ISSN: 1692-7257 - Volumen 1 - Número 25 - 2015

Revista Colombiana de Tecnologías de Avanzada

Recibido: 4 de Junio de 2014
Aceptado: 15 de Octubre de 2014

DIGITAL SOCIAL NETWORKS: AN APPROACH TO RISK MANAGEMENT INFORMATION SYSTEMS

REDES SOCIALES DIGITALES: UNA APROXIMACIÓN A LOS RIESGOS EN SISTEMAS DE INFORMACIÓN GERENCIAL

MSc. José Gregorio Arévalo Ascanio*, MSc. Ramón Armando Bayona Trillos*
MSc. Dewar Willmer Rico Bautista**

*** Universidad Francisco de Paula Santander – Sede Ocaña.**
Grupo de Investigación en Desarrollo Socioempresarial (GIDSE).
Ocaña, Norte de Santander, Colombia, Tel.:+(57-7)-5690088.
E-mail: jgarevaloa@ufpso.edu.co, rabayonat@ufpso.edu.co
**** Universidad Francisco de Paula Santander Ocaña.**
Grupo de Investigación en Ingenierías Aplicadas (INGAP).
Ocaña, Norte de Santander, Colombia, Tel.:+(57-7)-5690088/5698118.
E-mail: dwricob@ufpso.edu.co

Abstract: This paper makes a review on the basic concepts related to security management information systems, along with organizational risks and the implementation of social networks as a tool for corporate management. Also, it emphasizes the need to reach an excellent positioning in regard with the newest security systems that are used within the scope of social networking. Finally, an entire analysis was made which allowed identifying the convergences and divergences on each nucleus. Thus, it was possible to formulate hypotheses, along with conclusions and the subsequent suggestions.

Keywords: Risk management; digital social networking; information security; information systems management; ITC.

Resumen: En este artículo se realiza una revisión de los conceptos fundamentales ligados a la seguridad en sistemas de información gerencial, riesgos en organizaciones y el uso de las redes sociales digitales a nivel organizacional. Al mismo tiempo se hace hincapié de cara a las empresas de la necesidad de posicionarse en las nuevas formas de protección incluyendo las redes sociales digitales. Finalmente, se realizó un análisis global mediante el cual se identificaron las convergencias y divergencias del análisis de cada uno de los núcleos temáticos, se formularon ciertas hipótesis, conclusiones y se hicieron algunas recomendaciones.

Palabras clave: Administración de riesgo, redes sociales digitales, seguridad de la información, sistemas de información gerencial, TICs.

1. INTRODUCCIÓN

Según (Alexander, 2007), el concepto de sistemas de información gerencial ha evolucionado desde su concepción hasta el punto de la incorporación de la seguridad como aspecto importante en la protección de la información como activo principal para los niveles gerenciales y directivos para la toma de decisiones. Por tanto es apremiante que las empresas a través de los sistemas de información gerencial establezcan un vínculo más cercano con los actores involucrados en el entorno, cliente interno y cliente externo. (Cano, 2013)

La estructura del presente trabajo parte de una breve ubicación del tema de la seguridad en sistemas de información gerencial. En la segunda y la tercera parte se revisan los principales estudios sobre riesgos y, en particular, según (Santos et al., 2009), de las redes sociales digitales, temas relacionados con las organizaciones.

El interés de este trabajo por la revisión de la bibliografía sobre seguridad en sistemas de información gerencial se explica por tres razones. Primero, porque la seguridad debe ser incorporada en las políticas de la organización para que la continuidad del negocio no sea afectada. Segundo, porque el análisis del riesgo expresa el impacto de pérdidas por confidencialidad, integridad y disponibilidad, y poder priorizar aquellos que son más problemáticos para la organización. Y tercero, porque la comprensión, la práctica y el uso de las redes sociales digitales se está incorporando como herramienta de mercadeo en el desempeño de las organizaciones empresariales.

2. METODOLOGÍA DE LA REVISIÓN DE LITERATURA

El presente trabajo es una investigación teórico descriptiva de tipo documental, dado que el procedimiento implica la búsqueda, organización y análisis de un conjunto de documentos electrónicos, ver Fig. 1, sobre los temas de seguridad en sistemas de información gerencial, riesgos en organizaciones y el uso de las redes sociales digitales, en el período comprendido en los últimos ocho años. La estructura metodológica del artículo se fundamenta en el establecimiento de tres fases, cuya dinámica implicó: en la primera, la búsqueda de los documentos, en la segunda la organización de los mismos y en la tercera la identificación de sus interrelaciones. (Sánchez, 2011). El objetivo de la primera fase es realizar la búsqueda de los documentos, en cada una de las bases de datos, se preseleccionaron artículos, al final en total cincuenta referencias, de acuerdo con los criterios de inclusión y exclusión. No se tomaron en consideración para el análisis aquellos artículos que no hacían alusión a los núcleos temáticos y/o aquellos que no se encontraban en revistas indexadas.

La revisión documental se realizó en revistas de alto impacto publicados en las bases de datos *IEEE, ACM, SCOPUS, Science Direct, SciELO, Directory of Open Access Journals (DOAJ), The National Academies Press, Redalyc, y LATINDEX*.

Como criterios de búsqueda, se incluyeron los siguientes descriptores: "Administración de riesgo"; "Redes sociales digitales"; "Seguridad de la Información"; "Sistemas de Información gerencial"; "Tecnologías de la Información y la Comunicación"; "*Risk management*"; "*Digital Social networking*"; "*Information security*"; "*Information systems management*"; "*Information Technology and Communication*". Estos descriptores fueron combinados de diversas formas al momento de la exploración con el objetivo de ampliar los criterios de búsqueda.

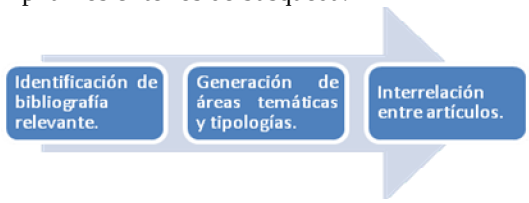

Fig. 1. Proceso estructurado de revisión bibliográfica.

El objetivo de la segunda fase es la organización de los documentos, se creó un archivo de Word, con los siguientes campos: título del artículo, autor, año, revista, información de la revista, problema de investigación, objetivos, tipo de investigación, método, descripción, instrumentos utilizados, resultados y núcleo temático. Una vez organizada la información, se agruparon los documentos en tres núcleos temáticos, a saber: seguridad en sistemas de información gerencial, riesgos en organizaciones y el uso de las redes sociales digitales.

El objetivo de la tercera fase es identificar interrelaciones a partir de un análisis de las similitudes, diferencias y contraposiciones de los conceptos planteados entre los artículos revisados y concluir sobre las perspectivas respecto al tema.

Posteriormente, se realizó el análisis de cada uno de los núcleos temáticos, identificando los problemas abordados, metodologías, instrumentos, población y resultados, definiendo lo más relevante y describiendo los aspectos comunes y divergentes entre los documentos seleccionados, mediante un ejercicio de comparación constante. Finalmente, se realizó un análisis global mediante el cual se identificaron las convergencias y divergencias del análisis de cada uno de los núcleos temáticos, se formularon ciertas hipótesis y conclusiones y se hicieron algunas recomendaciones.

Es de aclarar que de ninguna manera se pretende que esto sea trabajo completo, por lo cual es necesario y pertinente ampliar considerablemente las investigaciones reseñadas.

3. LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN GERENCIAL

Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las empresas (Rico Bautista et al., 2011). A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos y suministran una plataforma de información necesaria para la toma de decisiones; los actores empresariales que toman decisiones, han comenzado a comprender que la información no es sólo un subproducto de la conducción empresarial, sino que alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de éstos. Es por ello, que el manejo de los –SI– dentro de las empresas, constituye una decisión relevante en relación a la permanencia de las mismas en el actual mercado competitivo (Artigas et al., 2010).

La necesidad de obtener información del entorno, como elemento para reducir la incertidumbre para la toma de decisiones, está presente en todos y cada una de las actividades realizadas por el ser humano. La sistematización de la recopilación de informaciones, con un fin previamente definido, ha sido descrita por numerosos historiadores a lo largo de los siglos. Desde Herodoto, en su descripción de las fuentes informativas de Pericles para preparar las guerras Médicas, o Calístenes, en su descripción de los servicios de espionaje de Alejandro Magno que le facilitaban la información para preparar sus batallas contra el rey persa Dario, pasando por Walshingham, Secretario de Estado de la Reina Isabel de Inglaterra en el siglo XVI, quien gracias a la obtención y análisis sistemáticos de información sobre el desarrollo de la Armada Invencible española, contribuyó de manera fundamental a la victoria de los británicos; hasta llegar a Nathan Rothschild (S. XIX) que construyó una red de agentes en toda Europa, gracias a la cual fue el primero en conocer la derrota de Napoleón en Waterloo, información que le permitió contar con una ventaja a la hora de la compra/venta de bonos de Tesoro en la Bolsa de Londres (Farias y Gómez, 2011).

Una manera eficiente de acceder a la información del entorno y suministrar información al entorno, es valiéndose de las tecnologías de la información, para producir, generar y obtener información, la cual debe poseer características como: la precisión, la oportunidad, la pertinencia y la integridad de la misma (Machez, 2003).

El impacto de las Tecnologías de la Información y las Comunicaciones –TIC– no es ajeno al Derecho, por el contrario, cada día los avances de la tecnología imponen mayores retos a los operadores jurídicos; el Derecho participa en la gestión de la protección de la información, máxime cuando este tema es para las organizaciones uno de los que mayor preocupación genera para las áreas directivas, la protección de la información no es un querer arbitrario de los operadores jurídicos, es el resultado de un estudio profundo y concienzudo del sector real de la economía, al punto que organizaciones como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) han formulado recomendaciones en este sentido, las cuales hoy día están consignadas en la ISO 27 001. (Velasco, 2008)

En este contexto, se puede inferir que el delito informático es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien informático jurídico y/o material que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho; y en Colombia se rige con la Ley 1273 del 5 de enero de 2009 reconocida como la Ley de Delitos Informáticos. (Ojeda, Rincón, Arias, & Daza, 2010)

Desde esta óptica el desarrollo de una estrategia global de seguridad de la información a nivel nacional con políticas centradas en la necesidad de desarrollar herramientas de investigación y de concienciación del público disminuirán cada vez más las amenazas y vulnerabilidades de la seguridad en línea (Alamillo, 2009).

El papel importante asociado a los sistemas de información, el valor conferido a la información y el conocimiento que de ellos se puede extraer, coloca en el centro de la discusión el asunto de la seguridad de los sistemas informáticos. No sólo hay que tener buenos sistemas hay que tener sistemas seguros, con protecciones razonables contra ataques a la privacidad, la continuidad y la confiabilidad (Duque et al., 2007).

También la información es un valor de cambio dentro de sus riesgos: la información vale. La historia del periodismo relata que esto es así, en la llamada centuria de profesionalización periodística (1850-1950) cuando el desarrollo tecnológico provoca el surgimiento de las primeras empresas periodísticas y con ello el crecimiento de tiradas que, a su vez, implican la búsqueda de un número mayor de lectores, así como, de la publicidad como principal fuente de ingreso; pero probablemente la intuición marxista nos obligue a tomar en cuenta una situación tan actual como problemática: la configuración empresarial de medios de comunicación que tienen que obtener beneficios vendiendo información (Chillón, 2011).

Actualmente los direccionamientos estratégicos empresariales, bajo una perspectiva de la seguridad de la información son factores críticos de éxito para cualquier empresa madura en el uso y la adopción de los Sistemas de Información –SI– y las Tecnologías de la Información y la Comunicación –TIC–. Estos planes deben poseer un enfoque sistémico, ya que para ser completos deben abarcar aspectos relacionados con: la seguridad lógica y la seguridad física, el factor humano, la gerencia, la cultura y la estructura organizacional; convirtiéndose en una valiosa herramienta para aquellos trabajadores, encargados de la seguridad de la información ya que ayuda a comprender el problema en sus organizaciones y a bajar la incertidumbre frente al riesgo (Viloria y Blanco, 2009).

La seguridad informática contempla en la actualidad un importante número de disciplinas y especialidades distintas y complementarias, que se han convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de los países. Por ejemplo Cuba realiza grandes esfuerzos e invierte considerables recursos, para llevar la informatización a todos los niveles de la sociedad, pero producto de los avances alcanzados en los últimos años, con el incremento del uso de tecnologías de la información en todos los sectores surge como una necesidad del Estado cubano la creación de la Oficina de Seguridad para las Redes Informáticas (OSRI), adscripta al Ministerio de la Informática y las Comunicaciones (MIC), con el objetivo de prevenir, evaluar, investigar y dar respuesta a las acciones tanto internas como externas que afecten el normal funcionamiento de la Tecnología de la Información y las Comunicaciones –TIC– en el país (Díaz-Ricardo et al., 2014). En el campo médico, la seguridad y confiabilidad de los datos son dos de los aspectos más relevantes para almacenar, acceder y transmitir la información médica de los pacientes, y se conoce como telemedicina; para un sistema de Telemedicina como para cualquier sistema, una falla particular puede causar la caída del sistema por completo. En general, las amenazas y ataques sobre una red de datos, obligan a establecer parámetros para prevenir o mitigar estas falencias, más aún cuando la información médica que se maneja, es en general de tipo confidencial y por lo tanto, requiere resguardarse de ataques y amenazas que puedan afectar el derecho a la intimidad, la privacidad y la protección de los datos de los pacientes (Guillén et al., 2011).

Según (Melchor et al., 2012), desde el escenario empresarial, el Instituto Americano de Contadores Públicos Certificados en los Estados Unidos reporta la necesidad a partir del 2004, que los conceptos de tecnologías de información –TI– (incluido el manejo eficiente de datos) deben formar parte del conocimiento, destrezas y habilidades de los profesionales de la contabilidad. Pero pese a los beneficios que pueden percibirse del uso de los –SIC– para los contadores, los avances tecnológicos también han incrementado la vulnerabilidad de estos sistemas. Las amenazas a los sistemas de información en general ocurren durante el procesamiento u operación de los mismos; por ejemplo, creando programas ilegales, accediendo o eliminando archivos, destruyendo o corrompiendo la lógica de un programa con virus, entre otros aspectos de riesgo. El problema de la inseguridad de la información existe a pesar de que se han hecho cosas importantes, aunque no de manera sistemática, para atender esta debilidad como el adecuar los procesos del manejo de los –SIC.

En la Sociedad de la información, en un mundo cada vez más competitivo y globalizado, la información y su gestión se han convertido en un recurso valioso y estratégico para las empresas. Las –TI– afectan tanto a aspectos internos como externos de las empresas, a sus procesos, productos y comunicaciones, añadiendo valor a sus actividades, incrementando su eficacia y su eficiencia. Este panorama, supone que las empresas que no quieran quedar fuera deben ser capaces de identificar el valor estratégico de las –TI– en sus procesos de gestión y saber entender y aprovechar su potencial para mejorar la posición de sus negocios frente a la competencia (Paños, 2005). Por estas consideraciones es imprescindible

elaborar nuevos modelos para alcanzar desarrollos en distintos campos de la ciencia y la tecnología, que integren los flujos de tecnología, información y capital humano con el fin de realizar de forma rápida y efectiva los procesos relevantes de las empresas para su buen funcionamiento. Existe la necesidad de cambiar las técnicas administrativas tradicionales por las modernas empleando recursos tecnológicos como son los –SI– con el fin de contribuir con su desarrollo, crecimiento y competitividad. La integración de estos sistemas de información con enfoques modernos de sistemas de gestión del conocimiento y estrategias empresariales hace que los empresarios adopten un pensamiento sistémico y estratégico (Vega y Rincón, 2008). Las circunstancias que caracterizan el ambiente de negocios actual, que pueden resumirse en la internacionalización y la globalización de los mercados, junto al pleno desarrollo de la denominada Sociedad de la Información, han obligado a las empresas a mejorar su competitividad; ante tal panorama, la información aparece como un recurso estratégico de primer orden, cuya adecuada administración puede aportar a las empresas nuevas fórmulas de competir.

4. RIESGO EN LAS ORGANIZACIONES: PREVENIR VS. CORREGIR

Una política de seguridad eficaz de riesgos y la ejecución de las operaciones correctivas de seguridad de incidentes son procedimientos muy diferentes. Un gerente de una empresa debe equilibrar sus operaciones de seguridad a través de ambos paradigmas dependiendo el contexto de su organización. (Ansari et al., 2013) (Ghiglieri et al., 2014).

El primer paradigma es cuando se genera en un acontecimiento de seguridad fundamental un control preventivo. En el segundo la noción de un incidente representa un acontecimiento que evade cualquier mando preventivo y realiza cambios a sistemas de información. (Conti et al., 2012) (Gates y Proctor, 2014).

El momento del incidente es el punto de encuentro del riesgo y la prevención contra la respuesta. Si se conoce una amenaza en el pasado, los principios de fiabilidad y la explotación pueden ser aplicados en procesos de dirección para tomar decisiones y prevenir el daño de la amenaza. (Barth y Rubinstein, 2012) (Johnston y Wilson, 2012)

La corrección y las actividades de prevención son mutuamente exclusivas. Las tecnologías de corrección, como la detección de intrusión no eliminan la necesidad de tecnologías de prevención, como por ejemplo el manejo de acceso usando contraseña (Yadav y Dong, 2014). La prevención y la corrección de respuesta deben ser equilibradas para generar un estado estable de seguridad. Es importante entender las diferencias fundamentales entre los mecanismos de prevención y los de corrección de seguridad. (Gundecha et al., 2014)

Los de prevención son basados en experiencias pasadas con amenazas conocidas y estimando futuros acontecimientos similares (Ahmed y Matulevicius, 2014). Para impedir que un acontecimiento ocurra, primero es necesario desarrollar algunas pruebas sobre los acontecimientos pasados. La prevención demanda la predicción, pronosticando las valoraciones de la naturaleza y la probabilidad de un acontecimiento basado en pruebas de incidentes anteriores (Rai y Chukwuma, 2014).

El análisis de riesgo, lo más fundamental de todas las técnicas de dirección de seguridad, por lo general implica la cuantificación de las probabilidades de un acontecimiento de pérdida basado en la experiencia pasada y, asimismo los gastos de la pérdida asociada con aquel acontecimiento (Baskerville et al, 2014). La prevención principalmente implica acciones de control para ser tomadas ahora, antes de que el siguiente acontecimiento predicho ocurra (Rocha et al., 2014).

Los de corrección implican la planificación para acciones que principalmente ocurren en el futuro, incorporan preparativos de amenazas desconocidas, inesperadas o imprevisibles que aún pueden ocurrir. Pueden implicar procesos de detección para identificarse cuando un acontecimiento de pérdida de seguridad ha ocurrido (von y van, 2013). Se preparan para reacciones rápidas y eficaces a los nuevos tipos de acontecimientos. Una característica clave de respuesta es la agilidad. La respuesta principalmente implica la preparación para acciones de control a ser tomado en el futuro después de que un acontecimiento imprevisible ocurre (Webb y Ahmad, 2014) (van y Buchanan, 2013).

5. REDES SOCIALES DIGITALES EN EL DESEMPEÑO ORGANIZACIONAL

Este aparte profundiza en la naturaleza de las redes sociales, mediante una revisión de la literatura que aborda el tema desde la perspectiva empresarial. Las opiniones sobre la comprensión, la práctica y el uso de las redes sociales digitales resultan ser muy distintas, su auge en los últimos años, despierta cierto interés por parte del sector productivo, quienes conscientes de que sus stakeholders son parte activa de las redes sociales digitales, han cambiado la forma de comunicarse con cada uno de ellos.

Desde esta perspectiva, una de las herramientas utilizadas para mejorar la evaluación, el acercamiento y las preferencias de los consumidores, es la gestión de las relaciones con el cliente o CRM (Customer Relationship Management); así como un manejo eficiente de la información de ellos dentro de la organización. (Montoya & Boyero, 2013)

Uno de los posibles errores en que se puede incurrir durante la implementación de la herramienta –CRM– es asumir la tecnología como único elemento que da beneficio; por tanto, si la estrategia –CRM– no está bien estructurada, ya sea por no contar con herramientas tecnológicas adecuadas o porque no ha sido bien comunicada e implementada en la empresa, la información recolectada en los puntos de contacto con los clientes puede "diluirse" dentro de la empresa y llegar distorsionada al área de innovación o bien, nunca llegar. (Gil & Luis, 2011)

En este sentido, es pertinente considerar como lo menciona Harris y Rae, (Saavedra y Rialp, 2013), "las empresas, viendo el crecimiento de la actividad de las redes sociales digitales, están comenzando a utilizarlas en su estrategia de marketing debido al bajo costo de uso y su popularidad, siendo utilizadas para la construcción de marca y para medir la reputación de las relaciones con los clientes".

Según (Sandoval-Almazan y Nava, 2012) uno de los primeros estudiosos sobre las redes sociales es Katz quien por primera vez realiza un análisis de la teoría de redes y los grupos sociales con el uso de la tecnología.

A la anterior consideración cabría añadir la conceptuación de (Pérez y & Aguilar, 2012) sobre redes sociales "como un término que ha sido socialmente construido de manera reciente al menos desde dos dimensiones: 1) Como categoría de análisis socio-relacional y 2) Para referirse al conjunto de herramientas informáticas en línea que permiten la administración de contactos (entre las que destacan por su popularidad actual Facebook y Twitter)".

Dada la novedad de estas redes muy poco se ha investigado al respecto, a pesar de que ya muchas organizaciones empresariales han comenzado a utilizar las plataformas de redes sociales digitales en su accionar.

Estas son algunas de las investigaciones que se han realizado en torno a las redes sociales digitales a nivel empresarial:

En los últimos seis años se han realizado estudios sobre este tema, (García y Núñez, 2009), es uno de los primeros en analizar las redes sociales y su relación con el concepto de bloggers y su utilidad para la imagen de marca de las empresas. (Sandoval y Gutiérrez, 2010), a través de su investigación titulada "Twitter y Facebook en la estrategia empresarial", midieron el impacto que han tenido las nuevas tecnologías de redes sociales dentro de 40 empresas mexicanas. En el año 2011, (Gustavo da Cruz y Velozo , 2011) y (Ferreras, 2011), se generaron dos investigaciones, la primera pretendió analizar las estrategias promocionales realizadas por el Ministerio de Turismo de Brasil en las comunidades virtuales de Twitter y Youtube y la segunda orientada hacia mostrar cómo la corporación pública Euskal Irratia Telebista EITB gestiona su presencia en Facebook y Twitter.

El mayor número de investigaciones relacionadas con redes sociales digitales a nivel de empresas se concentra en el año 2012. En primer lugar, (Ruiz, 2012) con su investigación en las cinco mayores empresas españolas hizo un análisis que le permitió estudiar el contenido y el estilo de la información publicada en las redes sociales Facebook y Twitter de cada empresa. Autores como (Gonzalo y Toloza, 2012) se encargaron de hacer un estudio comparativo acerca del uso de redes sociales por parte de cinco Universidades Iberoamericanas. En otra dirección, (Aguilar y Perez, 2012), efectuaron un recorrido de la teoría a las prácticas comunicativas en Facebook, Twitter y Google+, con el objetivo de revisar campos semánticos del término de Redes Sociales y destacar los evidentes puntos de contacto entre ellos. (Sandoval y Nava,

2012), con su trabajo pretenden mostrar cómo diecisiete empresas mexicanas líderes en su ramo utilizan la plataforma Twitter para comunicarse con clientes, proveedores y público en general. Finalmente en este año, (López y Gonzalez, 2012), presentan los resultados de consultar por las Tecnologías de la Información y Comunicación –TIC– y Redes Sociales que emplean los productores y comercializadores del café colombiano, para promocionar o vender su café.

Para el año 2013, el estudio de la literatura en torno a las redes sociales digitales en las empresas muestra que autores como (Saavedra y Llonch, 2013), se preocupan por el uso de las redes sociales digitales como herramienta de marketing en el desempeño empresarial, en la cual toman una muestra de empresas españolas de distintos sectores y tamaños. En la misma dirección (Pérez et al., 2013), hacen una visión general sobre el uso de Facebook y Twitter en las principales marcas comerciales en España, para lo cual seleccionaron las cuentas de las tres marcas con mayor inversión publicitaria en 15 sectores.

La revisión de los estudios muestra que el uso de las redes sociales digitales se están implementando con éxito en las empresas de diversos países, ya que autores como (Sesma et al., 2014), se han preocupado por proponer la medición del desempeño social empresarial, definido como la satisfacción de los stakeholders, a través de las redes sociales. Además, (Palazón et al., 2014), en su investigación evaluaron en qué medida las comunidades de marca que se están desarrollando en las redes sociales sirven para que se ame más a las marcas.
Es pertinente señalar, que este aparte pretende mostrar el interesante ejercicio de acumulación de conocimiento sobre el uso de las redes sociales digitales por parte de las empresas, haciendo énfasis en el papel crucial que ha desempeñado la utilización de ellas para incrementar su participación en el mercado y por ende mejorar su nivel de competitividad. En este sentido, los estudios que permiten reconstruir la trayectoria del uso de ellas a nivel empresarial son detallados, en la descripción y explicación de su propósito de no solo buscar vender sino también fidelizar haciendo que los grupos de interés se sientan atendidos y escuchados. (Garfinkel, 2012)

Sin embargo, el estudio de la literatura en torno a las redes sociales digitales muestra la necesidad de que el tema ocupe un lugar central en la investigación académica, dado que en líneas generales las empresas tienen que percatarse de que es necesario incluir dichas redes en sus estrategias de marca y planes de comunicación.

6. CONCLUSIONES

El uso de las tecnologías de información en las Mipymes cobra vital importancia si se considera que hoy en día representan un elemento fundamental para incrementar la competitividad de las mismas. Dichas tecnologías mejoran el desempeño de la empresa por medio de la automatización, el acceso a información, las relaciones con el contexto e incorporación de procesos de aprendizaje continuo.

En este nuevo milenio, caracterizado por la sociedad de la información y las comunicaciones, requiere que todas las organizaciones, sean éstas públicas o privadas, nacionales o transnacionales, cualquiera que sea el sector económico en que desarrollen su objeto social, están directamente relacionadas con la tecnología informática y los sistemas de información, sea que adquieran o desarrollen activos de información; realidad que hace que la seguridad sea algo que demande su permanente atención y salvaguarda. La alta gerencia frente al tema de la seguridad de la información deberá mantener una mentalidad de servicio que no busque protagonismos en las funciones de negocio, sino la perfecta sinergia que agregue valor al proceso y a sus clientes. Así mismo, deberá promover una cultura de apoyo y educación que promueva desde su propio ejemplo las practicas que desee desarrollar en la organización. Los resultados sobre las dimensiones del uso de las redes sociales digitales en las empresas varían en contenido y cantidad según los autores, el enfoque, la metodología, el tiempo y el tipo de institución donde se realiza el estudio.

La revisión sirve a otros investigadores que necesiten conocer el estado y evolución de la investigación en torno a la seguridad en sistemas de información gerencial, riesgos en organizaciones y el uso de las redes sociales digitales a nivel empresarial.

REFERENCIAS

Alamillo, I. (2009). Las políticas públicas en materia de seguridad en la sociedad de la

información. *Revista de Internet, Derecho y Política*(9), 13-24.

Aguilar Edwards , A., & Perez Salazar, G. (Julio de 2012). Reflexiones conceptuales en torno a las redes sociales en las redes sociales: un recorrido de la teoría a las prácticas comunicativas en facebook, twitter y google+. *Razón y Palabra, 17*.

Ahmed, N., & Matulevicius, R. (2014). Securing business processes using security risk-oriented patterns. *Computer Standards and Interfaces, 36*(4), 723-733.

Alexander, A. (2007). *Diseño y gestión de un sistema de seguridad de información* (Vol. 1). Bogotá, Cundinamarca, Colombia: Alfaomega.

Ansari, F., Akhlaq, M., & Rauf, A. (11 de Diciembre de 2013). Social networks and web security: Implications on open source intelligence. *Information Assurance (NCIA), 2013 2nd National Conference on* , 79,82.

Artigas, W., Fernández, Y., & Useche, M. C. (Agosto de 2010). Adquisición de sistemas de información en empresas. *Multiciencias, 10*(2), 155-162.

Barth, A., & Rubinstein, B. (Agosto de 2012). A Learning-Based Approach to Reactive Security. *Dependable and Secure Computing, IEEE Transactions on , 9*(4), 482,493.

Baskerville, R., Spagnoletti, P., & Ki, J. (Enero de 2014). , Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138-151.

Cano, J. (2013). *Inseguridad de la información: Una visión estratégica.* Bogota, Cundinamarca, Colombia: Alfaomega.

Chillón Lorenzo, J. (2011). Ética y empresa informativa: notas para un discurso integrador. *Comunicación y Hombre*(7), 107-118.

Conti, M., Poovendran , R., & Secchiero, M. (26-29 de Agosto de 2012). FakeBook: Detecting Fake Profiles in On-Line Social Networks. *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on* , 1071,1078.

Díaz-Ricardo, Y., Pérez-del Cerro, Y., & Proenza-Pupo, D. (Junio de 2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de. *Ciencias Holguín, 20*(2), 1-14.

Duque Mendez, N., & Chavarro Porras, J. (Agosto de 2007). Seguridad inteligente. *Scientia Et Technica, 13*(35), 389-394.

Farias, P., & Gómez, M. (Julio de 2011). Productividad empresarial de la información: organización . *Razón y Palabra*.

Ferreras Rodríguez, E. (Julio de 2011). La estrategia de la corporación eitb (euskal irratia telebista) en facebook y twitter. *Razón y Palabra, 2011*(76).

García Guardia, M., & Núñez, P. (2009). Los bloggers y su infuencia en la imagen de una marca. *Revista icono 14: Revista de comunicación y nuevas tecnologías, 2009*(12), 242-252.

Garfinkel, S. (Junio de 2012). The cybersecurity risk. *Commun. ACM 55, 55*(6), 29-32.

Gates, C., & Proctor, R. (Junio de 2014). Effective Risk Communication for Android Apps. *Dependable and Secure Computing, IEEE Transactions on* , 252,265.

Ghiglieri, M., Stopczynski, M., & Waidner , M. (24-28 de Marzo de 2014). Personal DLP for Facebook. *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on* , 629,634.

Gil, A., & Luis, C. (2011). La innovación centrada en el cliente utilizando el modelo de inferencias en una estrategia CRM. *Investigaciones Europeas de Dirección y Economía de la Empresa, 17*(2), 15-32. Recuperado el 11 de 03 de 2015

Gonzalo Brito, J., Laaser, W., & Toloza, E. (Agosto de 2012). El uso de redes sociales por parte de las universidades a nivel institucional. Un estudio comparativo. *RED. Revista de Educación a Distancia.*, 1-38.

Guillén Pinto, E., Ramírez, L., & Estupiñán Cuesta, E. (2011). Análisis de seguridad para el manejo de la información médica en telemedicina. *Ciencia e Ingeniería Neogranadina, 21*(2), 57-89.

Gundecha, P., Barbier, G., & Tang, J. (2014). User vulnerability and its reduction on a social networking site. *ACM Transactions on Knowledge Discovery from Data, 9*(2).

Gustavo da Cruz, G., & Velozo , T. (2011). Twitter, youtube e innovación en la promoción turística online. *Estudios y perspectivas en turismo, 20*, 627-642.

Johnston, A., & Wilson, S. (2012). Privacy Compliance Risks for Facebook. *Technology and Society Magazine, IEEE, 31*(2), 59,64.

López Cardona, D., & Gonzalez Gómez, J. (Diciembre de 2012). Uso de las TIC y redes sociales paravender café colombiano. *Ventana Informática*(27), 81-96.

Machez, M. (Junio de 2003). Propuesta de optimización de la gestión de información en la pequña empresa y mediana empresa, sector turístico . *Ciencia y Sociedad, 28*(2), 253-270.

Melchor Medinaa, J., Lavín Verástegui, J., & Pedraza Melo, N. (Diciembre de 2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. *Contaduría y administración*, 11-34.

Montoya, C., & Boyero, M. (2013). El CRM como herramienta para el servicio al cliente en la organización. *Vis. futuro [online], 17*(1), 130-151. Recuperado el 11 de 03 de 2015

Ojeda, J., Rincón, F., Arias, M., & Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuad. Contab., 11*(28), 41-66. Recuperado el 05 de 03 de 2015

Palazón, M., Sicilia, M., & Delgado, E. (Marzo de 2014). El papel de las redes sociales como generadoras de "amor a la marca". *Universia Business Review*(41), 18-39.

Paños Álvarez, A. (2005). Análisis de factores contingentes en el estudio de la relevancia estratégica de las tecnologías de la información en la empresa. *Anales de Documentación , 8*, 187-216.

Pérez Dasilva, J., Genaut Arratibel, A., & Meso Aierdi, K. (2013). Las empresas en Facebook y Twitter. Situación actual y estrategias comunicativas. *Revista Latina de Comunicación Social*(68), 676-695.

Pérez Salazar, G., & Aguilar Edwards, A. (Julio de 2012). Reflexiones conceptuales en torno a las redes sociales en las redes sociales. *Razón y Palabra, 17*(79).

Rai, S., & Chukwuma, P. (2014). 2014 Top Security Topics. *EDPACS, 49*(3), 22-28.

Rico Bautista, D., Quel Hermosa, E., & Carvajal Mora, H. (2011). Redes y tecnologías de banda ancha.tecnologías de acceso de banda ancha. *Revista Colombiana de Tecnologías de Avanzada, 1*(17), 113-120.

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (Junio de 2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110.

Ruiz Iniesta, C. (Julio de 2012). La comunicación empresarial en redes sociales. El caso de las cinco mayores. *Razón y Palabra, vol. 17*.

Saavedra, F., & Rialp Criado, J. (Diciembre de 2013). El uso de las redes sociales digitales como herramienta de marketing en el desempeño empresarial. *Cuadernos de Administración, 26*(48), 205-231.

Saavedra, F., Rialp Criado, J., & Llonch Andreu, J. (Diciembre de 2013). El uso de las redes sociales digitales como herramienta de marketing en el desempeño empresarial. *Cuadernos de Administración, 26*(47), 205-231.

Sánchez Upegui, A. A. (2011). *Manual de redacción académica e investigativa: cómo escribir, evaluar y publicar artículos.* Medellin, Antioquia, Colombia: Fundación Universitaria Católica del Norte.

Sandoval Almazán, R., & Gutiérrez Alonzo, M. (2010). Twitter y Facebook en la estrategia empresarial.

Sandoval Almazan, R., & Nava Rogel, R. (Octubre de 2012). Uso de twitter en la empresa mexicana: un modelo de análisis. *Razón y Palabra, 17*.

Sandoval-Almazan, R., & Nava Rogel, R. (Octubre de 2012). Uso de twitter en la empresa mexicana: un modelo de análisis. *Revista de Estudios en Contaduría, Administración e Informática, 17*(80).

Santos Jaimes, L., Portilla Jaimes, J., & Méndez, J. (2009). Plataformas J2EE y .net en el desarrollo de servicios web. *Revista Colombiana de Tecnologías de Avanzada, 1*(13), 125-132.

Sesma, J., Husted, B., & Banks, J. (Junio de 2014). La medición del desempeño social empresarial a través de las redes sociales. *Contaduría y Administración , 59*(2), 121-143.

van Deursen, N., & J. Buchanan, W. (Septiembre de 2013). Monitoring information security risks within health care. *Computers & Security, 37*, 31-45.

Vega Escobar, A., & Rincón , E. (Junio de 2008). Sistemas de Información como una Estrategia de Desarrollo, Crecimiento y Competitividad. de las Pequeñas y Medianas Empresas del Sector Servicios de Vigilancia en Bogotá D.C. *Revista Avances en Sistemas e Informática, 5*(2), 121-130.

Velasco Melo, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *REVISTA DE DERECHO*(29), 333-366.

Viloria, O., & Blanco, W. (Junio de 2009). Modelo sistémico de la seguridad de la información. *Revista Venezolana de Análisis de Coyuntura, 15*(1), 219-240.

von Solms, R., & van Niekerk, J. (Octubre de 2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Webb, J., & Ahmad, A. (Julio de 2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15.

Yadav, S., & Dong, T. (2014). A comprehensive method to assess work system security risk. *Communications of the Association for Information Systems*, *34*(8), 169-198.