas veces. Se puede decir que las instalaciones y configuraciones de las tecnologías de la información (TI) implementadas en las pymes de Santiago de Cali son las adecuadas para el desarrollo de sus procesos de información. Así mismo, las (TI) son de alta calidad, con la tendencia a una baja probabilidad de generar errores e incidencias que afecten su funcionalidad (Gráfica 7).



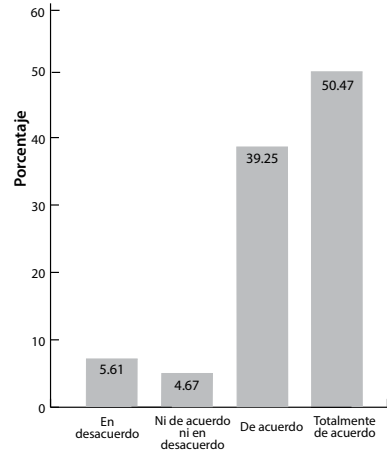
**Gráfica 7.** ¿El software o programas en su empresa presentan fallas técnicas muy pocas veces?

La disponibilidad de la información y de los sistemas de información en las Pymes equivale a un aspecto importante, considerando las respuestas entregadas por las Pymes consultadas.

**Seguridad: Confiabilidad**

**¿En la empresa hay software o programas especializados que requieren contraseñas?**

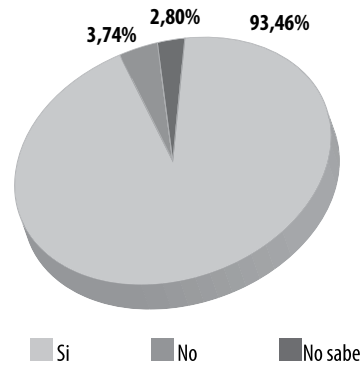
El 89.72% total de la muestra están de acuerdo en que hay programas o tecnologías de información (TI) especializados, que requieren contraseñas o password para controlar el acceso no autorizado; de esta forma se fortalece la seguridad de la información y se mantiene la confidencialidad, disponibilidad e integridad de la misma (Gráfica 8).



**Gráfica 8.** ¿En la empresa hay software o programas especializados que requieren contraseñas?

**¿La información generada por los sistemas de información de su empresa es confiable?**

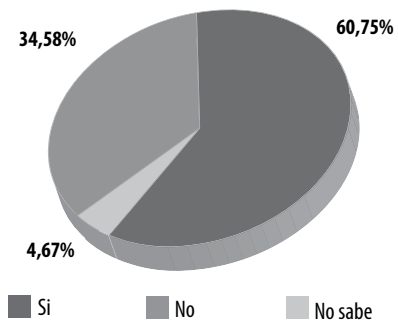
El 93.46% del total de la muestra aceptan que la información generada por los sistemas de información es confiable. Es decir, los métodos de recolección y captura utilizados para ingresar datos al sistema de las diferentes fuentes de información



primaria o secundaria permiten desarrollar procesos y generar información de calidad, segura y confiable (Gráfica 9).

**Gráfica 9.** ¿La información generada por los sistemas de información de su empresa es confiable?

**¿La empresa posee mecanismos de seguridad (firma digital, encriptado, cifrado) para el envío y recepción de información?**



El 60.75% del total de la muestra tienen mecanismos de seguridad para el envío y recepción de información. Es decir, la transferencia de datos está asistida por procesos de seguridad que proporcionan mayor protección de la información contra amenazas y factores de riesgo (Gráfica 10).

**Gráfica 10.** ¿La empresa posee mecanismos de seguridad para el envío y recepción de información?

La confiabilidad de los sistemas de información se encuentra en un nivel alto de efectividad, lo cual permite que las Pymes puedan utilizar la información generada por estos para propiciar estrategias competitivas.

## Conclusiones

El concepto de seguridad de la información en las organizaciones ha evolucionado favorablemente y eso se refleja en la implementación de diferentes mecanismos inmersos en la gestión tecnológica de las Pymes, esto permite salvaguardar uno de los activos más importantes de las organizaciones como es la información.

Por otra parte, este estudio evidenció que las Pymes de Santiago de Cali – Colombia, han implementado políticas y normas de seguridad que facilitan asegurar la integridad y la confiabilidad de los sistemas de información.

La disponibilidad de la información y los sistemas de información es vital para las Pymes, si se considera que estas herramientas son fundamentales para la construcción de estrategias organizacionales que les permitan ser más competitivas.

En el aspecto de la confiabilidad se estima que las Pymes de Santiago de Cali han generado mecanismos para propiciar confianza en sus sistemas de información, como por ejemplo los medios seguros de ingreso y envío de información y las contraseñas.

Finalmente, la seguridad en los sistemas de información de las Pymes de Santiago de Cali – Colombia, se puede catalogar como de alto nivel, considerando las políticas y normas, además de la preocupación constante por capacitar a los empleados en este tema clave para el direccionamiento estratégico de las organizaciones.

## Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

## Referencias bibliográficas

1. Cámara de Comercio de Cali. (2009). Las TIC impulsan la competitividad de las Mipymes. *Revista Acción No. 109*.
2. Cámara de Comercio de Manizales. (2009). *Masificación del uso de TIC en las mipymes de Manizales, estado actual y perspectivas futuras*.

3. Castillo, I., Caldera, R., Losavio, F., & Matteo, A. (2006). Caracterización de sistemas fiables basada en un modelo estándar de calidad. Proceeding XXXII, Conferencia Latinoamericana de Informática CLEI'2006. Santiago de Chile.
4. COBIT (1998): COBIT, Resumen ejecutivo. 2ª edición. Comité Directivo de COBIT y la Information Systems Audit and Control Foundation.
5. COBIT (2001): COBIT, 3ª. Edición. Comité Directivo de COBIT y la Information Systems Audit And Control Foundation.
6. ISO. (2002). ISO 17799. Obtenido de Wikipedia: [http://es.wikipedia.org/wiki/ISO/IEC\\_17799](http://es.wikipedia.org/wiki/ISO/IEC_17799)
7. ISO 9126. (s.f.). ISO/IEC 9126. Recuperado el 2009, de Wikipedia: [http://es.wikipedia.org/wiki/ISO/IEC\\_9126](http://es.wikipedia.org/wiki/ISO/IEC_9126)
8. Galin, D. (2004). Software Quality Assurance: From Theory to implementation. Madrid: Pearson.
9. González, J. M. (2001). Metodologías de control interno, seguridad y auditoría informática. En M. Piattini, Auditoría Informática, un enfoque práctico (págs. 45-91). Alfaomega: México.
10. Oficina Técnica de Difusión Estadística y Tecnología Informática del Instituto Nacional de Estadística e Informática (INEI). ¿Qué es la Teoría General de Sistemas?. Disponible en: [cmappublic.ihmc.us/rid=1G5HBCLFM-FG05P-LBF/TGS.pdf](http://cmappublic.ihmc.us/rid=1G5HBCLFM-FG05P-LBF/TGS.pdf). Consultado Enero 20 del 2014.
11. Laudon K. y Laudon J. (1998). Sistemas de Información Gerencial. Prentice Hall. 6ª Edición.
12. Lodensteijn, B. (2000). Auditing Quality is Quality Auditing. En M. Piattini, Auditing Information Systems (págs. 189-216). Estados Unidos: Idea Group Publishing (IGP).
13. Rakiting, S. (1997). Software Verification and validation: a practitioner's Guide. Boston: Artech House.
14. Ramió, J. (2006). Libro Electrónico de Seguridad Informática y Criptografía. Madrid España: Escuela electrónica de informática.
15. Riascos, S. (2008). Modelo para la evaluación de la efectividad de la tecnología informática en el entorno empresarial. *Ingeniería e investigación, Vol. 28, No. 002*, 158 – 166.
16. Ribagorda, A. (1997). Glosario de términos de seguridad de las T.I. Madrid: Ediciones CODA.
17. Robbins, S., & Coulter, M. (2005). Administración, 8va. Edición. México: Pearson Educación.
18. Sieber, S., Porta, V., Valor, J. (2006), Los sistemas de información en la empresa actual: aspectos estratégicos y alternativas tácticas. Mc GrawHill. España
19. Vidal (2004). Diagnóstico Organizacional, Evaluación sistémica del desempeño empresarial en la era digital. ECOE Ediciones.
20. Weber, R. (1999). *Information systems control and audit*. New Jersey: Prentice Hall.
21. Whitten, J, Bentley, L. y Barlow, V. (2003). Análisis y diseño de sistemas de información. México : McGraw-Hill.
22. Zambrano, K. (2004). Planificación y control de la Producción Pública. Caracas: S-PlanyCGKillian Z.D.