GESTIÓN DE SEGURIDAD DEL CONOCIMIENTO EN LOS PROCESOS ADMINISTRATIVOS DE LAS INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR: EL CASO DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

LEIDY JOHANNA CÁRDENAS SOLANO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
MAESTRÍA EN INGENIERÍA INDUSTRIAL
BUCARAMANGA
2017

GESTIÓN DE SEGURIDAD DEL CONOCIMIENTO EN LOS PROCESOS ADMINISTRATIVOS DE LAS INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR: EL CASO DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

LEIDY JOHANNA CÁRDENAS SOLANO

Trabajo de grado para optar por el título de Magister en Ingeniería Industrial

Director
HUGO ERNESTO MARTÍNEZ
Magíster en Ingeniería Electrónica
Doctor en Ingeniería

Codirector
LUIS EDUARDO BECERRA ARDILA
Magíster en Ingeniería Industrial
Profesor Titular Escuela de Estudios Industriales y Empresariales

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
MAESTRÍA EN INGENIERÍA INDUSTRIAL
BUCARAMANGA
2017

CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

RESUMEN

TÍTULO: GESTIÓN DE SEGURIDAD DEL CONOCIMIENTO EN LOS PROCESOS ADMINISTRATIVOS DE LAS INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR: EL CASO DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

AUTORA: LEIDY JOHANNA CÁRDENAS SOLANO[1] [2] [3]

PALABRAS CLAVES: Educación Superior, Gestión del conocimiento, Seguridad de la Información, Tecnologías de Información, Análisis de Riesgos

DESCRIPCIÓN

La influencia de la gestión de conocimiento en la obtención de ventajas competitivas y en el desempeño de la organización, y la problemática de la comprensión de la gestión de seguridad del conocimiento que afronta en la actualidad el sistema administrativo de cualquier organización, incluyendo las instituciones de educación superior pública han sido los principales aspectos que motivaron está investigación, en la cual siguiendo la metodología de investigación acción y tomando como unidad de intervención la Universidad Industrial de Santander, se busca identificar conocimientos y acciones relevantes para asegurar el conocimiento y proteger los activos de información, como soporte a la gestión sostenible de las IES Públicas colombianas, el cual guie a las IES (Instituciones de Educación Superior) en la incorporación de la gestión de conocimiento de manera segura de acuerdo a las necesidad y estrategias definidas por la institución, garantizando los tres pilares fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad. De acuerdo con los principales hallazgos se recomienda proporcionar diferentes tipos de mecanismos para proteger el conocimiento sensible, capacitar el personal, fomentar una cultura desde las directrices hasta la operación de la institución, crear y/o actualizar la documentación existente en la institución del tema y hacer buen uso de los sistemas de información como apoyo a la gestión sostenible de seguridad del conocimiento e información.

[1] Trabajo de grado

[2] Facultad Fisicomecánicas. Escuela de Estudios industriales y empresariales. Director Hugo Ernesto Martínez Ardila. Codirector Luis Eduardo Becerra Ardila.

[3] Correo electrónico: leidy.cardenas2@correo.uis.edu.co

ABSTRACT

TITLE: SAFETY MANAGEMENT OF KNOWLEDGE IN ADMINISTRATIVE PROCESSES OF PUBLIC HIGHER EDUCATION INSTITUTIONS. CASE STUDY: INDUSTRIAL UNIVERSITY OF SANTANDER, COLOMBIA.

AUTHOR: LEIDY JOHANNA CÁRDENAS SOLANO[4] [5]

KEYWORDS: Higher Education, Knowledge Management, Information Security, Information Technology, Risk Analysis

DESCRIPTION:

The influence of knowledge management in obtaining competitive advantages and organizational performance, and the problem of understanding the safety management of knowledge currently facing the administrative system of any organization, including the institutions of public higher education have been the main aspects that motivated this research, in which following the action research methodology and taking as an unit of analysis the Industrial University of Santander, seeks to identify relevant knowledge and actions to ensure knowledge and protect information assets, as a support for sustainable management of public HEIs in Colombia, which will guide HEIs (Higher Education Institutions) in the incorporation of knowledge management in a secure manner according to the needs and strategies defined by the institution, guaranteeing the three pillars of Information security: confidentiality, integrity and availability. According to the main findings, it is recommended to provide different types of mechanisms to protect sense knowledge, to train staff, to promote a culture from the guidelines to the operation of the institution, to create and / or update existing documentation in the institution of the topic and make good use of information systems as support for sustainable management of knowledge and information security.

[4] Bachelor Thesis

[5] Facultad Fisicomecánicas. Escuela de Estudios industriales y empresariales. Director Hugo Ernesto Martínez Ardila. Codirector Luis Eduardo Becerra Ardila.

INTRODUCCIÓN

En una “economía del conocimiento”, el conocimiento se compone del conjunto de información, inteligencia y experiencia práctica que, transformado en capacidad para la acción, constituye la base de las cualidades que atesoran las organizaciones[6]. Así pues, la habilidad para adquirir información, transformarla en conocimiento, incorporarlo como aprendizaje, compartirlo rápidamente y ponerlo en práctica dónde, cómo y cuando sea necesario, constituye la capacidad organizativa más importante para enfrentarse a las turbulencias del entorno[7] [8] [9] [10] [11] [12]. De esta manera, se crea la necesidad de implementar acciones que lleven a las organizaciones hacia una adecuada gestión de conocimiento, entre las cuales se encuentran las prácticas de seguridad de la información. Dichas prácticas se refieren en la literatura a la protección de todas las actividades de manejo de la información, pueden éstas ser técnicas o no técnicas[13], puesto que, la seguridad de la información ya no es principalmente un problema técnico como lo fue considerado

[6] PRIETO PASTOR, Isabel María. Una valorización de la gestión del conocimiento para el desarrollo de la capacidad de aprendizaje en las organizaciones: propuesta de un modelo integrador. Tesis de doctorado. España: Universidad de Valladolid, Facultad de Ciencias Económicas y Empresariales, Departamento de Economía y Administración de Empresas, 2003, 310p.

[7] DOGSON, Mark. Organizational Learning: A Review of Some Literatures. En: Organization Studies. Mayo, 1993, vol.14, no. 3, p. 375-394.

[8] NONAKA, Ikujiro. A Dynamic Theory of Organizational Knowledge Creation. En: Organization Science, Febrero, 1994, vol.5, no. 1, p.14-37.

[9] NONAKA, Ikujiro y TAKEUCHI, Hirotaka. The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press, 1995. p. 298. ISBN 978-0195092691

[10] BIERLEY, Paul y CHAKRABARTI, Alok. Generic Knowledge Strategies in the U.S. Pharmaceutical Industry. En: Strategic Management Journal. Diciembre, 1996, vol.17 (winter special issue), p. 123-135.

[11] GRANT, Robert M. Prospering in Dynamically-Competitive Environments: Organizational Capability as Knowledge Integration. En: Organization Science. Julio-agosto, 1996, vol. 7, no. 4, p. 375-387

Capability as Knowledge Integration. Organization Science, vol. 7, nº4, July/August, págs. 375-387.

[12] GRANT, Robert M. Toward a Knowledge-Based Theory of the Firm. En: Strategic Management Journal. Diciembre, 1996, vol.17 (winter special issue), no. 52, p. 109-122.

[13] DHILLON, Gurpreet. Principles of Information Systems Security: text and cases. 1 ed. New York: John Wiley and Sons, 2007. 464 p. ISBN 978-0471450566

en los años 80, conocida como la “ola técnica” según von Solms[14], sino un problema de gestión o de negocio[15] [16] [17] [18] [19].

Asimismo, la ‘Sociedad de la Información’ que se refiere a un modo de desarrollo social y económico en el que la adquisición, almacenamiento, procesamiento, valorización, transmisión, distribución y diseminación de información que conduce a la creación de conocimiento y a la satisfacción de las necesidades de los ciudadanos y de las empresas, desempeñan un papel central en la actividad económica, en la creación de riqueza, en la definición de la calidad de vida de los

[14] VON SOLMS, Bassie. The 5 Waves of Information Security: From Kristian Beckman to the Present. En: Security and Privacy - Silver Linings in the Cloud - 25th IFIP TC-11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010. Memorias. Brisbane, Australia, 2010; p. 1.

[15] DHILLON, G. and BACKHOUSE, J. Information system security management in the new millennium. En: Communications of ACM. 2000, vol. 43, no. 7, pp. 125-8. Citado por: CHANG, Shuchih Ernest y HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

[16] VERMEULEN, Clive y VON SOLMS, Rossouw. The information security management toolbox – taking the pain out of security management. En: Information Management & Computer Security. 2002, vol. 10, no. 2/3, pp. 119-25. Citado por: CHANG, Shuchih Ernest y HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

[17] DUTTA, Amitava y MCCROHAN, Kevin. Management’s role in information security in a cyber economy. En: California Management Review. Octubre, 2002, vol. 45, no. 1, pp. 67-87. Citado por: CHANG, Shuchih Ernest y HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

[18] SO, May W.C. y SCULLI, Domenic. The role of trust, quality, value and risk in conducting e-business. En: Industrial Management & Data Systems. 2002, vol. 102, no. 9, pp. 503-12. Citado por: CHANG, Shuchih Ernest y HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

[19] VON SOLMS, B. y VON SOLMS, Rossouw. The 10 deadly sins of information security management. En: Computers & Security. 2004, vol. 23, no. 5, pp. 371-6. Citado por: CHANG, Shuchih Ernest y HO, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

ciudadanos y de sus prácticas culturales[20] [21]. La sociedad de la Información corresponde, por consiguiente, a una sociedad cuyo funcionamiento recurre crecientemente a redes digitales de información[22], y es cada vez más dependiente de la Gestión de la Seguridad de los Sistemas de Información (SGSI) y el conocimiento de los riesgos de seguridad asociados con el valor de sus activos[23].

Con relación a la literatura en el área de la gestión de seguridad de la información (GSI), la información es considerada como un "activo" discreto y relativamente estático que se puede cuantificar con fines contables y de auditoría de seguridad[24]. Por tanto, existen muchas metodologías teóricas y estándares prácticos alineadas con los objetivos de negocio, que en su mayoría son demasiado engorrosas para ser adoptadas por una organización, por lo que, tampoco existe un marco unificado para gestionar sistemáticamente las tediosas tareas de gestión de la seguridad de la información[25].

Estos objetivos no están enmarcados en términos de ventaja competitiva, lo cual significa que la literatura sobre GSI no tiene en cuenta la información como un tipo

[20] Misión para la Sociedad de la Información de Portugal (1997). Livro verde para a sociedade da informação em Portugal. Disponible en: http://www.posc.mctes.pt/documentos/pdf/LivroVerde.pdf. Citado por CASTELLANO AZÓCAR, Luis Eliseo (n.d). Modelo para la detección de necesidades de información de los organismos públicos como estrategia para el desarrollo de programas de gobierno electrónico. pp. 1-48 Disponible en: http://siare.clad.org/fulltext/0076542.pdf

[21] Universidad Nacional de San Juan (n.d). Concepto de la sociedad de la información. (Recuperado en 22 de agosto de 2017). Disponible en: http://www.unsj.edu.ar/unsjVirtual/comunicacion/seminarionuevastecnologias/wp-content/uploads/2015/05/concepto.pdf

[22] RODRIGUEZ DE ALMEIDA, Reginaldo. De la sociedad de la información a la sociedad del conocimiento: la sociedad del BIT. 2003. (Recuperado en 22 de agosto de 2017). Disponible en: http://biblioteca.ucm.es/tesis/inf/ucm-t26909.pdf

[23] SANTOS OLMO PARRA, Antonio; SANCHEZ CRESPO, Luis Enrique; ALVAREZ, Esther; HUERTA, Mónica y FERNANDEZ MEDINA PATON, Eduardo. Methodology for Dynamic Analysis and Risk Management on ISO27001. En: IEEE Latin America Transactions. 2016, vol. 14, No. 6, pág. 2897-2911. DOI 10.1109/TLA.2016.7555273

[24] SHEDDEN, P.; SCHEEPERS, R.; SMITH, W. y AHMAD, A. Incorporating a knowledge perspective into security risk assessment. En: VINE Journal Knowledge Management. 2011, vol. 41, no. 2. p. 152-166.

[25] CHENG-YUAN, Ku, MAN-NUNG, Liu y TSUNG-HAN, Yang. An integrated system for information security management with the unified framework. En: Journal of risk research. Julio, 2014, vol. 19, no. 1, p. 21-41

de conocimiento que podría generar o agregar valor. Por consiguiente, aunque la gestión de conocimiento ha sido implementada en las organizaciones con el objetivo de lograr ventajas competitivas, las prácticas de gestión de seguridad de la información, por el contrario, no están alineadas a ello. Es por eso por lo que existe la necesidad de conciliar la preservación de la confidencialidad del conocimiento con el fin de lograr y mantener estas ventajas, de una parte; y aumentar el intercambio de conocimientos por otro, con la intención de favorecer los procesos de gestión del conocimiento. Lo anterior, en suma, se convierte en un dilema clave para las organizaciones, y constituye la justificación de proponer un modelo de gestión de seguridad del conocimiento guiado a través de la gestión de la seguridad de la información, dado que "la información es la base fundamental sobre la cual la seguridad desarrolla su dinámica y propone las acciones de protección"[26].

En este contexto, se encuentra la Universidad Industrial de Santander - UIS, institución pública con un importante avance en materia de protección intelectual, con un modelo MECI[27] 1000:2014 (Modelo Estándar de Control Interno) establecido para la gestión de sus riesgos operativos y un sistema de gestión de calidad consolidado. Bajo estos antecedentes, el presente estudio buscó responder a la pregunta ¿Cómo desarrollar el proceso de gestión de seguridad de la información y el conocimiento en los procesos estratégicos y de apoyo de la Universidad Industrial de Santander?

Para responder esta pregunta, el presente trabajo tuvo como objetivo principal diseñar un modelo de gestión de seguridad del conocimiento para los procesos

[26] LACEY, David. Managing the human factor in information security: how to win over staff and influence business managers. Chichester: John Wiley & Sons, 2009. 384 p. ISBN: 978-0-470-72199-5. p. 15-16.

[27] Fue reglamentado por el Gobierno Nacional a través del Decreto 1599 de 2005, por medio del cual se dispone la implementación del Modelo Estándar de Control Interno MECI en todas las entidades que hacen parte del ámbito de aplicación de las Leyes 87 de 1993 y 489 de 1998. Este modelo es el medio a través del cual se realiza seguimiento y evaluación a lo dispuesto en el Decreto 2482 de 2012 en cuanto al Modelo Integrado de Planeación y Gestión.

administrativos en la Universidad Industrial de Santander como referencia para otras Instituciones públicas de Educación Superior colombianas, por tanto, se inició esta investigación comprendida por cuatro fases.

A continuación, en la primera sección se abordan los principales fundamentos teóricos y los consensos de la literatura para proceder a explicar en el segundo capítulo la metodología de investigación cualitativa utilizada. Luego, en el tercer capítulo se exponen los resultados obtenidos divididos en cuatro partes; (i) resultados de la revisión de la literatura; (ii) descripción del estado actual de la seguridad de la información y la gestión del conocimiento en las Instituciones públicas de educación superior colombianas; (iii) el nivel de madurez de la UIS en gestión del conocimiento y su estado actual de cumplimiento de los controles de seguridad de la información establecidos por la norma ISO/IEC 27001:2005; y (iv) el modelo de seguridad de la información y el conocimiento de acuerdo al ciclo PHVA (Planificar, Hacer, Verificar y Actuar). Por último, se exponen las conclusiones del trabajo y se presentan los aportes y limitaciones de la investigación.

1. MARCO TEÓRICO

Hace más de 20 años, algunos académicos como Drucker[28], Porter y Millar[29], fueron los primeros en reconocer que una "Revolución de la Información" estaba teniendo lugar, la cual tuvo un impacto inmediato, con efectos significativos en todos los aspectos de la vida organizacional[30]. A través de los años, la experiencia ha comprobado que una buena gestión de la información no sólo puede mejorar significativamente el desempeño organizacional[31] [32] [33], sino que también puede transformar radicalmente los procesos, estructura y cultura de la organización[34] [35].

Dada su creciente importancia, la información es a menudo vista como análoga a la "sangre" de la organización[36] [37] [38]. Por consiguiente, si el flujo de información es continuo, los procesos y tareas se ejecutarán de manera óptima; por el contrario, si

---

[28] DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. 1988, vol. 66, no. 1. p. 47

[29] PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. 1985, vol. 64, no. 4. p. 149

[30] ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Septiembre, 2007, vol. 18, no. 5. p. 751

[31] BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Abril, 1996, vol. 42, no. 4. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Diciembre, 2009, vol. 29, no. 6. p. 449

[32] SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. 2009, vol. 19, no. 3. Citado por DOHERTY, ANASTASAKIS y FULFORD. Op. cit.

[33] WARD, John y PEPPARD Joe. Strategic planning for information systems. 3 ed. Chichester: John Wiley & Sons Ltd., 2002. 624 p. Citado por: DOHERTY, ANASTASAKIS y FULFORD. Op. cit.

[34] DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Octubre, 2003, vol. 41, no. 1. p. 50

[35] MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. 2004, vol. 19, no. 1. p. 4.

[36] HALLIDAY, S., BADENHORST, K. y VON SOLMS, R.A business approach to effective information technology risk analysis and management. En: LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Diiembre, 2006, vol. 2006, no. 12. p. 17

[37] WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. 2005, vol. 24. p. 17

[38] PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. 2007, vol. 16, no. 1. p. 339

este es restringido o seriamente perturbado, entonces la organización puede deteriorarse o incluso morir.

Moore[39] (1997) afirma en un documento publicado por la UNESCO desde hace ya casi una década como la información afecta desde finales del siglo XX la vida económica, social, cultural y política de los países del mundo. Además, presenta tres características principales de la sociedad de la información. En primer lugar, la información como un recurso económico; segunda, un mayor uso de la información por el público en general; y la tercera característica, el desarrollo del sector de la información en la economía, con la función de satisfacer la demanda global o servicios de información, lo que conlleva que, una parte significativa de la industria se centre en la infraestructura de la tecnología, por ejemplo, las telecomunicaciones, sector que está creciendo más rápido que la economía en general.

Respecto a la relación entre información y conocimiento, el conocimiento es más que información y datos. Este puede ser descrito como la "mezcla fluida de experiencias enmarcadas, valores, información contextualizada y la visión de expertos"[40]. El conocimiento es indispensable para la innovación y se manifiesta en forma de activos intangibles y tangibles de conocimiento. Los activos intangibles de conocimiento se plasman en los seres humanos, mientras que los activos tangibles de conocimiento se integran con el tiempo en los procedimientos, rutinas, procesos y documentos de la organización[41]. Dado el entorno de negocios altamente competitivo y la presión continua en la que las organizaciones compiten, los activos de conocimiento son vitales para que las organizaciones mantengan su ventaja

[39] MOORE, Nick. Chapter 20. The information society. En: World Information. Report 1997/98. UNESCO Publishing. Quétigny (Francia): Yves Courrier. 1997. p. 271-284. ISBN 92-3-103341-7

[40] DAVENPORT, Thomas H. y PRUSAK, Lawrence. Working knowledge: how organizations management what they know. En: Harvard Business School Press, Boston. 1998

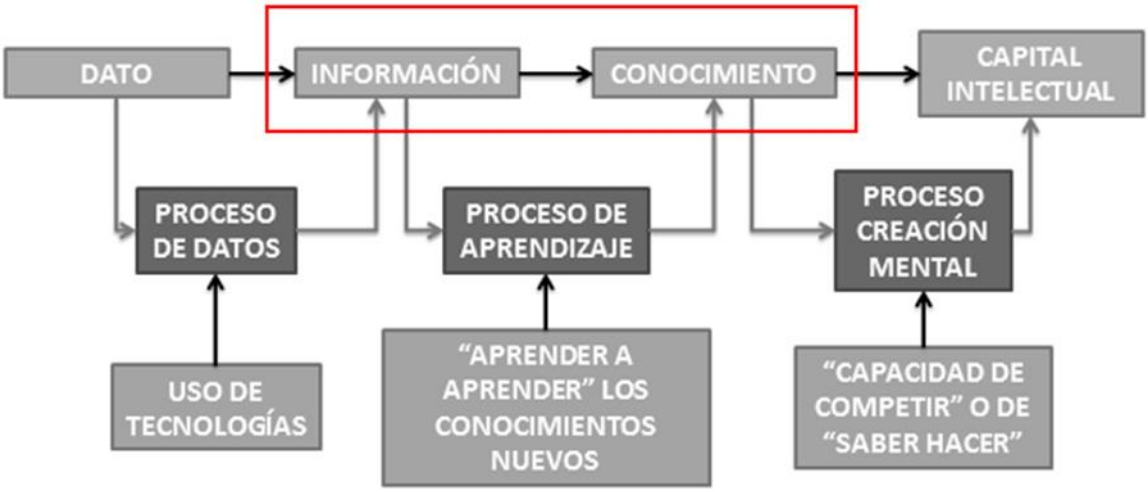
[41] AHMAD, Atif; BOSUA, Rachelle y SCHEEPERS, Rens. Protecting organizational competitive advantage: A knowledge leakage perspective. En: computers & security. Mayo, 2014, vol. 42. p 27-39

competitiva[42] [43]. Para diferenciar información de conocimiento, uno de los modelos frecuentemente citados es la pirámide de Russell Ackoff[44]. La cimentación de esta estructura se asienta directamente sobre los datos, a partir de los cuales se van superponiendo la información, el conocimiento, el entendimiento y la sabiduría.

Sin embargo, existen otras definiciones, una de ellas es de Bueno[45], quien se centra en el proceso de creación de capital intelectual. En este modelo la información es la materia prima, y el conocimiento puede ser ya considerado como el producto final[46]. De este modo, las personas reciben como *input* la información construida a través de los datos y, tras su análisis, obtienen como *output* el conocimiento; que una vez usado se convierte en el capital intelectual de la organización, es decir, cuando se suma el conocimiento de los miembros y la interpretación práctica del mismo (ver Ilustración 1). La diferencia clave entre el conocimiento y la información es que el conocimiento nos da poder para tomar decisiones[47].

[42] GRANT, Robert M. Toward a knowledge-based theory of the firm. En: Strategic Management Journal. Vol. 17 (Edición especial de invierno,1996); p. 110
[43] GRANT, Robert M. The knowledge-based view of the firm: Implications for management practice. En: Long Range Planning. 1997, vol. 30, no. 3. p. 450-454
[44] ACKOFF, Russell. L. From Data to Wisdom. En: Journal of Applied Systems Analysis. 1989, vol. 16. p. 3-9.
[45] BUENO, Eduardo. La gestión del conocimiento: nuevos perfiles profesionales. [En línea]. (1999). [Consultado el 6 de agosto de 2012]. Disponible en <http://www .sedic.es/bueno.pdf>
[46] RENDÓN, Miguel. Relación entre los conceptos: información, conocimiento y valor. Semejanzas y diferencias. En: Ciência da Informação, Brasília. Vol. 34, No. 2 (2005); p. 53.
[47] FIGUEROLA, Norberto. Gestión del Conocimiento (Knowledge Management) Pirámide D-I-K-W. [En línea]. (2013). [Consultado el 25 de mayo de 2014]. Disponible en <http://articulospm.files.wordpress.com/2013/08/gestic3b3n-de-conocimiento-dikw.pdf>

Ilustración 1. Proceso de creación del capital intelectual



Fuente: Autora del proyecto. Adaptado de BUENO, Eduardo. La gestión del conocimiento: nuevos perfiles profesionales. [En línea]. (1999). [Consultado el 6 de agosto de 2012]. Disponible en <http://www .sedic.es/bueno.pdf>

Partiendo de la necesidad de fomentar una gestión para el conocimiento y la información, y siendo el conocimiento uno de los recursos estratégicos más valiosos y una herramienta para generar valor en las organizaciones, a lo que Grant[48] llama la visión basada en el conocimiento, y otros autores lo llaman "economía basada en el conocimiento"[49] [50] [51]; se busca entonces, que dicho conocimiento esté disponible y accesible para quien necesite hacer uso de el mismo.

[48] GRANT, Robert M. Prospering in dynamically-competitive environments: organizational capability as knowledge integration. En: Organization Science. Julio-Agosto, 1996, vol. 7, no. 4. p. 375-387

[49]MORTAZAVI, S. Habib y BAHRAMI, Mahdi. Integrated approach to entrepreneurship – knowledge based economy: a conceptual model. En: Procedia – Social and Behavioural Sciences. Vol. 41 (2012); p. 283.

[50]SABAU, Gabriela. Know, live and let live: towards a redefinition of the knowledge-based economy – sustainable development nexus. En: Ecological Economics. Vol. 69, No. 6 (Abr. 2010); p. 1193.

[51] GRANT, Robert M. Prospering in dynamically-competitive environments: organizational capability as knowledge integration. En: Organization Science. Julio-Agosto, 1996, vol. 7, no. 4. p. 375-387

Por otra parte, el creciente desarrollo de internet y herramientas de tecnologías de información y comunicación –TIC- para facilitar e impulsar cada vez los procesos de generación, codificación y transferencia del conocimiento dentro de una organización, ha dado lugar a lo que hoy en día se conoce como Sistemas de Gestión de Conocimiento (*Knowledge Management System*, KMS por sus siglas en ingles), definidos en la literatura como "herramientas, tecnologías o software diseñados para soportar los procesos de gestión del conocimiento" [52] [53] [54] [55] [56] [57] [58].

Como afirma McPherson[59], "la información es vital para el éxito del negocio y será responsable de una parte significativa de los diversos indicadores de la empresa de éxito, incluyendo su flujo de caja y el valor de mercado". Sin embargo, Doherty[60] dice que tales beneficios no se obtienen sólo usando la información, sino también haciendo uso de sistemas y tecnologías de la información que deben ser aplicados de una manera enfocada y sistemática. Por tal razón, las TIC se consideran un facilitador de la gestión del conocimiento, ellas permiten una mejor comunicación y

[52] VON KROGH, Georg. Care in Knowledge Creation. En: California Management Review. 1998, vol. 40, no. 3. p. 133-154

[53] ORGLAND, Magne y VON KROGH, Georg. Initiating, Managing and Sustaining Corporate Transformation: A case Study. En: European Management Journal. 1998, vol. 16, no. 1. p. 31-38

[54] CROASDELL, David; JENNEX, Murray; ZHIHONG, Yu; CHRISTIANSON, Tony; CHAKRADEO, Meenal y MAKDUM, Wagas. A meta-analysis of methodologies for research in knowledge management, organizational learning and organizational memory: five years at HICSS. En: System Sciences. Proceedings of the 36th Hawaii intl conf on system sciences, 2003. Disponible en: http://www.computer.org/csdl/proceedings/hicss/2003/1874/04/187440110a-abs.html

[55] BARONI DE CARVALHO, Rodrigo y TAVARES FERREIRA, Marta. Using information technology to support knowledge conversion processes. En: Information Research. 2001, vol. 7, no. 1

[56] BENBYA, Hind; PASSIANTE, Giuseppin y AISSA, Nassi. Corporate portal: a tool for knowledge management synchronization. En: International Journal of Information Management. Junio, 2004, vol. 24, no. 3. p. 201-220. Disponible en: http://choo.fis.utoronto.ca/fis/courses/lis2102/Readings/benbya.pdf

[57] NEVO, Dorit y CHAN, Yolande E. A Delphi study of knowledge management systems: Scope and requirements. En: Information & Management. Septiembre, 2007, vol. 44, no. 6. p. 583–597.

[58] RICHARDSON, Sandra; COURTNEY, James y HAYNES, John. Theoretical principles for knowledge management system design: application to pediatric bipolar disorder. En: Decision support systems. 2006, vol. 42, no. 3. p. 1321-1337

[59] McPHERSON, P.K. The inclusive value of information. En: International Federation for Information and Documentation – 48th congress. Graz, 1996. p. 41–60.

[60] DOHERTY, Neil Francis; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: A critical study of the content of university policies. En: International Journal of Information Management. 2009, vol. 29, no. 6. p. 449–457

flujo del conocimiento en la organización. Tanto es así que algunos autores como Khandelwal y Gottschalk[61] señalan que *"la aplicación de las TIC para el apoyo de la gestión del conocimiento influye en los resultados, en la creación y transferencia de conocimientos en la organización".* Por otra parte, Sher y Lee[62] sugieren que tanto los conocimientos endógenos como los exógenos son efectivamente manejables a través de la aplicación de TIC, lo cual posibilita incrementar la capacidad dinámica de la organización.

Sin embargo, garantizar la seguridad de la información corporativa que se almacena, procesa y difunde a través de las TIC, se ha convertido en una actividad sumamente compleja y desafiante. Esta es una preocupación muy importante para las organizaciones intensivas en conocimiento, como las universidades[63]. Por ejemplo, en el caso colombiano, las Instituciones de Educación Superior –IES- quienes enfrentan retos con relación al uso responsable y seguro de la información, el conocimiento y las nuevas tecnologías, porque tanto los procesos de gestión administrativa como el proceso de enseñanza y las actividades de investigación son cada vez más dependientes de la disponibilidad, integridad y exactitud de los recursos de información. Según la opinión de Rodríguez[64] dado que la mayor parte de la información esta soportada sobre las TIC, la mejor manera de asegurarla es mediante el uso de las propias TIC[65].

---

[61] KHANDELWAL, Vijay y GOTTSCHALK, Petter. Information technology support for interorganizational knowledge transfer: an empirical study of law firms in Norway and Australia. En: Information resources management journal. 2003, vol. 16, no. 1. p. 14-23

[62] SHER, Peter y LEE, Vivid. Information technology as a facilitator for enhancing dynamic capabilities through knowledge management". En: Information & management. 2004, vol. 41, no. 8. p. 933-945

[63] DOHERTY; ANASTASAKIS y FULFORD, The information security policy unpacked: A critical study of the content of university policies, Op. cit.

[64] Jefe del área de seguridad e integración de Sistemas de la Dirección General de Informática del gobierno del Principado de Asturias.

[65] LABIANO, Javier. Las TIC en la Seguridad y Protección de Datos. [En línea]. Marzo (2009). [Consultado el 10 Junio de 2013]. Disponible en <http://www.socinfo.info/contenidos/pdf56mar09/p14-25datos.pdf>

Según, Ward y Peppard [66] el desafío real es garantizar que la información sea de la mejor calidad posible, especialmente en términos de exactitud, integridad, confianza en la fuente, fiabilidad y conveniencia. Desafortunadamente, en la práctica, muchas organizaciones no proporcionan de forma coherente los activos de información con la alta calidad que sus directivos requieren, debido a altos niveles de violación de seguridad que experimentan[67]. Por ejemplo, Austin y Darby[68], señalan que en los Estados Unidos "las brechas de seguridad afectan a 90% de todos los negocios cada año, y cuestan alrededor de $17 mil millones de dólares", y las medidas de protección llegan a ser muy costosas: «una empresa promedio puede gastar fácilmente entre un 5% -10% de su presupuesto de TI en seguridad". Por tanto, uno de los mecanismos importantes para proteger la información corporativa, en un intento de detectar, prevenir y responder a las violaciones de seguridad es a través de la formulación y aplicación de una política de seguridad de la información[69] [70].

La literatura en Gestión de Seguridad de la Información –GSI- sugiere una serie de controles formales, informales y técnicas para salvaguardar la confidencialidad, así como la integridad y la disponibilidad[71]. Los controles formales incluyen las evaluaciones de riesgo, las auditorías, las políticas y procedimientos, y el esquema de medidas ejemplares en caso de incumplimientos, entre otros. Los controles técnicos son *firewalls*, sistemas de detección de intrusos, y otros dispositivos que regulan el acceso a los recursos, mientras que los controles informales incluyen la capacitación y la educación que influyen en la cultura de seguridad.

---

[66] WARD y PEPPARD. Op. cit.
[67] GARG Ashish; CURTIS Jeffrey y HALPER Hilary. Quantifying the financial impact of Information technology security breaches. En: Information Management and Computer Security. 2003, vol. 11, no. 2. p. 74–83
[68] AUSTIN, Robert D. y DARBY, Christopher A.R. The myth of secure computing. En: Harvard Business Review. Junio, 2003, vol. 81, no. 6. p.121–126
[69] HONE, Karin and ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers and Security. Octubre, 2002, vol. 21, no. 5. p. 402–409
[70] VON SOLMS, Basie y VON SOLMS, Rossouw. The ten deadly sins of information security management. En: Computers and Security. 2004, vol. 23, no. 5. p. 371–376
[71] DHILLON, Gurpreet. Principles of Information Systems Security: text and cases. 1 ed. New York: John Wiley and Sons, 2007. 464 p. ISBN 978-0471450566

En este sentido, las compañías empezaron a investigar los aspectos relacionados con mejores prácticas en seguridad de la información, y empiezan a preocuparse por conocer los principales componentes de un buen plan de seguridad, entonces aparecen nuevos intereses como establecer políticas de seguridad, evaluar la seguridad de la información frente a las partes interesadas mediante monitoreo y medición, obtener algún tipo de certificación oficial, entre otros[72]. Además, el rol del empleado como usuario final de la información llama la atención y con esto cobra importancia el empleado en este proceso, conduciendo por tanto a una estandarización de la seguridad de la Información en las organizaciones, haciendo evidente que la seguridad de la información está constituida por varias dimensiones interrelacionadas, y no solamente una dimensión técnica como se había creído en un comienzo[73].

Por tanto, empieza a tomar relevancia la concienciación en seguridad de la información, dado que un trabajador desinformado acerca de los riesgos de seguridad puede poner en peligro la ventaja competitiva de la organización[74]. No obstante, a pesar de la creciente preocupación de profesionales y académicos por la ausencia de una base teórica y un acercamiento formal a la gestión de seguridad de la información, la investigación relacionada con el factor humano ha sido

[72] VON SOLMS, Bassie. Information Security: the fourth wave. En: Computers & Security. Vol. 25, No. 3 (May. 2006); p. 165.
[73] VON SOLMS, Bassie. Op. Cit.
[74] HONG, Kwo-Shing, et al. An integrated system theory of information security management. En: Information Management & Computer Security. 2003, vol. 11, no. 5. p. 243

limitada[75]. Con excepciones en temas como la generación de contraseñas[76] [77] y la investigación empírica sobre las conductas en los usuarios de la información y los factores que influyen en ellas[78]. Lo anterior, en parte porque la tecnología es a menudo falsamente percibida como la respuesta inmediata a los problemas de seguridad de la información[79], y se ha subestimado que la seguridad de la información es ante todo un problema de factores humanos que no se ha resuelto[80], y que según Deloitte[81], se declara abrumadoramente como la mayor debilidad de la seguridad (86%), seguido por la tecnología (63%).

En este sentido, dado que los individuos son el factor común al sistema de gestión de la seguridad de la información y a la Visión Basada en el Conocimiento[82], puesto que, por una parte son ellos los mayores responsables de la cantidad de eventos potenciales de riesgo asociados a los procesos de gestión de información, y por otra parte, son ellos también el principal repositorio de conocimiento, las proposiciones con las que se pretendió responder a la pregunta de investigación de este estudio fueron: *"La gestión de seguridad de la información sirve para para la mejora de los*

[75] METALIDOU, Efthymia; MARINAGI, Catherine; TRIVELLAS, Panagiotis; EBERHAGEN, Niclas; SKOURLAS, Christos y GIANNAKOPOULOS, Georgios. The Human Factor of Information Security: Unintentional Damage Perspective. En: Procedia - Social and Behavioral Sciences. Agosto, 2014, vol. 147, no. 25, p. 424-428, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2014.07.133. Disponible en: http://www.sciencedirect.com/science/article/pii/S1877042814040440

[76] AHMED, Fawad y SIYAL, M.Y. A novel approach for regenerating a private key using password, fingerprint and smart card. En: Information Management & Computer Security. 2005, vol. 13, no. 1, p. 39-54.

[77] SHENG, Weiguo; HOWELLS, Gareth; FAIRHURST, Michael; DERAVI, Farzin y CHEN, Shengyong. Reliable and secure encryption key generation from fingerprints. En: Information Management & Computer Security. 2012, vol. 20, no. 3, p. 207 – 221.

[78] HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008. Dissertation (Doctor of Philosophy). University of New York. Faculty of the graduate school. p. 9.

[79] HINSON, Gary. Human factors in information security. En: NoticeBored is a service from IsecT Ltd. 2003. [En línea]. (Recuperado en 22 agosto 2017). Disponible en http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf. Citado por: METALIDOU, Efthymia; *et al.* Op. cit.

[80] SCHULTZ, Eugene. The human factor in security. En: Computers & Security, 2005, vol. 24, no 6, p. 425-426.

[81] Deloitte Touche Tohmatsu. Protecting what matters. The 6th Annual Global Security Survey. 2009. (Recuperado en 22 agosto 2017). Disponible en: https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf

[82] GRANT, Robert M. Towards a knowledge-based view of the firm. En: Strategic Management Journal. Diciembre, 1996. Vol. 17, p. 109–122

procesos de gestión del conocimiento en las áreas administrativas de las Instituciones de Educación Superior" y, *"la utilización de tecnologías de información de forma controlada y segura favorece la gestión del conocimiento"*.

Teniendo en cuenta que, una vez resuelta la pregunta, se mitiga el riesgo de que el conocimiento se pierda, ya sea por fuga[83], por el envejecimiento de la fuerza de trabajo[84], por fallas de confidencialidad y pase a manos de la competencia; o se vuelva en su defecto obsoleto, considerando que, el conocimiento debe hacerse presente en el momento justo en el que se necesita, para ser aplicado en el contexto adecuado, de la manera correcta, por cualquier persona que lo requiera, para que sea oportuno en la toma de decisiones, diseño, planeación, diagnóstico, análisis y evaluación.

Lo anterior, sugiere entonces que las organizaciones que desean seguir siendo competitivas podrían desarrollar mecanismos para captar el conocimiento pertinente y difundirlo de manera precisa, consistente o íntegra y oportuna a quien lo necesite[85]. Lo cual implica un proceso de identificación y valoración que permita saber cuál es el conocimiento estratégico, y se defina el interés en protegerlo, aprovecharlo y generar a través de él valor para la organización[86].

[83] MA, Zhenzhong; QI, Liyun; WANG, Keyi. Knowledge sharing in Chinese construction project teams and its affecting factors: an empirical study. Chinese Management Studies, 2008, vol. 2, no 2, p. 97-108.
[84] MARTIN, Angela. Talent Management: Preparing a "Ready" agile workforce, International Journal of Pediatrics and Adolescent Medicine, Volume 2, Issues 3–4, September–December 2015, Pages 112-116, ISSN 2352-6467, http://dx.doi.org/10.1016/j.ijpam.2015.10.002.
[85] BOLLINGER, Audrey S.; SMITH, Robert D. Managing organizational knowledge as a strategic asset. En: Journal of knowledge management, 2001, vol. 5, no 1, p. 8-18.
[86] LOPERA LONDOÑO, Maria Eugenia y QUIROZ GIL, Nora Ledis (2013). Caracterización de un modelo de gestión del conocimiento aplicable a las funciones universitarias de investigación y extensión: Caso Universidad CES. Tesis de maestría en dirección, Universidad CES – Universidad del Rosario, Medellín.

2. DISEÑO METODOLÓGICO

Algunas fuentes bibliográficas mencionan la importancia de la protección del conocimiento en las organizaciones[87] [88] [89] [90], pero no proporcionan orientación sobre 1) los diferentes tipos de mecanismos necesarios para proteger el conocimiento sensible, y 2) las directrices estratégicas y operativas sobre cómo se puede proteger el conocimiento organizativo sensible. En este contexto, Según, Desouza y Vanapalli[91] el interés en el campo de la gestión del conocimiento sigue creciendo a una velocidad asombrosa, y con el tiempo este campo se hace más dinámico y complejo. Sin embargo, Desouza y Vanapalli[92] señalan que hay muchos estudios que abordan cómo se debe aprovechar los activos de conocimiento, pero el trabajo sobre cómo se puede asegurar estos activos y los procesos de conocimiento existentes es escaso.

En este orden de ideas, y teniendo en cuenta que la gestión de conocimiento ha sido implementada en las organizaciones con el objetivo de lograr mayor ventaja competitiva, existe la necesidad de conciliar la preservación de la confidencialidad del conocimiento con el fin de mantener estas ventajas. Algunas fuentes bibliográficas mencionan la importancia de la protección del conocimiento en las

---

[87] BLOODGOOD, James M. y SALISBURY, Wm. David. Understanding the influence of organizational change strategies on information technology and knowledge management strategies. En: Decision Support Systems - Knowledge management support of decision making. Mayo, 2001, vol. 31, no. 1. p. 55-69

[88] GOLD, Andrew H.; MALHOTRA, Arvind y SEGARS, Albert H. Knowledge management: an organizational capabilities perspective. En: Journal of Management Information Systems. Summer, 2001, vol. 18, no. 1. p. 185-214

[89] O'DONOGHUE, Nathan y CROASDELL, David T. Protecting knowledge assets in multinational enterprises: a comparative case approach. En: VINE. Octubre, 2009, vol. 39, no. 4. p. 298-318. ISSN: 0305-5728

[90] THOMPSON, E. Dale y KAARST-BROWN, Michelle L. Sensitive Information: a review and research agenda. En: Journal of the American Society for Information Science and Technology. Febrero, 2005, vol. 56, no. 3. p. 245-257

[91] DESOUZA, Kevin C. y VANAPALLI, Ganesh K. Securing knowledge in organizations: lessons from the defense and intelligence sectors. En: International Journal of Information Management. Febrero, 2005, vol. 25, no. 1. p. 85-98.

[92] Ibid, p. 85.

organizaciones[93] [94] [95] [96], pero no proporcionan orientación sobre 1) los diferentes tipos de mecanismos necesarios para proteger el conocimiento sensible, y 2) las directrices estratégicas y operativas sobre cómo se puede proteger el conocimiento organizativo sensible[97] [98] [99] [100]. Por tanto, es necesario alinear las prácticas de gestión de seguridad de la información a los procesos de gestión del conocimiento. Lo anterior, considerando que, en la literatura, en el área de la gestión de seguridad de la información el concepto de "conocimiento" no es muy usado, sino más bien el de información (y datos)[101]. Lo cual se convierte en un dilema clave para las organizaciones, y constituye la justificación de proponer un modelo de gestión de seguridad del conocimiento guiado a través de la gestión de la seguridad de la información, dado que “la información es la base fundamental sobre la cual la seguridad desarrolla su dinámica y propone las acciones de protección”[102].

Para el logro del general objetivo planteado en este estudio, se establecieron los siguientes objetivos específicos: 1) Realizar una revisión de literatura que permita identificar los determinantes de la gestión de seguridad del conocimiento en Instituciones Públicas de Educación Superior; 2) Caracterizar los procesos de gestión del conocimiento dentro del contexto administrativo realizados en las

[93] BLOODGOOD y SALISBURY. Op. cit.
[94] GOLD, MALHOTRA y SEGARS. Op. cit.
[95] O'DONOGHUE y CROASDELL. Op. cit.
[96] THOMPSON y KAARST-BROWN. Op. cit.
[97] DESOUZA, Kevin C. Knowledge Security: an interesting research space. En: Journal of Information Science and Technology. 2006, vol. 3, no. 1. p. 85-98. Citado por: AHMAD, BOSUA y SCHEEPERS. Op. cit.

[98] DESOUZA y VANAPALLI. Op. cit. Citado por: AHMAD, BOSUA y SCHEEPERS. Op. cit.
[99] EASTERBY-SMITH, Mark; LYLES, Marjorie A. y TSANG, Eric W. K. Inter-Organizational Knowledge Transfer: Current Themes and Future Prospects. Journal of Management Studies. Junio, 2008, vol. 45, no. 4. p. 677-690. Citado por: AHMAD, BOSUA y SCHEEPERS. Op. cit.
[100] TRKMAN y DESOUZA. Op. cit. Citado por: AHMAD, BOSUA y SCHEEPERS. Op. cit.
[101] SHEDDEN, P.; SCHEEPERS, R.; SMITH, W. y AHMAD, A. Incorporating a knowledge perspective into security risk assessment. En: VINE Journal Knowledge Management. 2011, vol. 41, no. 2. p. 152-166.
[102] LACEY, David. Managing the human factor in information security: how to win over staff and influence business managers. Chichester: John Wiley & Sons, 2009. 384 p. ISBN: 978-0-470-72199-5. p. 15-16.

Instituciones Públicas de Educación Superior colombianas para identificar los activos clave de conocimiento; 3) Analizar las vulnerabilidades y amenazas de los activos identificados en el proceso de gestión del conocimiento para determinar su nivel de riesgo en la organización; 4) Formular un plan de implementación del modelo propuesto para la gestión de seguridad de los activos de conocimiento clave que impactan los procesos administrativos de la Universidad Industrial de Santander.

El posicionamiento epistemológico para el desarrollo de esta investigación es interpretativista, de tipo cualitativa y un enfoque inductivo. La metodología implementada consta de cuatro fases, las cuales son:

1. Revisión sistemática de la literatura
2. Caracterizar el proceso de gestión de conocimiento
3. Análisis de la madurez en gestión de conocimiento y gestión de seguridad de la información
4. Establecimiento del modelo

2.1 FASE I: REVISIÓN SISTEMÁTICA DE LA LITERATURA

La revisión sistemática realizada tuvo como base elementos metodológicos definidos por Rashman et al.[103] y Tranfield et al.[104], con el fin de obtener resultados transparentes, científicos y replicables. En primer lugar, se realizó un protocolo para planificar y orientar el proceso descrito en el Anexo 1. La fuente de información para búsqueda de documentos fue la base de datos *Social Sciences Citation Index* (SSCI) de la *ISI Web of Knowledge,* la cual es una de las bases de referencia internacional por su contenido de artículos de calidad y traslape de

[103] RASHMAN, Lyndsay; WITHERS, Erin; HARTLEY, Jean. Organizational learning and knowledge in public service organizations: A systematic review of the literature. En: International Journal of Management Reviews, 2009, vol. 11, no 4, p. 463-494.

[104] TRANFIELD, David; DENYER, David y SMART, Palminder. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. En: British Journal of Management, 2003, Vol.14, No.3, p.207-222.

cerca del 80% con la base de datos Scopus[105], seleccionada debido a que comprende revistas especializadas de calidad en las ciencias sociales y además es una de las más importantes e influyentes del mundo[106] [107]. Sólo artículos científicos fueron tenidos en cuenta debido a su mayor rigurosidad respecto a otros documentos. Segundo, se diseñó una ecuación de búsqueda que fue definida después de un proceso iterativo de identificación de principales palabras clave y la asesoría de expertos. La ecuación de búsqueda fue: TITLE: ("information security management" OR "intellectual capital security" OR "knowledge security"). Timespan=2001-2014. Indexes=SCI-EXPANDED, SSCI, A&HCI. En total se obtuvieron un total de 57 resultados.

Los artículos encontrados se analizaron a través del software de minería de datos *vantage point* ®, y fueron filtrados por título, resumen e introducción evaluando su pertinencia hacia los objetivos principales del protocolo; por lo que, en algunos casos se realizó la lectura completa de los resultados y conclusiones de los documentos recuperados más relevantes. También se utilizó el seguimiento de citaciones o método bola de nieve[108], en inglés "*citation pearl growing*", como técnica para identificar documentos seminales para la investigación. Esto permitió añadir 46 documentos más, 7 estudios sugeridos por expertos de la *Sociedade Brasileira de gestão do conhecimento*, y adicionalmente la tesis de doctorado facilitada por Wagner Junqueira, titulada *A segurança do conhecimento nas*

[105] MARTÍNEZ, Álvaro Javier, FORERO, Diana Magally, PINTO PRIETO, Laura Patricia y BECERRA ARDILA, Luis Eduardo. Ponencia titulada: Análisis bibliométrico de la producción científica acerca de técnicas de adquisición y representanción de conocimiento a través del Social Science Citation Index (2001-2013).

[106] TESTA, James. (1998) La base de datos del ISI y su proceso de selección de revistas. [versión online] Disponible en: http://www.bvs.sld.cu/revistas/aci/vol9_s_01/sci23100.htm. Consultado en 29 de septiembre de 2016. Trabajo originalmente publicado por el ISI en formato electrónico: (URL: http://www.isinet.com) y presentado en el Seminario sobre Evaluación de la Producción Científica, realizado en São Paulo por el Proyecto SciELO, del 4 al 6 de marzo de 1998.

[107] LIM, Kwanghui. The relationship between research and innovation in the semiconductor and pharmaceutical industries (1981–1997). En: Research Policy. Vol. 33 (2004); pág. 287–321 [citado en 10 de octubre de 2015] Disponible en Elsevier Research Databases.

[108] DOLAN, Paul, et al. QALY maximisation and people's preferences: a methodological review of the literature. En: Health economics, 2005, vol. 14, no 2, p. 197-208.

práticas da gestão da segurança da informação e da gestão da conhecimento.

Esta revisión de literatura se realizó a través del uso de métodos mixtos, es decir, análisis de contenido[109] y análisis estadístico[110], es decir, no sólo se identificaron tendencias de publicación, principales autores, revistas sino además se codificaron y analizaron los diversos elementos de los documentos con el apoyo del software de análisis cualitativo de datos MAXQDA ®. Finalmente, el reporte de la revisión sistemática fue construido, y actualizado en el transcurso de la investigación.

2.2 FASE II: ANÁLISIS DE LOS MODELOS DE GESTIÓN DE CONOCIMIENTO Y SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR COLOMBIANAS

En esta fase se buscó estudiar las características del contexto colombiano, reconociendo si existen modelos que faciliten la gestión del conocimiento y la información en las instituciones públicas de educación superior colombianas[111], y conociendo la forma como esta se está llevando a cabo la seguridad de los activos intangibles. Para esto, se realizó un diagnóstico general a través del diseño y aplicación del cuestionario titulado “Cuestionario para valorar la gestión y seguridad del conocimiento y la información en las organizaciones de servicios” (Ver Anexo 2).

Este cuestionario se constituía de 26 preguntas, donde las primeras dos eran de

[109] «es una técnica de investigación para la descripción objetiva, sistemática y cuantitativa del contenido manifiesto de las comunicaciones, teniendo como fin interpretarlos» Tomado de: PINTO, R.; GRAWITZ, M. (1967). Analyse de contenu et theorie. En: Méthodes des sciences sociales. Dalloz. Paris. p. 456-499.

[110] LU, Weisheng, et al. A decade's debate on the nexus between corporate social and corporate financial performance: a critical review of empirical studies 2002–2011. Journal of Cleaner Production, 2014, vol. 79, p. 195-206.

[111] Definidas en el capítulo IV de la Ley 30 de Diciembre 28 de 1992 y en el artículo 213 de la Ley 115 de 1994.

contexto, 3 y 4 sobre el concepto de conocimiento y gestión del conocimiento, de la 5 a la 9 el proceso o área de la organización en la cual se generaba el mayor volumen de conocimiento importante, de la 10 a la 13, la importancia y asignación de recursos que da la institución a los procesos de gestión del conocimiento, la pregunta 14 indagaba sobre el papel de las TIC en la gestión del conocimiento, de la 15 a la 25 los aspectos relacionados con la seguridad del conocimiento y las buenas prácticas de seguridad de la información. Finalmente, la pregunta 26 permitía hacer observaciones que contribuyeran al diseño del modelo de gestión de seguridad de la información y el conocimiento.

El cuestionario fue construido a partir de: (i) la encuesta sobre percepciones de la gestión del conocimiento: comparaciones y contrastes aplicada a empresarios en la ciudad de Bogotá en el año 2007 basada principalmente en el estudio exploratorio de Rodney McAdam y Renee Reid (1999) de la percepción del conocimiento en pequeñas y grandes empresas de la ciudad de Londres, Inglaterra; así como además, la encuesta desarrollada por el profesor Carlos Blanco PhD, y el Ingeniero Jose Obagui de la universidad Javeriana[112]; y otros autores como Barker and Barker, 1997; Nonaka and Takeuchi, 1995; y Demarest, 1997; (ii) el documento "*Metodologia de implantação da gestão do conhecimento no Governo de Minas Gerais*" (Instituto de Pesquisa Económica Aplicada, 2013) y (iii) el cuestionario para la valoración de seguridad del capital intelectual en grupos de investigación (Cárdenas y Contreras, 2012). Teniendo en cuenta aspectos propios de la cultura institucional colombiana, algunas preguntas desarrolladas en el cuestionario fueron adaptadas para una mejor comprensión.

Este cuestionario fue aplicado vía web en el período junio-diciembre de 2015 tanto

[112] ESCOBAR BARRETO, Carmen Liliana. Percepción sobre la gestión del conocimiento en la empresa de telecomunicaciones Comcel S.A. Facultad de administración de empresas de la Universidad de la Salle (2008), 105 p. Disponible en: http://repository.lasalle.edu.co/bitstream/handle/10185/4277/T11.08%20E18p.pdf?sequence=1

a la comunidad UIS (Ver Anexo 3) como a la base de datos de contactos de instituciones de educación superior del país facilitada por el proyecto GEFIES[113] y otras organizaciones de servicios como centros de investigación, corporaciones, parques tecnológicos, entidades bancarias, y Centros de Apoyo a la Tecnología y la Innovación -CATI (Ver Anexo 4. Base de datos de IES Públicas Colombianas y otras Organizaciones de Servicios). En total se recolectaron 91 respuestas, de las cuales 86 completaron la mayoría de las preguntas. De estas 86 personas, 12 respuestas corresponden a empleados de entidades bancarias, 13 a organizaciones prestadoras de servicios y 61 a instituciones de educación superior. Tras la recopilación de los resultados, se procedió a complementar a través de la revisión y análisis de documentos que reportan información relacionada con modelos de medición del capital intelectual, metodologías para la evaluación del capital intelectual (Ver Anexo 5. Modelos de medición del capital intelectual), modelos de gestión del conocimiento y las tendencias de las tres últimas encuestas realizadas en Latinoamérica de seguridad de la información realizadas por ACIS[114], CSIRT[115] e ISACA® [116].

Por último, para identificar los activos de conocimiento se utilizó el modelo *Technology Broker* creado por Annie Brooking (1997), ya que era el que más se ajustaba a la realidad de la institución y el que permitía tener un panorama más claro sobre su situación actual. No se optó por utilizar modelos como el *Balanced*

[113] GESTIÓN FINANCIERA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS EN COLOMBIA (GEFIES): Proyecto realizado en 2013 por el Ministerio de Educación con el apoyo de la Universidad Industrial de Santander, líder del proyecto «Towards Sustainable Financial Management Of Universities In Latin America – SUMA»

[114] Asociación Colombiana de Ingenieros de Sistemas. ACIS realiza año a año la Encuesta Latinoamericana de Seguridad de la Información, que este año (2017) llega a su versión número 9, investigación neutral y académica, que busca conocer y medir la realidad de la seguridad de la información en los países latinoamericanos y con ello construir referentes regionales sobre esta temática.

[115] Centro de Coordinación Seguridad Informática Colombia, dedicados a la gestión de incidentes de seguridad informática y de telecomunicaciones

[116] *Information Systems Audit and Control Association* - Asociación de Auditoría y Control de Sistemas de Información

Scorecard o el navegador de Skandia, porque en el momento de realizar el diagnóstico, la institución no contaba con una cantidad de indicadores que permitieran que a través de estos modelos se pudiera tener una visión lo suficientemente amplia de la situación actual y obtener los resultados que se necesitaban para generar posteriormente el plan de implementación del modelo de gestión de seguridad del conocimiento.

2.3 FASE III: ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL CONOCIMIENTO EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

Para el desarrollo de esta fase se tuvo en cuenta dos aspectos claves en la organización que afectan la seguridad del conocimiento y son; en primer lugar, la cultura (implica los recursos humanos) y, en segundo lugar, la memoria institucional (lecciones aprendidas que reposan en el ser humano), ambas relacionadas con la incidencia de las acciones de las personas en la sistematización segura de la información y la conservación de la memoria institucional[117]. Según lo anterior, para este análisis se fue consciente que la seguridad comienza y termina con cada persona involucrada con la infraestructura física y de TI (Tecnología de Información), ya que, la imprevisibilidad (o previsibilidad) del comportamiento humano puede convertir los sistemas de información más seguros en algo inexistente[118].

En vista de lo anterior, para la consolidación y ejecución de esta investigación, se plantea una metodología de Investigación Acción Participativa – IAP - que permita trabajar mancomunadamente junto con la comunidad un diagnóstico social participativo, basado en el principio de Comte: “conocer para actuar”, priorizando problemas y definiendo estrategias eficaces, que propician además de un

[117] METALIDOU, Efthymia, et al. The human factor of information security: Unintentional damage perspective. Procedia-Social and Behavioral Sciences, 2014, vol. 147, p. 424-428.
[118] ORSHESKY, Christine M. Beyond technology–The human factor in business systems. Journal of business strategy, 2003, vol. 24, no 4, p. 43-47.

aprendizaje activo, participativo y cooperativo, el desarrollo de buenas prácticas de gestión de seguridad de la información, de manera que se logre un impacto favorable en la comunidad, se fortalezca el proceso de gestión de conocimiento en cada área académico administrativa, se logre mantener una cultura donde se valoren los comportamientos positivos de seguridad y se entienda como resolver los desafíos asociados con la seguridad de la información que los funcionarios/personal que labora en la UIS enfrentan a diario.

El proceso metodológico está planteado por cuatro etapas basadas en los documentos de IAP del autor Rodríguez y Hernández[119], el cual permite establecer unas actividades de investigación, necesarias para facilitar la implementación de alternativas de seguridad de información y gestión del conocimiento hacia la recuperación, conservación, y particularmente desarrollo de curvas de aprendizaje valiosas para el presente y para el futuro de la institución, así mismo colaborar en el incremento de los capitales: intelectual, tecnológico y organizacional, necesarios para el desarrollo de la competitividad de la misma y para conducirla culturalmente en su camino hacia el desarrollo de una organización de aprendizaje, autogeneradora. Cada una de estas cuatro etapas es descrita a continuación.

Etapa Uno (1) Sensibilización del proyecto: Se realizó la difusión del proyecto y se llegó al acuerdo que los actores clave que asumirían el rol activo en el proceso de implementación de las alternativas de seguridad de la información y del conocimiento eran los líderes de la División de Servicios de Información –DSI– encargados del área de redes, de los recursos del CENTIC[120], de los servidores, del sistema de información financiero, del sistema de información de recursos humanos y del sistema de información académico en cabeza de la jefatura de la División,

[119] RODRÍGUEZ Villasante, Tomás y HERNÁNDEZ, Loli (2012). Metodologías participativas de investigación-acción. Conversatorio Universidad de la República de Uruguay
[120] Centro de Tecnologías de Información y Comunicación de la Universidad Industrial de Santander

apoyados por el equipo de calidad, la jefatura de gestión documental y quienes conforman la vicerrectoría administrativa.

Etapa Dos (2) Diagnóstico Participativo: Se obtiene conocimiento contextual para realizar un análisis crítico de los factores de riesgo, de modo que se disponga de suficiente información para adoptar las decisiones acerca de las prioridades y de las estrategias de seguridad de la información y el conocimiento. Para ello, se llevó a cabo la revisión de documentos institucionales y documentos enviados por consultoras para apoyar el tema. Estos documentos fueron obtenidos de una convocatoria realizada por la universidad con organizaciones como SISA, BPSERVICES S.A.S, IBM *Security Services y Strategik* (Ver Anexo 6. Resumen de propuestas de servicio de consultores en el SGSI), entrevistas individuales semiestructuradas a los líderes de la DSI, una entrevista al equipo directo de apoyo a la Jefatura de la DSI en la UIS, otras entrevistas con el equipo de calidad, la jefatura de gestión documental y quienes conforman la Vicerrectoría Administrativa, lo cual permitió la medición del nivel de madurez a través de la evaluación de los 133 controles de la ISO/IEC 27001:2005 (Ver Anexo 7. Evaluación 11 Dominios ISOIEC 27001:2005 en la UIS). Finalmente, la recolección y análisis de información se realizó a través de triangulación de fuentes de información.

Etapa Tres (3) Generación de estrategias y alternativas: Esta fase define las medidas o estrategias para prevenir riesgos y proceder a la programación y ejecución de un plan de acción, donde se establece las estrategias de seguridad de la información y del conocimiento, que permitan mitigar los problemas existentes y definir e implementar acciones y políticas en función de desarrollo de habilidades y capacidades de la comunidad UIS. Por tanto, esta etapa permitió la construcción de las políticas de seguridad de la información y del conocimiento para la UIS.

Etapa Cuatro (4) Lanzamiento de resultados: Proceso de transferencia de conocimiento, desde una retroalimentación donde participan los saberes y

opiniones de los profesionales que participaron de la ejecución del proyecto, que en este caso fue el equipo directo de apoyo a la Jefatura de la DSI en la UIS liderado en el año 2015 por el Ingeniero Mauricio Tarazona Álvarez y las profesionales Laura Rueda, y Paola Díaz, quienes evaluaron el documento de políticas entregado.

2.4 FASE IV: DISEÑO DEL MODELO PARA LA GESTIÓN DE SEGURIDAD DE INFORMACIÓN Y CONOCIMIENTO DESARROLLADO EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

En esta fase se construyó el modelo para la gestión de seguridad de información y conocimiento UIS, teniendo como insumo todas las etapas previas del estudio y como herramienta de apoyo el software de análisis cualitativo MAXQDA, acción que posibilitó la asignación de códigos específicos que permitieron la agrupación y clasificación de la información con la cual se estableció el marco conceptual del tema. Además, se realizó una formación de auditores en Seguridad de la Información NTC ISO 27001:2013, un curso a través de la plataforma MOOC acerca de la adopción de buenas prácticas sobre gestión y seguridad de TI dirigido por el Ministerio de TIC y la Red Nacional Académica de Tecnología Avanzada (RENATA) y un curso e-learning de especialización sobre Gestión del conocimiento en Red con la organización ARSChile Redes Sociales.

Lo anterior, permitió dar cumplimiento al último objetivo específico de esta investigación, y a partir del análisis de madurez de la UIS en gestión de conocimiento y seguridad de la información, sumado al documento de políticas de la división de servicios de información del año 2014, el documento de política de seguridad de la información del grupo de investigación INNOTEC y el paquete premium de documentos sobre ISO 27001 de la Academia de Advisera implementados en más de 100 países[121], se formularon el Anexo 8

[121] Advisera, se especializa en brindar apoyo a las organizaciones para implementar las principales normas y marcos referenciales como, por ejemplo, ISO 27001, ISO 9001, ISO 13485, ISO 14001,

que contiene la versión 1.0 del plan del proyecto para la implementación del Sistema de gestión de Seguridad de la información y el Anexo 9 que contiene las políticas de gestión de seguridad de la información y el conocimiento para la UIS, las cuales aplican al alcance del proceso de gestión de conocimiento descrito en el Anexo 10. Caracterización del proceso de gestión de conocimiento en la UIS.

OHSAS 18001, IATF 16949, AS9100, ISO 20000 e ITIL. Con los años, Advisera se ha convertido en líder mundial en brindar cursos de capacitación y documentación para ISO 27001 (gestión de seguridad de la información) e ISO 22301 (gestión de la continuidad del negocio) a través de Internet. Sus productos son de la más alta calidad y se han implementado en más de 100 países.

3. RESULTADOS

Se lograron cuatro resultados en esta investigación. El primero consiste en los factores determinantes de la gestión de seguridad del conocimiento relacionados directamente con características de Instituciones Públicas de Educación Superior. El segundo, es la identificación de acciones de gestión del conocimiento para mejorar los procesos de instituciones de educación superior, tomando el caso particular de la UIS, a través de la caracterización del proceso de gestión del conocimiento siguiendo el ciclo PHVA e incluyendo factores asociados a la seguridad de la información (Ver Anexo 10), validando la proposición[122] que la gestión de la información es un factor determinante de la capacidad de gestionar el conocimiento de las organizaciones y además, que los procesos o actividades de gestión del conocimiento del numeral 1.2.1 de este documento pueden ser parte de la forma de trabajo de cualquier organización y se deben realizar en la gestión de procesos y la gestión de proyectos[123] [124].

[122] TELLIS, Winston. Application of a Case Study Methodology. En: The Qualitative Report. Septiembre, 1997. Vol. 3, No. 3. [En línea]. [Citado 10 Enero, 2012]. Disponible en internet: <http://www.nova.edu/ssss/QR/QR3-3/tellis2.html>.

[123] BATISTA, F. F. Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2012.

[124] BATISTA, F. F. et al. Casos reais de implantação do modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2014. (Texto para Discussão, n. 1941).

3.1 FACTORES DETERMINANTES DE LA GESTIÓN DE SEGURIDAD DEL CONOCIMIENTO RELACIONADOS DIRECTAMENTE CON CARACTERÍSTICAS DE INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR

No es sólo el uso de la información lo que causa conmoción en las organizaciones; durante los últimos años, se ha generado la necesidad de reconocer la importancia de gestionar de forma activa y explícita el conocimiento[125]. Uno de los aspectos que muchas organizaciones dejan de lado radica en que no basta con preservar la confidencialidad, integridad y disponibilidad de la información, también es necesario garantizar la protección del conocimiento, pues es este último el que les aporta mayor valor, especialmente en el caso de las KIFs (*knowledge intensive firm*) como las universidades. Según Mok[126], este tipo de instituciones deben tener un mayor enfoque del tema, puesto que son organizaciones con intensiva generación de conocimiento; la calidad y la seguridad de sus activos de información deberían ser una prioridad.

En este tipo de instituciones la realización efectiva de sus actividades educativas y de investigación es cada vez más dependiente de la disponibilidad, integridad y exactitud de los recursos de información. Sin embargo, según una investigación realizada por Doherty, Anastasakis y Fulford[127], en la que se estudió una muestra de 61 universidades pertenecientes al "Ranking mundial universitario 2007" del *"Times Higher Education Supplement",* solo el 7% de las políticas de seguridad de

[125] JOHANNESSEN, Jon-Arild y OLSEN, Bjørn. Knowledge management and sustainable competitive advantages: the impact of dynamic contextual training. En: International Journal of Information Management. Agosto, 2003, vol. 23, no. 4. p. 278.

[126] MOK, Ka Ho. Fostering entrepreneurship: changing role of government and higher education governance in Hong Kong. En: Research Policy. 2005, vol. 34, no. 4. p. 540. Citado por: ALVESSON, Mats. A Review of "Knowledge Work and Knowledge Intensive Firms". En: Journal of Management & Governance. Enero, 2005, vol. 9 no. 1. p. 101-105. Una KIF es una organización que se especializa en la prestación de servicios basados en conocimiento único. Ejemplos típicos de KIFs incluyen firmas de abogados y contadores, compañías de consultoría en administración, ingeniería y computación, agencias publicitarias, unidades de investigación y desarrollo, y empresas de alta tecnología.

[127] DOHERTY; ANASTASAKIS y FULFORD, The information security policy unpacked: A critical study of the content of university policies, Op. cit. p. 455

las universidades seleccionadas contenían una mención explícita de la prioridad especial concedida a la seguridad de la información, dada la naturaleza de conocimiento que tiene la organización.

Para asegurar el éxito, las organizaciones deben tratar de maximizar el nivel de conocimiento exclusivo utilizable dentro de sí mismas. Actualmente, este objetivo se aborda desde dos campos de actividad principales: Gestión del Conocimiento y Gestión de la Seguridad de la Información. El triunfo de ambas disciplinas depende fuertemente de las personas. En la Gestión del Conocimiento, las personas tienen que compartir su conocimiento individual – tanto tácito como explícito – con otros para formar y establecer un cuerpo de conocimiento comprensible que pueda ser usado (y aprovechado) por toda la organización.

Según Nonaka y Takeuchi un activo del conocimiento son las entradas, salidas, y los factores de moderación de creación del proceso de conocimiento[128]. Así mismo, consideran que los activos de conocimiento son específicos de las organizaciones y se pueden categorizar en cuatro grupos: (1) conocimiento experimental que agrupa actividades e iniciativas desde su creación interna, con aprendizaje por ejecución de actividades y la adquisición por medios externos (clientes, proveedores o competidores), lo cual incrementa la base de conocimiento a escala

[128] GEYTERE, T. (n.d.) Un modelo unificado de la creación dinámica de conocimiento: Descripción del Modelo SECI de Nonaka y Takeuchi. Consultado el 1 de febrero de 2012, de: http://www.12manage.com/methods_nonaka_seci.html. Citado por: MARTÍNEZ, Manuel Alejandro y OCAMPO Ana Catalina (2012). El valor de los activos de conocimiento y su incidencia en las organizaciones inteligentes. En: Blog ACTIVOS DE CONOCIMIENTO VS PASIVOS DE CONOCIMIENTO. El gestor del Conocimiento. Disponible en: http://gestorconocimiento.blogspot.com.co/2012/02/v-behaviorurldefaultvmlo.html

organizacional [129] [130] [131] [132], (2) conocimiento conceptual, basado en conocimiento explicito articulado a través de imágenes, símbolos y señales, invención de metáforas, analogías, conceptos, hipótesis o modelos propios[133] [134], (3) Conocimiento Procedimental, conformado por el *Know-How* de las acciones diarias y la propia cultura Organizacional[135], (4) Conocimiento tecnológico, puede ser tanto explícito como tácito, y son tanto la entrada como salida del proceso de gestión de conocimiento[136].

Para que el conocimiento sea considerado un activo, este deberá estar al servicio de la organización, ponerse en funcionamiento afectando los procesos existentes y, contribuir al cumplimiento de los resultados propuestos por la administración[137].

Acerca de la Seguridad de la Información, después de décadas de acercamientos meramente técnicos, ahora es ampliamente aceptado que “las personas son la piedra angular de la seguridad de la información”[138]. Por tanto, "El conocimiento en sí mismo no se puede controlar. Lo que tiene que ser manejado son los seres humanos y las condiciones en que los procesos sociales se llevan a cabo",

[129] MARTIN, Julia, RASTROLLO, Ángeles, The Firm’s Internationalization: The Experiential Knowledge as Determinant of Performance in Foreign Markets. Cuadernos de Economía y Dirección de la Empresa. Núm. 39, junio 2009, págs. 123-150, ISSN: 1138-5758

[130] ANDERSON, Eddse. GATIGNON, Harndol. Modes of foreign entry: A transaction cost analysis and propositions. En: Journal of International Business Studies, (1986) vol. 17, pp.1-25.

[131] ANDERSON, J. C. Y GERBING, D. W. Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. En: Psychological Bulletin (1988), vol. 103, núm. 3, págs. 411-423.

[132] ANDERSSON, S. (2004). Internationalization in different industrial contexts. En: Journal of Business Venturing, 19, p. 851-875

[133] DUTTA, Snider. Conceptualizing and measuring capabilities: methodology and empirical application, Strategic Management Journal, 2005. Pág. 277 – 285

[134] SEGARRA, Mercedes., Configuración del conocimiento como activo estratégico, (2010).

[135] DÍAZ, Nieves Lidia. Los activos de conocimiento tecnológico en las empresas industriales españolas. 2005

[136] BOHMER, R.M. Learning how and learning What: effects of tacit and codified Knowledge on Performance Improvement. En: Following Technology Adoption, Vol. 34. Pag. 197 - 223.

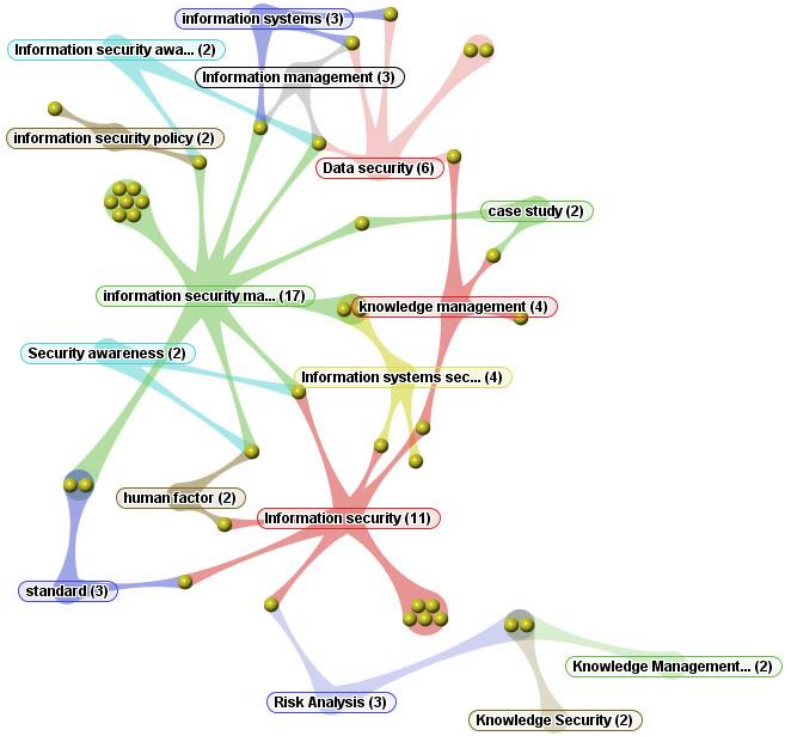
[137] Plan de Incentivos Explorando el Conocimiento. Colombia, Ministerio de Educación Nacional República de. 2011. Bogotá : CETICS, 2011.

[138] BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Julio, 2005, vol. 3, no. 4. p. 49

considerando que el conocimiento está ligado a los individuos y que el conocimiento es creado únicamente por los individuos a través de procesos sociales[139]. Sin embargo, según Ahmad, Bosua y Scheepers[140], la literatura en el área de la gestión de seguridad de la información no se ha relacionado directamente con el concepto de "conocimiento", sino más bien con el de información y datos.

A continuación, se exponen los resultados del análisis bibliométrico que se realizó con el fin de evaluar la evolución en el tiempo de las temáticas anteriormente presentadas según la frecuencia de publicación y la relación entre las mismas.

Ilustración 2. Relaciones entre palabras claves



FUENTE: Autora, usando VANTANGE POINT ®

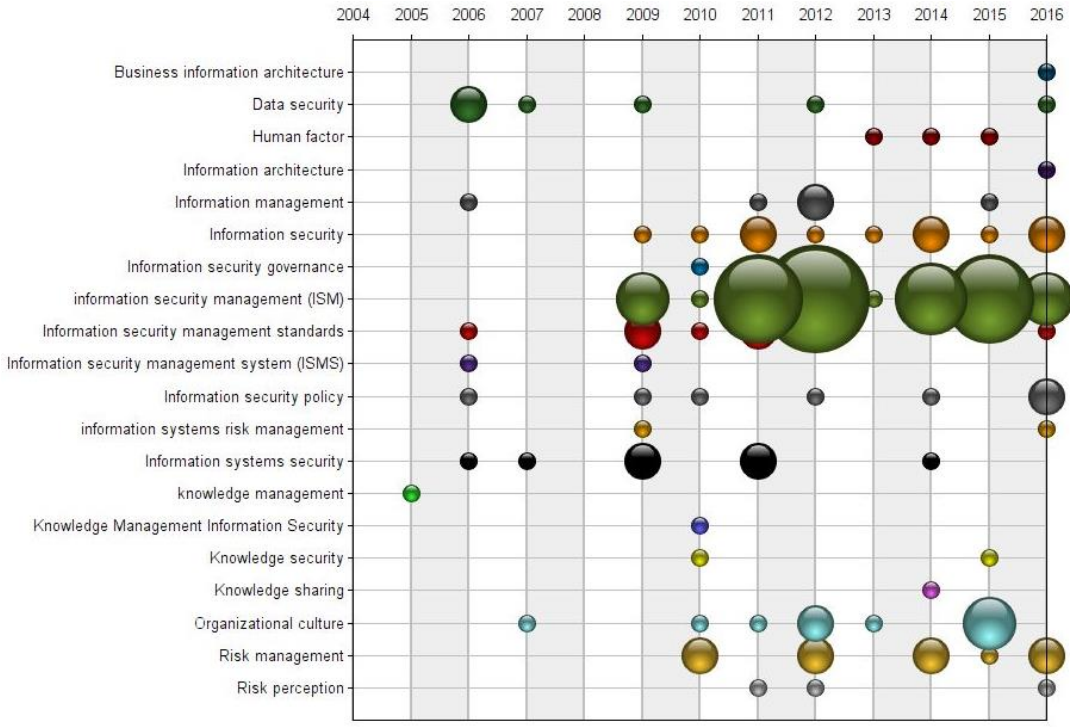
[139] WUNRAM, Michael; WEBER, Frithjof; PAWAR, Kulwant S. y GUPTA, Abhishek. Proposition of a Human-centred Solution Framework for KM in the Concurrent Enterprise. Proceedings of the 8th International Conference on Concurrent Enterprising – Ubiquitous Engineering in the Collaborative Economy, Rome, Italy, 17th-19th June 2002, pp. 151 – 158

[140] AHMAD, BOSUA y SCHEEPERS. Op. cit.

En la Ilustración 2 se puede observar que sólo 4 récords, que representan el 10,53% de los artículos encontrados con la ecuación de búsqueda principal tratan acerca de *"knowledge security"* y *"knowledge management information security"*, mientras que, el 44,73% de los artículos recuperados de la base de datos ISI web of knowledge, es decir, 17 récords se publican en el tópico de *"information security management"* y de estos sólo dos documentos incluyen también en las palabras claves del autor *"knowledge management".*

Por otra parte, en la Ilustración 3 se evidencia la dinámica de publicación en los últimos años, de acuerdo con los resultados de 62 artículos recuperados con la ecuación de búsqueda: "*information security management* OR *intellectual capital security* OR *knowledge security*" corrida en febrero de 2016 y actualizada en octubre del mismo año en la base de datos ISI web of science.

Ilustración 3. Dinámica de publicación según palabras claves a través del tiempo



FUENTE: Autora, usando VANTANGE POINT ®

Según el número de documentos en los que fueron referidas las palabras claves con mayor frecuencia, se determinó que *"information security management"* ha sido estudiado de forma continua desde el 2009 a la fecha mientras que los tópicos *"knowledge security"* y *"knowledge management information security"* sólo han sido abordados en dos documentos, uno en 2010 por Desouza y otro en 2015 por Manhart y Thalmann, lo cual muestra la oportunidad de retomar el tema de investigación con la ventaja del recorrido y profundización que sigue teniendo la gestión de seguridad de la información, puesto que, puede llegar a ser usado como apalancamiento y facilitador del estudio de la gestión de seguridad del conocimiento.

Una vez finalizados los anteriores análisis, se documentaron los factores determinantes de las temáticas *"information security management"*, *"knowledge security"* y *"knowledge management information security"*. Por una parte, se realizó un artículo que fue publicado en 2016 en la revista especializada El profesional de la información ubicada en cuartil Q2 indexada en Scopus (Ver Anexo 18). Este artículo consolida el estado del arte sobre el tópico "*information security*" para la ventana de tiempo 2001-2015, obtenida de una revisión de literatura realizada en tres etapas: a) Revisión de información no estructurada, b) Análisis bibliométrico y c) Análisis, organización y síntesis del contenido. Como resultado se extrajo un amplio marco de trabajo multi-dimensional como referencia para relacionar gestión del conocimiento, gestión de riesgos, incidentes de seguridad, sistemas de información y redes, recursos humanos, aspectos económicos, gobernanza, políticas y buenas prácticas. Además, concluyendo que deben continuar investigaciones encaminadas hacia estudiar los riesgos correspondientes al conocimiento más allá de la misma información, así como lo advierte Herath[141], quien indica que la investigación empírica sobre las conductas en los usuarios de la información y los factores que influyen en ellas apenas ha comenzado, y la razón

[141] HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008. Dissertation (Doctor of Philosophy). University of New York. Faculty of the graduate school. p. 9.

exacta de la ausencia de una base teórica y un acercamiento formal a la gestión de seguridad del conocimiento no se conoce.

Por otra parte, se determinaron relevantes los siguientes factores para asegurar o proteger el conocimiento (Ver Tabla 1), a pesar de que autores como Manhart y Thalmann[142], quienes investigan sobre protección del conocimiento, aseguran que esta temática es a menudo un área descuidada o subdesarrollada. Esto es preocupante dado que la protección del conocimiento juega un papel esencial en la preservación de la ventaja competitiva de una organización. A pesar del reconocimiento de esta cuestión por parte de los estudiosos, la literatura sobre gestión del conocimiento hasta ahora ha tendido a concentrarse en la facilitación del intercambio de conocimientos y no en la protección del conocimiento[143].

Tabla 1. Factores determinantes de la seguridad o protección del conocimiento

Factor determinante	Descripción	Autores
Infraestructura TIC, software y tecnología de GC	Las TIC deben promover la captura eficaz de los conocimientos tácitos y explícitos y apoyar el intercambio de conocimientos en toda la organización. Además de garantizar a los trabajadores el acceso a la base de conocimientos de la organización. Las redes de comunicación, los correos electrónicos, la intranet, el almacenamiento de datos y los sistemas	(Martin, 2000), (Stankosky, 2005)

[142] MANHART, Markus; THALMANN, Stefan. Protecting organizational knowledge: a structured literature review. Journal of Knowledge Management, 2015, vol. 19, no 2, p. 190-211.
[143] Ibid., p. 190

Factor determinante	Descripción	Autores
	de apoyo a la toma de decisiones son algunos de los elementos básicos de la infraestructura tecnológica de la GC. Además, se deben incluir sistemas de gestión de documentos y de flujo de trabajo, bases de conocimiento avanzadas y el desarrollo de sistemas de memoria corporativa, minería de datos y filtrado, así como tecnologías tales como groupware, intranets e Internet que enlacen la organización a nivel intra e inter-organizacional y al mundo exterior.	
Oportunidades de obtención de información	Este factor se refiere a la actitud de la organización hacia la valoración de la información como un recurso y los procesos consecuentes de hacer que el aprendizaje de la organización y los conocimientos estén disponibles, facilitando la transferencia de conocimientos y el intercambio entre el personal. Son ejemplos de este factor, el acceso o fácil disponibilidad de la información de expertos o información técnica y profesional.	Brown y Starkey (1994)
Apoyo del liderazgo a actitudes de	La alta dirección y los líderes necesitan lograr una cultura y mantener un ambiente de intercambio de conocimientos. Deben	(Barnes, 2001)

Factor determinante	Descripción	Autores
intercambio de conocimientos	proporcionar apoyo financiero a aquellos que demuestren actitudes de intercambio de conocimientos, y deben demostrar compartir sus propios conocimientos, usar el conocimiento de los demás en su toma de decisiones y dar crédito a los colaboradores que comparten sus conocimientos.	
Conocimientos y habilidades TIC	La literatura ha demostrado que cuanta más capacitación se proporciona para el mejoramiento de las habilidades de los trabajadores en el uso de las tecnologías de la información y las comunicaciones (TIC), más informadas estarían las personas y por tanto, más conocimiento puede ser transferido y compartido dentro y fuera de la organización, lo que resulta en un mejor desempeño organizacional.	(Syed-Ikhsan y Rowland, 2004)
Programas de rotación de puestos de trabajo	Los empleados aportan su educación previa, sus experiencias, conocimientos y habilidades que agregan valor al capital humano de la organización. A través de este factor, parte de los conocimientos y la experiencia adquirida de un proceso o unidad anterior pueden ser transportados a otro proceso o unidad favoreciendo el proceso de transferencia de	(Bogdanowicz y Bailey, 2002)

Factor determinante	Descripción	Autores
	conocimientos, ya que incrementa el aprendizaje o conocimiento de los empleados, así como el aprendizaje o conocimiento organizativo.	
Protección del conocimiento en alianzas	Los estudiosos que se centran en este factor se ocupan básicamente de la llamada paradoja de frontera presentada por las organizaciones que desean acceder al conocimiento externo y, al mismo tiempo, proteger el conocimiento interno	(Quintas et al., 1997, Norman, 2001, Jordan y Lowe, 2004)
Asegurar el capital intelectual	Los artículos que tratan este tema discuten frecuentemente la efectividad de las medidas para proteger los derechos de propiedad intelectual, es decir, las patentes, los secretos comerciales, los derechos de autor y las marcas registradas. Sin embargo, el desafío es cómo aplicar estas medidas a un conocimiento más inmaduro e informal y proponer medidas adecuadas.	(Hannah, 2005, Arundel, 2001)
Protección del conocimiento para mantener la ventaja competitiva	Los autores se centran en la investigación de factores como la confianza y el tamaño del sector o de la empresa, influyen en el comportamiento de protección de las organizaciones.	(Norman, 2002), (Brouwer y Kleinknecht, 1999)

Factor determinante	Descripción	Autores
Protección del uso de las redes sociales	Un foco importante de la GC es el riesgo de usar las redes sociales y cómo esto podría poner en peligro la ventaja competitiva. En general, se hace hincapié en que el mantenimiento de la ventaja competitiva depende de la prevención adecuada de los efectos secundarios no deseados, especialmente, en lo relacionado con el espionaje organizativo.	(Väyrynen et al., 2013), (Snyder y Crescenzi, 2009)
Protección del conocimiento para prevenir la pérdida de conocimiento	Los documentos que tratan este tema se centran en el riesgo de pérdida de conocimiento causada por los empleados que abandonan la organización y no se adaptan a las medidas, marcos normativos o políticas de gestión. La pérdida de conocimientos, complementaria al desborde del conocimiento, se investiga en su mayor parte desde la perspectiva de los recursos humanos.	(Jennex y Durcikova, 2013; Boyles et al., 2009).
Fomento de una cultura de aprendizaje	Debido al actual dilema del envejecimiento de la fuerza de trabajo que genera que un gran grupo generacional de personas se retiren al tiempo, hace necesario pronosticar y planificar las necesidades futuras de capital humano, así como comenzar a preparar el personal	(Martin, 2015), (Holsapple y Singh, 2003)

Factor determinante	Descripción	Autores
	que hará el relevo y desarrollar las competencias necesarias para que estén listos a ocupar especialmente las posiciones o cargos críticos, además de asegurarse que cuentan con una fuerza preparada, Informada, motivada y comprometida. Esto sugiere que los empleados deben recibir capacitación continua para enriquecer sus conocimientos y mejorar sus capacidades.	
Fomento de una cultura de intercambio de conocimientos	La cultura de compartir el conocimiento no ocurrirá en una organización a menos que sus empleados y grupos de trabajo muestren un alto nivel de confianza y comportamiento cooperativo. El cambio en la cultura y en el comportamiento individual debe tener como objetivo fomentar el uso del conocimiento no para beneficio individual, sino para el beneficio de la organización como un todo.	(Salleh y Goh, 2002), (Barnes, 2001)

Fuente: Autora, a partir de Manhart y Thalmann[144], Martin[145], Manhart y Thalmann[146], Chong et. al[147]

[144] Ibid., p. 196

[145] MARTIN, Angela. Talent Management: Preparing a “Ready” agile workforce, International Journal of Pediatrics and Adolescent Medicine, Volume 2, Issues 3–4, September–December 2015, Pages 112-116, ISSN 2352-6467, https://doi.org/10.1016/j.ijpam.2015.10.002. Disponible en: http://www.sciencedirect.com/science/article/pii/S2352646715001088

[146] MANHART, Markus y THALMANN, Stefan (2015). Protecting organizational knowledge: a structured literature review. En: Journal of Knowledge Management. Vol. 19 Issue: 2, pp.190-211, https://doi.org/10.1108/JKM-05-2014-0198

[147] CHOY CHONG, Siong, et al. KM implementation in a public sector accounting organization: an empirical investigation. Journal of Knowledge Management, 2011, vol. 15, no 3, p. 497-512.

3.2 CARACTERIZACIÓN DE LA GESTIÓN DEL CONOCIMIENTO EN LAS INSTITUCIONES PÚBLICAS DE EDUCACIÓN SUPERIOR COLOMBIANAS

Los cambios que se han generado de los paradigmas en los sistemas económicos a lo largo de la historia ubican actualmente a las organizaciones en la denominada "Sociedad del Conocimiento", que se empezó a gestar en los años sesenta con la aparición de las computadoras, la expansión de las multinacionales y la formación de un mercado internacional de capitales. En los ochenta con el mercadeo internacional que se fortaleció debido a las innovaciones tecnológicas en comunicaciones y en los noventas con la masificación de Internet se aceleró la globalización, es así como aparecen los nuevos conceptos de competencia y competitividad y se empieza a hablar de la "Sociedad de la Información" que tiene como eje central la gestión y difusión de la información soportado en tecnologías para almacenamiento y transmisión de datos"[148].

Ahora bien, la disponibilidad de información generó nuevas capacidades para que la sociedad "identifique, produzca, transforme, difunda y utilice la información con el objetivo de crear y aplicar los conocimientos necesarios para el desarrollo humano"[149], capacidad que se definió como la "Economía basada en el Conocimiento" descrita por Montuschi[150] como la "capacidad de innovar y crear valor más rápido en base al conocimiento y a su rápida actualización en diversos ámbitos por medio del aprendizaje".

[148] PELUFFO A., Martha Beatriz y CATALÁN CONTRERAS, Edith. Introducción a la gestión del conocimiento y su aplicación al sector público. Instituto Latinoamericano y del Caribe de Planificación Económica y Social – ILPES. Santiago de Chile, diciembre de 2002, 92 p. Disponible en: http://repositorio.cepal.org/bitstream/handle/11362/5586/S2002617_es.pdf?sequen

[149] UNESCO. (2005). Hacia las sociedades del conocimiento. Informe Mundial. Ediciones UNESCO. Paris. 2005. 240 p.

[150] MONTUSCHI, Luisa, et al. La economía basada en el conocimiento: importancia del conocimiento tácito y del conocimiento codificado. Documentos de trabajo, 2001, vol. 1.

Es importante identificar dos características del conocimiento: el tipo de conocimiento y el contexto de aplicación. Los tipos de conocimiento que tienen influencia en la eficiencia de las organizaciones son tres: el primero, es el conocimiento tácito que Smith[151] definía como "la aptitud, destreza y sensatez con que generalmente se ejercita el trabajo". El segundo tipo es el conocimiento científico y tecnológico que toma importancia a medida que aumenta la exigencia de los mercados conllevando a las organizaciones a innovar y ser más eficientes productivamente; y el tercero, es el conocimiento que define cómo organizar y gestionar las actividades económicas, especialmente aquellas que comprenden la aplicación de nuevas perspectivas científicas y tecnológicas[152].

La característica de contexto de aplicación tiene en cuenta que cada sociedad tiene sus propios puntos fuertes en materia de conocimiento, por lo que es necesario hacer gestión del conocimiento en dos sentidos: haciendo que el conocimiento propio de las organizaciones sea evidente y genere valor para la organización; y generando capacidades para absorber nueva información y articularla con el conocimiento propio[153]. En resumen, y como lo se muestra en la Ilustración 4, actualmente el conocimiento contextualizado y la capacidad de aprender y vincular el conocimiento a las actividades productivas son la base para la innovación y la competitividad organizativa[154] [155].

[151] SMITH, Adam (1776). Investigación de la naturaleza y causas de la riqueza de las naciones. Tomo I. Disponible en: http://www.marxistsfr.org/espanol/smith_adam/1776/riqueza/smith-tomo1.pdf
[152] STEINMUELLER, W. Edward. Las economías basadas en el conocimiento y las tecnologías de la información y la comunicación. Revista Internacional de Ciencias Sociales, 2002, vol. 171, p. 1-17.
[153] UNESCO. Op. Cit.
[154] DIAZ MUÑANTE, Jorge Raúl. Modelo de Gestión del Conocimiento (GC) aplicado a la Universidad Pública del Perú, publicado en el SISBIB "sistema de bibliotecas del Perú", 2003. 40 p
[155] GONZÁLEZ ARIZA, Angel León; CASTRO, Jean Paul; RONCALLO, Mayra. Diagnóstico de la gestión de conocimiento en una empresa grande de Barranquilla (Colombia). Una actividad de vinculación cooperativa universidad-sector productivo. Ingeniería y Desarrollo, 2004, no 16.

Ilustración 4. Relación conocimiento – competitividad en la Sociedad del Conocimiento

Fuente: Autora a partir de STAPLES, Sandy; GREENAWAY, Kathleen y MCKEEN, James. Opportunities for research about managing the knowledge-based enterprise. En: International Journal of Management Reviews. 2001, vol. 3. p. 1-20.

En las Instituciones de Educación superior se está entendiendo este nuevo paradigma y reconocen la gestión del conocimiento como esencial para la generación de valor y ventajas competitivas en las instituciones. Por tanto, mediante este trabajo y siguiendo el proceso cíclico Deming se pretende inicialmente establecer las pautas del PHVA existente en cualquier sistema de gestión, teniendo en cuenta que una caracterización de procesos consiste en identificar condiciones y/o elementos que hacen parte del proceso, tales como: el objetivo del proceso, ¿quién lo hace?, ¿Para quién o quienes se hace?, ¿Por qué se hace?, ¿Cómo se hace?, ¿Qué se requiere para hacerlo?, por tanto se establecieron en la estructura de la misma, los proveedores, las entradas o insumos, los productos esperados o salidas del proceso, y el destinatario. Además, se muestra la articulación con otros procesos, riesgos, principales productos, procedimientos y documentos asociados, indicadores sugeridos para la verificación y las acciones de mejora (Ver anexo 10. Caracterización del proceso de gestión de conocimiento).

3.2.1 Identificación de activos de conocimiento

Gestionar el conocimiento implica la gestión de todos los activos intangibles que aportan valor a la organización para conseguir capacidades, o competencias esenciales, distintivas[156]. La gestión del conocimiento es un conjunto de procesos y sistemas que permiten que el capital intelectual de una organización aumente de forma significativa, mediante la gestión de sus capacidades para la solución de problemas y cuyo objetivo es crear ventajas competitivas. Por tanto, el capital intelectual es la materia prima fundamental para la gestión del conocimiento y comienza con el reconocimiento de los activos intangibles que hacen que una organización sea eficiente y competitiva[157].

Teniendo en cuenta lo anterior, para lograr implementar un modelo de gestión del conocimiento en una organización, es necesario primero hacer una medición de su capital intelectual[158], puesto que, el capital intelectual se promueve como un factor importante y necesario para la supervivencia organizacional y el mantenimiento de la fuerza competitiva[159], el cual de acuerdo al Euroforum[160] realizado en 1998, puede definirse como “el conjunto de activos intangibles de una organización que, pese a no estar reflejados en los estados financieros tradicionales, en la actualidad

[156] OSORIO NUÑEZ, Maritza (2003). El capital intelectual en la gestión del conocimiento. En: Revista cubana de los profesionales de la información y la comunicación en salud, vol. 6, No. 11. Facultad de Estomatología "Raúl González Sánchez". Salvador Allende y Calle G. Plaza de la Revolución. Ciudad de La Habana, Cuba. Disponible en: http://bvs.sld.cu/revistas/aci/vol11_6_03/aci07603.htm

[157] Ibid., p. 5

[158] DÍEZ JIMÉNEZ, D. A., & ZÚÑIGA PALTA, A. M. (2011). Implementación de un modelo de gestión del conocimiento para empresas de servicios. Universidad ICESI. Retrieved from https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/67420/1/implementacion_modelo_gestion.pdf

[159] DRAGHICI, A. (2013). A possible approach for generic model concerning intellectual capital evaluation. Annual session of scientific papers IMT, 12, 267-273. Citado por: Maria-Luminita Gogan, An Innovative Model for Measuring Intellectual Capital, Procedia - Social and Behavioral Sciences, Volume 124, 2014, Pages 194-199, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2014.02.477. Disponible en: http://www.sciencedirect.com/science/article/pii/S1877042814020254

[160] Euroforum. Modelos. Disponible en: http://www.gestiondelconocimiento.com/modelo_modelointelect.htm

generan valor o tiene potencial de generarlo en el futuro" y está compuesto por el capital humano, estructural y externo[161].

Para identificar los activos de conocimiento se utilizó el modelo Technology Broker creado por Annie Brooking (1997). Debido a que el modelo de Brooking define que el capital intelectual está conformado por activos de mercado, activos centrados en el individuo, activos de infraestructura y activos de propiedad intelectual, se llevó a cabo un diagnóstico para determinar cuáles de ellos tenían mayor prioridad para la institución. Este diagnóstico se hizo con base en la metodología sugerida por Brooking para auditar la información relacionada con el capital intelectual, a través de un cuestionario con preguntas que permitieron identificar el estado de cada uno de los activos nombrados (Ver Anexo 20. Cuestionario de auditoría de los activos de capital intelectual basado en Brooking), el cual fue respondido por la Ingeniera Piedad Arenas Díaz quien es docente planta de la UIS desde hace 18 años, actualmente profesora asociada de la Escuela de Estudios Industriales y Empresariales. Además, de ser docente ha estado en comisión de servicios como directora de la Escuela de Estudios Industriales y Empresariales, jefe de recursos humanos y directora de planeación de la UIS en diferentes momentos, quien asocia el concepto de gestión de conocimiento con la forma de agregar valor a partir de la generación, transformación y capitalización del conocimiento. A continuación, se detallan los resultados de la clasificación de los activos:

Activos de mercado: teniendo en cuenta que los activos que pertenecen a este grupo son aquellos que le dan a la institución una ventaja competitiva dentro del mercado, en esta clasificación se encuentran la información, clientes y denominación social de la institución.

Activos centrados en el individuo: Las universidades son instituciones de servicios, por lo que los activos que pertenecen a este grupo son los que tienen

[161] FUNES, Y. y HERNÁNDEZ, C. (2001). Medición del valor del capital intelectual, Revista Contaduría y Administración, 203, 47.

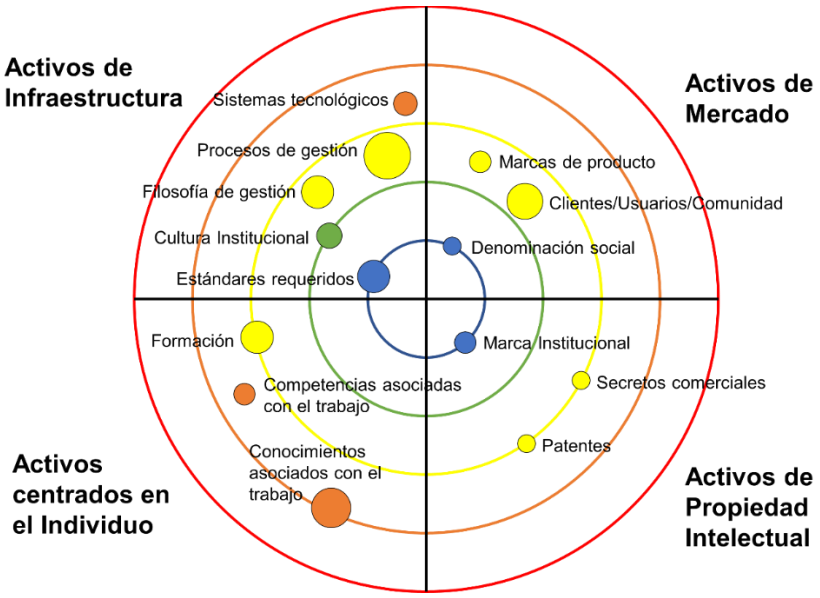
para ellas una prioridad más alta. Dentro de esta clasificación se encuentran la formación, los conocimientos y las competencias asociadas con el trabajo.

Activos de infraestructura: dentro de este grupo de activos se evaluaron la filosofía de gestión, la cultura corporativa, los procesos de gestión, los sistemas tecnológicos y los estándares requeridos.

Activos de propiedad intelectual: los activos estudiados que pertenecen a este grupo son marca (de fábrica), las patentes, modelos de utilidad y secretos comerciales.

Las respuestas a las preguntas realizadas tenían una escala de 1 a 5, donde 1 significaba que no se ha trabajado y 5 que el tema de la pregunta en cuestión funciona muy bien. Esto permitió que, de acuerdo con las respuestas obtenidas, el estado de los activos de capital intelectual se representa en un gráfico de 5 círculos, cada uno identificado con un color diferente (Ver ilustración 5).

Ilustración 5. Resultado Cuestionario Diagnóstico basado en Brooking



Fuente: Elaboración propia.

En el gráfico anterior puede notarse que existe un total de 14 puntos, cada uno de los cuales representa un activo, distribuidos de la siguiente manera: 3 activos en la zona azul, 1 en la verde, 3 en la naranja, 7 en la amarilla y ninguno en la roja. De acuerdo con Brooking, el hecho que la mayoría de activos del gráfico se encuentren en la zona amarilla, indica que en general la institución necesita mejorar su capacidad para retener, desarrollar, organizar y utilizar las capacidades de sus empleados, con el fin de convertirse así en una institución de la zona verde o azul, que son las que se consideran seguras, es decir, donde se tiene mayor posibilidad de crecimiento.

3.2.2 Guía para la gestión y clasificación de activos de conocimiento

La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico de la institución se debe realizar con el objetivo de dar cumplimiento al ítem A.8 Gestión de activos de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013. Los atributos generales con los que se identifica un activo pueden ser:

- Nombre del activo: nombre con el cual es conocido el activo en la Universidad.
- Descripción: Proporciona información más detallada del activo para conocer cuál es su fin en la Universidad.
- Fecha ingreso del Activo: Específica la fecha en la que el activo se incluyó como parte del inventario, se diligencia una sola vez.
- Fecha salida del Activo: Especifica la fecha en la que el activo fue excluido del inventario, este atributo solo se diligencia cuando el activo se saca del inventario de activos del proceso generalmente luego de la etapa de revisión.
- UAA: Nombre de la Unidad Académico Administrativa donde se identificó el activo
- Proceso: Nombre del proceso dónde se identificó el activo
- Categoría: Indica el tipo de activo. Se sugiere para la UIS las categorías relacionadas en la Tabla 2.

- Ubicación: Física o digital
- Propietario[162]: “Dueño” o “Propietario” identifica a un individuo o a una entidad que tiene responsabilidad aprobada por la Alta Dirección, para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.
- Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan los activos de información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.
- Derechos de acceso: Hace referencia a los usuarios y permisos establecidos para el uso del activo. Se han definido las siguientes letras para identificar el derecho de acceso: (L) Lectura; (M) Modificación; (E) Eliminación y (C) Creación.
- Nivel del activo: Determinar los activos críticos, para ello se debe clasificar el activo de conocimiento según el análisis del impacto que puede tener para la Universidad la pérdida de confidencialidad, integridad o disponibilidad del activo de información (Ver Tabla 3).

Tabla 2. Categoría de Activos de conocimiento

Categoría de Activo de Conocimiento	Descripción
Conocimiento tácito	El conocimiento es una mezcla de experiencia, valores, información contextual, conocimiento técnico y específico e intuición que proporciona bases para incorporar nuevas experiencias e información. Se origina y se aplica en la mente de los conocedores. En las organizaciones, a menudo se incrusta no sólo en documentos o repositorios, sino también en rutinas, procesos, prácticas y normas organizacionales[163].
Información	Información en cualquiera de sus formas: física, digital, oral. Ejemplo: bases de datos y archivos de datos, contratos, documentación del sistema, información sobre investigación, etc.

[162] El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

[163] TIWANA, Amrit. The knowledge management toolkit: practical techniques for building a knowledge management system. Prentice Hall PTR, 2000. Citado por: SCHOMBACHER, et al. Continuous Knowledge Transfer – A pragmatic approach to knowledge sharing in the European Patent Office, World Patent Information, Volume 47, 2016, Pages 1-11, ISSN 0172-2190, http://dx.doi.org/10.1016/j.wpi.2016.08.005. Disponible en: http://www.sciencedirect.com/science/article/pii/S0172219016300953

Categoría de Activo de Conocimiento	Descripción
Software	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y motores de bases de datos, etc.
Recurso humano	Empleados, contratistas y auxiliares con conocimiento, experiencia y criticidad para el proceso
Servicio	Servicios de computación y comunicaciones, tales como, correo electrónico, Internet, páginas de consulta, directorios compartidos e Intranet.
Hardware	Equipos de cómputo y de comunicaciones, medios removibles, teléfonos y otros equipos críticos para el proceso
Sitios	– Sitios ubicados en ambientes externos donde no se pueden aplicar los medios de seguridad de la organización. – Instalaciones limitadas por el perímetro de la organización en contacto directo con el exterior. – Zonas formadas por una frontera protectora física que forma divisiones dentro de las instalaciones de la Universidad.
Otros	Activos que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

Fuente: Empresa NewNet, Talleres de capacitación en SGSI, a partir de la norma técnica NTC ISO 27001:2013[164] [165].

Se considera importante además determinar los procesos críticos por donde iniciar, teniendo en cuenta que la implementación de un modelo de gestión de seguridad de información y conocimiento requiere cambios en toda la institución, y requiere también nuevas capacidades[166], por tanto, se debe preparar a los miembros de la comunidad UIS (esto es, profesores, estudiantes, administrativos, pensionados y

[164] BUSTAMANTE, Giovanny., OSORIO, Jorge. Metodología de la seguridad de la información como medida de protección en pequeñas empresas, 2014.
[165] ISO 27000. (2014). ISO/IEC 27000:2014 Information technology - Security techniques – Information security management systems - Overview and vocabulary. Recuperado de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411
[166] KOSUTIC, Dejan (2011). ¿Cuánto cuesta la implementación de la norma ISO 27001? En: The ISO 27001 & ISO 22301 Blog. Disponible en: https://advisera.com/27001academy/es/blog/2011/02/08/cuanto-cuesta-la-implementacion-de-la-norma-iso-27001/

egresados) a través de jornadas de sensibilización, contar con asistencia externa con amplia experiencia y, tener disponibilidad no sólo de recursos financieros para invertir en hardware o software, sino además disponer de horas y espacios para que la comunidad UIS, en especial los empleados puedan identificar dónde están los riesgos, cómo mejorar los procedimientos y políticas existentes o implementar nuevas; y también capacitarse para asumir las nuevas responsabilidades y adaptarse a las nuevas normas.

Tabla 3. Sistema de clasificación de activos de conocimiento

CRITICIDAD	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD	
ALTA	RESTRINGIDA	Conocimiento disponible sólo para un grupo de personas, dentro o fuera de la Universidad, y que en caso de ser conocido por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativo o económico para la Universidad, o de violación del derecho a la intimidad personal y familiar, honra y buen nombre de las personas.	IA	Conocimiento cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal y/o económico para la Universidad, o afectar la integridad, honra y buen nombre de las personas.	DA	La no disponibilidad del conocimiento puede conllevar un impacto negativo de índole legal, económica o de orden público para la Universidad.
	SIN CLASIFICAR	Conocimiento de uso interno que aún no ha sido sometido al procedimiento de clasificación. Este conocimiento debe tratarse como si fuese Restringido y sólo puede estar en este nivel por un período limitado de tiempo.				
BAJA	PÚBLICA	Conocimiento que puede ser transferido, entregado o publicado sin restricciones a cualquier persona dentro y fuera de la universidad, sin que esto implique daños a terceros ni a las actividades y procesos de la Universidad.	IB	Conocimiento cuya pérdida de exactitud y completitud conlleva un impacto no significativo de índole operativo, pero no legal ni económico, para la Universidad.	DB	La no disponibilidad del conocimiento puede afectar la operación normal de la Universidad, pero no conlleva implicaciones legales, económicas o de orden público.

Fuente: Autora

La tabla 4 permite evaluar la criticidad de los procesos que afectarían la continuidad de las operaciones a través de evaluar el impacto de los eventos de riesgo derivados de la prestación del servicio o del manejo de los activos de conocimiento en las variables estratégicas tomadas a partir de la Guía para la Administración del riesgo (DAFP) Del departamento Administrativo para la Función Pública[167] y que fueron adaptadas a la UIS. La escala con la cual se recomienda valorar el impacto se explica en la Tabla 5.

Tabla 4. Elementos y criterios de priorización para identificar los procesos críticos de la Institución

	CRITICIDAD DE LOS PROCESOS							
	PROCESO: _____							
	Unidad Académico Administrativa: _____							
	Variables Afectadas / **Eventos de Riesgo**	**NIVEL DE IMPORTANCIA**	RENTABILIDAD E INGRESOS (CAPITAL)	AL CLIENTE / USUARIO	IMAGEN INSTITUCIONAL	CUMPLIMIENTO LEGAL	OPERACIÓN	OTROS PROCESOS
PRESTACIÓN DEL SERVICIO	Prestación errada o demoras en la prestación del servicio	**4**						
	Ausencia de Personal	**5**						
	Falla de los sistemas tecnológicos	**4**						
	Falla de la prestacion de servicio por proveedores	**4**						
	Limitación en el acceso al sitio de trabajo	**4**						
MANEJO DE LOS ACTIVOS DE CONOCIMIENTO	Pérdida de confidencialidad por acceso no autorizado al activo de conocimiento que permite la utilización indebida o fraudulenta del mismo.	**5**						
	Pérdida de integridad del activo de conocimiento por alteracion de su contenido	**5**						
	Pérdida de disponibilidad del activo de conocimiento	**5**						

Fuente: Autora

Respecto a la columna “Nivel de importancia” en la Tabla 4, este nivel puede variar de 1 a 5, siendo 1 el menos importante y 5 el mayor nivel de importancia. Teniendo en cuenta que la gestión tradicional no puede captar que el valor en la nueva economía del conocimiento y la innovación se crea por los activos intangibles[168], y dado que el capital intelectual se presenta por algunos autores como el capital que

[167] Departamento Administrativo de la FUNCIÓN PÚBLICA (DAFP): Guía para la Administración del Riesgo. Bogotá, 2009. P 14-15.
[168] LEV, B., 2000. Risk management—Analysis Credit management--Analysis Lev, Baruch--Interviews Publication: The Journal of Lending & Credit Risk Management, vol. 82, No. 8.

deriva del conocimiento[169], y ha sido identificado como un conjunto de intangibles que impulsa el rendimiento organizacional y la creación de valor[170] [171] [172]. Esto explica porque el evento de riesgo "Ausencia de personal" y los riesgos relacionados con el manejo de los activos de conocimiento tienen una importancia de 5 frente a los demás que tienen una importancia de 4, con el fin de diferenciar el conocimiento, ya que se suele considerar como un activo clave y se espera que la pérdida de conocimiento reduzca el valor de este activo clave. La pérdida de fuentes de conocimiento humano ocurre de varias maneras, ya sea por error en su manejo, por retiro de la fuente de la institución debido a la edad avanzada, por rotación debida probablemente para unirse a otra compañía, o por incapacidad laboral[173].

Tabla 5. Escala de valoración del impacto del evento de riesgo sobre cada variable estratégica de la institución

Calificación	Concepto de calificación
5	Incapacidad para recuperarse. Cierre permanente del grupo o pérdida permanente de las instalaciones. Es muy probable una pérdida total de los negocios y operaciones.
4	Posible daño a la reputación del grupo. Cese prolongado de las actividades del grupo. Requiere la activación de un plan de contingencia. Meses de refuerzo son necesarios para la reparación/recuperación. Pérdida temporal de las instalaciones.
3	Semanas de esfuerzo son necesarias para la reparación/recuperación. Hay gastos importantes y pérdidas de ingresos.

[169] GOGAN, Luminita-Maria y DRAGHICI, Anca (2013). A model to evaluate the intellectual capital. En: CENTERIS 2013 - Conference on ENTERprise Information Systems / PRojMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies. Pág. 867 – 875

[170] Roos, G., Roos, J., 1997. Measuring Your Company's Intellectual Performance. Long Range Planning, Special Issue on Intellectual Capital, Vol. 30, No. 3, p. 413-426.

[171] Bontis, N., 1998. Intellectual capital: an exploratory study that develops measures and models, Management Decision, Vol. 36, No. 2, p. 63 – 76.

[172] Bontis, N., Keow, W.C. and Richardson, S., 2000. Intellectual capital and business performance in Malaysian industries, Journal of Intellectual Capital, Vol 1, No. 1, p. 85-100.

[173] JENNEX, Murray E. (2009). Assessing Knowledge Loss Risk. En: Conference: Proceedings of the 15th Americas Conference on Information Systems, AMCIS 2009, San Francisco, California, USA, August 6-9, 2009. DOI: 10.1109/HICSS.2013.103

Calificación	Concepto de calificación
2	Días de esfuerzo son necesarios para la reparación / recuperación. Hay gastos significativos y/o cierta pérdida de ingresos
1	Se requiere de algunos esfuerzos para reparar el daño. Los costos de recuperación son mínimos. No hay pérdidas de ingresos.
0	Sin impacto medible en este momento

Fuente: Autora. Adaptado de BITS[174], NIST[175] y LAYTON[176].

Finalmente, en la tabla 6 se relacionan los eventos de riesgo asociados a la divulgación, alteración, modificación o no disponibilidad según tipo de activo de conocimiento.

[174] BITS. Op. cit., p. 18.
[175] NIST. Op. cit., p. 23.
[176] LAYTON Op. cit., p. 16.

Tabla 6. Eventos de riesgo asociados a la divulgación, alteración, modificación o no disponibilidad según tipo de activo de conocimiento

Tipo de activo	Confidencialidad	Integridad	Disponibilidad
Conocimiento	Pérdida de conocimiento por jubilación, movilidad laboral, incapacidad de la institución de retener a los principales talentos, o difusión de conocimiento a través de redes sociales.	Trabajadores entrantes con habilidades inadecuadas o pérdida de talentos con habilidades críticas necesarias para el crecimiento futuro de la institución generan errores o incoherencias en los procesos	Que sólo una persona cuente con las habilidades o experiencia claves esenciales para mantener el proceso o crear nuevos productos o servicios. O la fuente posee un conocimiento único debido a su rol en eventos claves de la institución y no ha sido compartido o transferido a otras personas.
Información	Que un individuo, entidad o proceso no autorizado acceda o conozca el activo de información o su contenido.	Que se pierda la completitud, coherencia o precisión del activo de información. Ejemplo: Individuo, entidad proceso que con o sin autorización modifique el activo.	Que el activo de información no pueda ser accedido o utilizado cuando se requiera y por el personal que está autorizado.
Hardware	Que la información almacenada, procesada o transportada o que los servicios prestados por el activo de información sean accedidos o conocidos sin autorización.	Que la información almacenada, procesada o transportada pierda completitud, coherencia o precisión. Que los servicios prestados por el activo de información pierdan su fiabilidad.	Que el activo, la información almacenada, procesada o transportada o que los servicios prestados por el activo de información no estén disponibles cuando se requieran y por el personal autorizado.
Software	Que la información almacenada, procesada o transportada por el activo de	Que el activo de información, su configuración, la información que almacena, procesa o transporta	Que el activo de información, la información que almacena, procesa o transporta no esté

Tipo de activo	Confidencialidad	Integridad	Disponibilidad
	información sea accedida o conocida sin autorización.	pierdan completitud, coherencia o precisión.	disponible cuando se necesita por quien esté autorizado.
Personas	Esta dado por la información a la que tiene acceso un empleado según el cargo o rol que desempeñe. Aplica también para terceros.	Está dado por la información que puede modificar una persona, según su cargo o rol o tercero con o sin autorización y que ocasione pérdida de integridad a esta información.	Que la persona, rol o tercero no se encuentre disponible cuando se requiera.
Servicio	Que el servicio o que la información transportada o procesada por el servicio puedan ser accedidos o conocidos sin autorización.	Que el servicio, su configuración o que la información transportada o procesada por el servicio pierdan su completitud, coherencia o precisión.	Que el servicio o la información que transporta o procesa no estén disponibles cuando se necesita por quien esté autorizado.
Sitio	Que el sitio o lo que se necesite para su funcionamiento puedan ser conocidos o accedidos por terceros sin autorización.	Que el sitio o lo que se necesite para su funcionamiento pierdan su integridad	Que el sitio o lo que se necesite para su funcionamiento no esté disponible cuando se necesite.

Fuente: Autora a partir de JENNEX, Murray E. [177] (2009) y Financiera Comultrasan[178] (2010)

[177] JENNEX, Murray E. (2009). Assessing Knowledge Loss Risk. En: Conference: Proceedings of the 15th Americas Conference on Information Systems, AMCIS 2009, San Francisco, California, USA, August 6-9, 2009. DOI: 10.1109/HICSS.2013.103

[178] Financiera Comultrasan (2010). Esquema de valoración para el tratamiento de riesgos. En: Sistema de gestión de seguridad de la información NTC/ISO 27001:2005 para Financiera Comuntrasan asesorado por NewNet S.A.

3.3 ANÁLISIS DE LA GESTIÓN DE CONOCIMIENTO Y SEGURIDAD DE LA INFORMACIÓN

3.3.1 Estado de la gestión y seguridad del conocimiento y la información en las organizaciones de servicios en Colombia

Esta investigación se considera descriptiva, referida, principalmente, al estudio de los elementos constitutivos de las organizaciones de servicios, especialmente, instituciones de educación superior localizados en Colombia. Con respecto a los individuos que respondieron el cuestionario, cada individuo tanto de la UIS como de las demás organizaciones e instituciones a la que fue remitida a través de correo electrónico, redes sociales y la comunidad TEAM Ingeniería de conocimiento por medio de un afiche de difusión diseñado con código QR para facilitar el acceso (Ver Anexo 15). Las respuestas de acuerdo con la vinculación laboral del participante se presentan en la Tabla 7:

Tabla 7. Vinculación laboral participantes cuestionario SEGESCO

Vinculación laboral	Cantidad de Respuestas	Porcentaje (%)
Jefe de Proceso o Subproceso	44	48,35%
Profesional de Apoyo	25	27,47%
Auxiliar Administrativo	4	4,40%
Secretaria	2	2,20%
Técnico o Tecnólogo	2	2,20%
Otro	14	15,38%
Total	**91**	**100%**

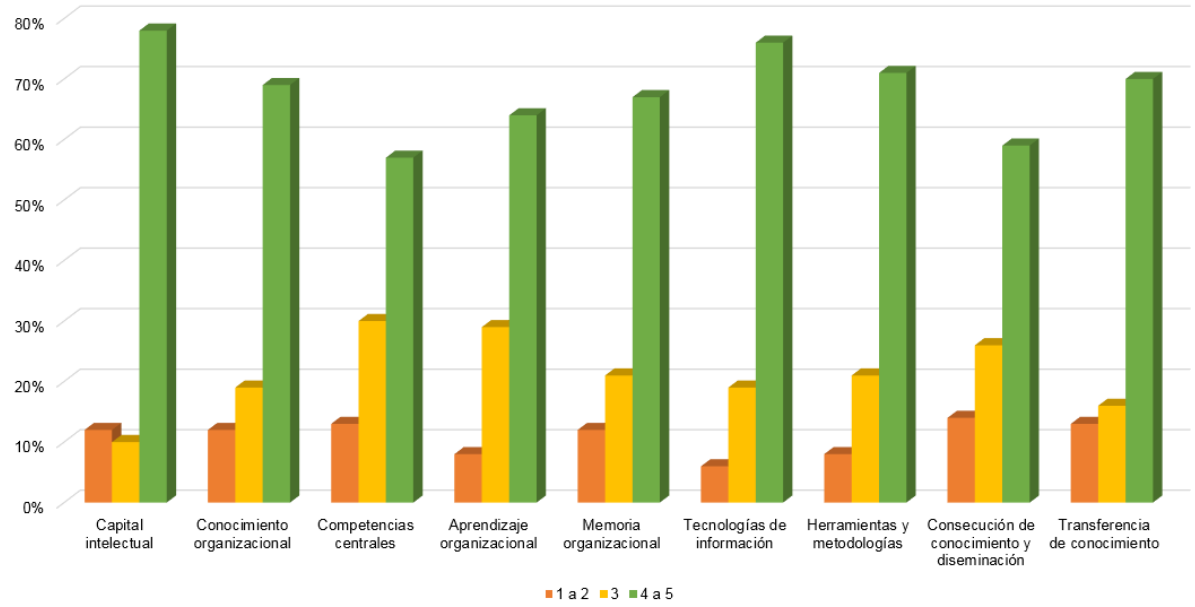
Fuente: Autora

De acuerdo con los resultados obtenidos para las instituciones y organizaciones participantes, los términos de mayor relevancia que denotan o indican conocimiento son: tecnologías de información, capital intelectual, herramientas y metodologías y, transferencia de conocimiento, puesto que más del 70% de las respuestas ubican

la calificación de estos términos en las puntuaciones 4 y 5 en una escala de Likert de 1 a 5, donde 1 era baja denotación y 5 alta denotación (Ver Ilustración 6).

Por otra parte, en lo que refiere al conocimiento organizacional, las competencias centrales, el aprendizaje organizacional, la memoria organizacional y la consecución de conocimiento y diseminación, los porcentajes están repartidos en un rango de 3 a 5, lo que quiere decir, que no hay una tendencia dentro de las organizaciones para considerar estos términos como conocimiento, lo que puede deberse al desconocimiento de dichos términos por parte de la institución. Se puede concluir que las organizaciones consideran como conocimiento todo aquello que les permite desarrollar y aplicar procesos y procedimientos para organizar mejor la información que poseen y generan con el fin de facilitar el uso y la aplicación de la misma a diferentes áreas.

Ilustración 6. Términos que denotan o indican conocimiento en la organización o institución



Fuente: Autora

Concepto de conocimiento y gestión del conocimiento

El 61,54% de las respuestas obtenidas muestran que las organizaciones asocian el concepto de gestión del conocimiento con la creación y la transferencia del conocimiento, el 16,48% con la Gestión de la información codificada (documentos, textos, artículos, investigaciones, manuales), el 15.38% lo asoció con el Aprendizaje organizacional, el 4.40% lo relacionó con el Capital intelectual y un 2.20% Sistemas tecnológicos (computadores). Además de esto, comentaron las siguientes frases las cuales relacionan con gestión del conocimiento:

- Análisis de datos.
- La colección de medidas establecidas con miras al aumento de la eficacia de las actividades realizadas en una organización, a través de la mejor utilización de los activos de conocimiento existentes dentro y fuera de la organización.
- Aprender a aprender.
- Identificación, captación, apropiación, asimilación, transferencia de conocimiento.
- Identificación, captura, procesamiento, transformación, y creación de nuevo conocimiento.

De acuerdo con esto se infiere que las organizaciones conciben la gestión del conocimiento como un proceso que se centra en la forma de crear, dar a conocer y administrar las actividades relacionadas con el conocimiento. Siendo que este concepto también implica la transmisión de habilidades y el desarrollo de las competencias necesarias al interior de la organización para compartirlo y utilizarlo entre sus miembros.

Proceso o área de la organización en la cual se generaba el mayor volumen de conocimiento importante

En cuanto al volumen de conocimiento que se genera de acuerdo con la fuente (Ver Tabla 8), el 30.12% de las organizaciones le otorgó un puntaje de 5 al conocimiento

creado de forma *Individual*, el 38.55% le dio un puntaje de 4, el 16.87% asignó un puntaje de 3, el 12,05% dio un puntaje de 2 y el 2,42% restante un puntaje de 1. Por otra parte, la generación de conocimiento de manera *Grupal homogéneo* (grupo con miembros de la misma área) obtuvo un puntaje de 5 por parte del 25.88% de las instituciones, un puntaje de 4 del 38.82% de ellas y el 23.53% le asignó un puntaje de 3. El otro 11.76% restante se repartió entre los puntajes 1 y 2.

En lo referente al conocimiento que se genera de manera *Grupal Heterogéneo* (Grupo con miembros de distintas áreas), 19 de las organizaciones, es decir, el 22.09% le asignaron un puntaje de 5, 32 de ellas (37.21%) le dieron un puntaje de 4, el 23.26% le asignaron un puntaje de 3. El 17.45% restante se repartió entre los puntajes 1 y 2. En cuanto a la generación de conocimiento de manera *Intergrupal* (entre grupos de distintas áreas) obtuvo un puntaje de 5 por parte del 17.44% de las instituciones, un puntaje de 4 del 32.56% de ellas, el 27.91% le asignó un puntaje de 3, el 12.79% le dio un puntaje de 2 y el 9,30% un puntaje de 1. Finalmente, en cuanto al volumen de conocimiento que se genera de manera *Mixta* (interna – externa, es decir, con personas ajenas a la empresa) el 15.12% de las instituciones le otorgó un puntaje de 5, el 32.56% le dio un puntaje de 4, el 25.58% asignó un puntaje de 3, el 15.12% dio un puntaje de 2 y el 11.63% restante un puntaje de 1.

Tabla 8. Fuentes que generan volumen importante de conocimiento en la organización o institución

Términos	1 a 2	3	4 a 5
Individual	14%	17%	69%
Grupal homogéneo (grupo con miembros de la misma área)	12%	24%	65%
Grupal Heterogéneo (grupo con miembros de distintas áreas)	17%	23%	59%
Intergrupal (entre grupos de distintas áreas)	22%	28%	50%
Mixta (interna – externa) (con personas ajenas a la organización)	27%	26%	48%

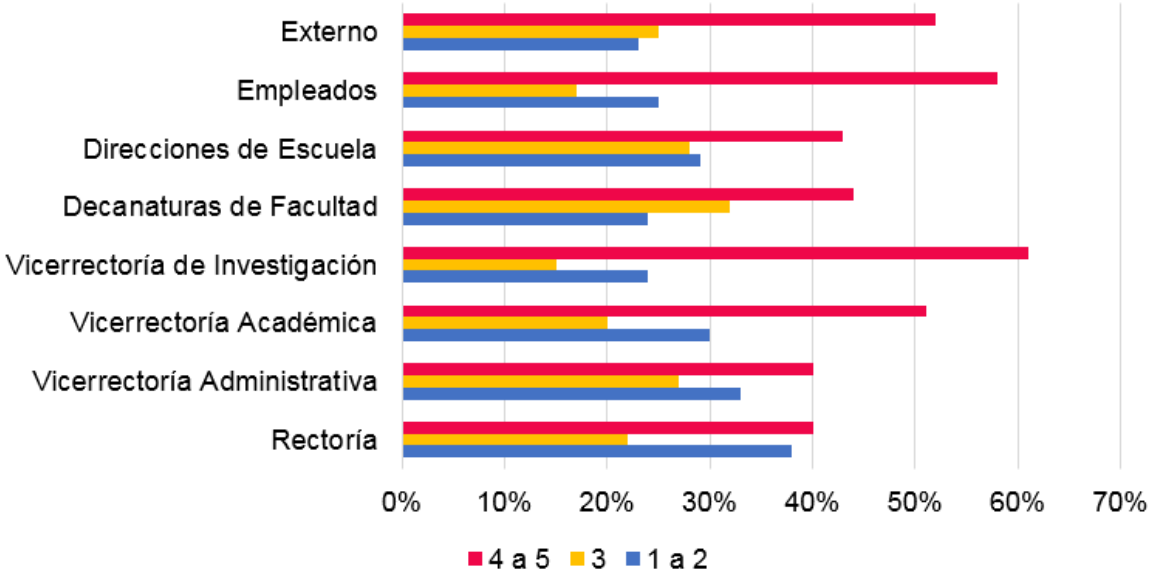
Fuente: Autora

Como conclusión, las calificaciones promedio se encuentran por encima de 3, esto indica que en un término medio en estas instituciones se está generando conocimiento de todas las maneras expuestas. De manera más específica, la información arrojada muestra que la mayor parte del volumen de conocimiento importante, que se genera en las organizaciones de servicio se da de forma individual puesto que más del 60% de las respuestas se ubican en el rango de 4 a 5 para este ítem, seguido del conocimiento generado de manera grupal homogéneo. La forma en la que menos se genera volumen de conocimiento importante en las organizaciones es Mixta (interna – externa) (con personas ajenas a la organización), por lo cual, se puede inferir que la mayoría de las organizaciones participantes, gestionan el conocimiento haciendo uso de la información y habilidades internas, y existe una oportunidad de mejora respecto a las rutinas de búsqueda de conocimiento externo en estas organizaciones, ya que a través de la colaboración con distintas fuentes de conocimiento tales como centros tecnológicos, universidades, clientes, proveedores de insumos y de tecnologías, intermediarios de innovación y competidores, entre otros, pueden incrementar su capacidad innovadora en cualquiera de sus distintas actividades[179].

Respecto al análisis de instituciones de educación superior (IES), según la ilustración 7, el volumen de conocimiento importante que proviene de *Rectoría*, el 59.72% de las instituciones lo puntuaron en un rango de 1 a 3, y el restante 40.28% de ellas calificaron de 4 a 5. Casi en igual proporción a la rectoría se presenta el volumen de conocimiento importante que proviene de *Vicerrectoría Administrativa* puesto que 59.99% de las instituciones lo puntuaron en un rango de 1 a 3, y el otro 40.01% de ellas lo calificaron de 4 a 5.

[179] BERNAL-TORRES, César Augusto y FROST-GONZÁLEZ Salomón. Innovación abierta en empresas colombianas: reto a superar. En: Revista Venezolana de Gerencia, Año 20. Nº 70, 2015, 252-267. ISSN 1315-9984

Ilustración 7. Volumen de conocimiento importante proveniente de las unidades o procesos de las IES



Fuente: Autora

Para el caso de la *Vicerrectoría Académica* el 49,3% de las entidades calificaron el volumen de conocimiento importante que proviene de allí en un rango de 1 a 3 y el 50,7% de ellas lo puntuaron entre 4 y 5. En lo que refiere al volumen de conocimiento importante que proviene de la *Vicerrectoría de Investigación* el 39.44% de las instituciones lo puntuaron en un rango de 1 a 3 y el 60.56% de ellas lo calificaron de 4 a 5.

Así también, al evaluar el volumen de conocimiento importante que proviene de *Decanaturas o Facultades* se obtuvo que el 15.49% señalaron con un puntaje de 5, y un puntaje de 4 fue señalado por el 28.17% de ellas, el 32.39% le asignó un puntaje de 3, el 11.27% le dio un puntaje de 2 y el 12.68% un puntaje de 1. En una proporción parecida a las decanaturas o facultades, el 20.29% de las instituciones calificaron el volumen de conocimiento importante que proviene de *Direcciones de Escuela*. Por su parte el volumen de conocimiento importante que proviene de los *Empleados,* el 58.33% de las instituciones lo calificaron en un rango de 4 a 5 y el

41.67% de ellas lo puntuaron entre 1 y 3. Finalmente, lo referente al volumen de conocimiento importante que proviene de *Fuentes Externas* fue calificado en el rango de 3 a 5 puntos por el 77% (Ver ilustración 7).

Acorde con los resultados se puede ver que aunque el volumen de conocimiento importante se da en todos los niveles de las instituciones, es notable que el conocimiento que proviene de los niveles más altos es menor al que proviene de los empleados o funcionarios, y a su vez este conocimiento es tan importante como el que proviene de la vicerrectoría de investigación, por tanto, se infiere que en las organizaciones hace falta más apropiación por parte de los altos mandos, acerca de la gran importancia de concentrar los esfuerzos en acciones para desarrollar la gestión de conocimiento de forma tal que este pueda convertirse en una ventaja competitiva.

Lo anterior, se debe a que, si bien la universidad es la institución por excelencia dedicada a la generación y transmisión del conocimiento[180], los participantes de este estudio consideran que son los docentes, los estudiantes, los grupos y centros de investigación quienes guardan una relación más estrecha con el volumen más importante de conocimiento. Lo anterior debido posiblemente a que la enseñanza, puede ser entendida como una actividad de transferencia en el proceso de la Gestión del Conocimiento –GC–, ya que cuando el conocimiento es creado y almacenado, debe ser transferido para que quien lo recibe lo haga propio y pueda hacer uso del mismo.

Asimismo, es relevante notar que, seguido a lo anterior, se destaca como un volumen de conocimiento importante el que proviene de fuentes externas, y aquí se incluyen los procesos de extensión y transferencia en los cuales la universidad

[180] BRUDNY, Paula (n.d.). Gestión del conocimiento en universidades. Examen de admisión al doctorado. Facultad de Ciencias Económicas – Orientación Administración.

establece vinculación con públicos más amplios que su alumnado, así como también realiza alianzas o trabajos conjuntos con otras entidades reconocidas.

Tabla 9. Volumen de conocimiento generado en los procesos de las IES

Términos	1 a 2	3	4 a 5
Financiero	19%	26%	54%
Gestión Documental	23%	32%	45%
Dirección Institucional	22%	33%	44%
Planeación Institucional	21%	21%	58%
Recursos Tecnológicos	15%	29%	56%
Recursos Físicos	31%	33%	36%
Servicios Informáticos y de Telecomunicaciones	16%	25%	59%
Admisiones y Registro Académico	25%	33%	42%
Contratación	32%	36%	32%
Talento Humano	21%	31%	49%

Fuente: Autora

Ahora bien, con relación al volumen de conocimiento importante generado en los procesos administrativos de las IES (Ver Tabla 9), el panorama cambia al del análisis anterior, y es precisamente en los procesos que se llevan a cabo por las instancias superiores de las IES los que, según los participantes de este estudio, aportan el mayor volumen de conocimiento a la institución.

De acuerdo con los resultados obtenidos (Ver ilustración 8), el volumen de conocimiento importante es generado por el proceso de dirección institucional, planeación institucional y talento humano. No obstante, si se amplía este análisis teniendo en cuenta los procesos evaluados con los puntajes 4 y 5, se observa que ahora los procesos más relevantes pasan a ser Financiero y servicios informáticos y de telecomunicaciones, con un 54 y 59% correspondientemente. Lo cual deja ver, que en todos los procesos se considera que se genera volumen de conocimiento importante. Lo anterior, podría deberse en parte, a que las organizaciones tienen

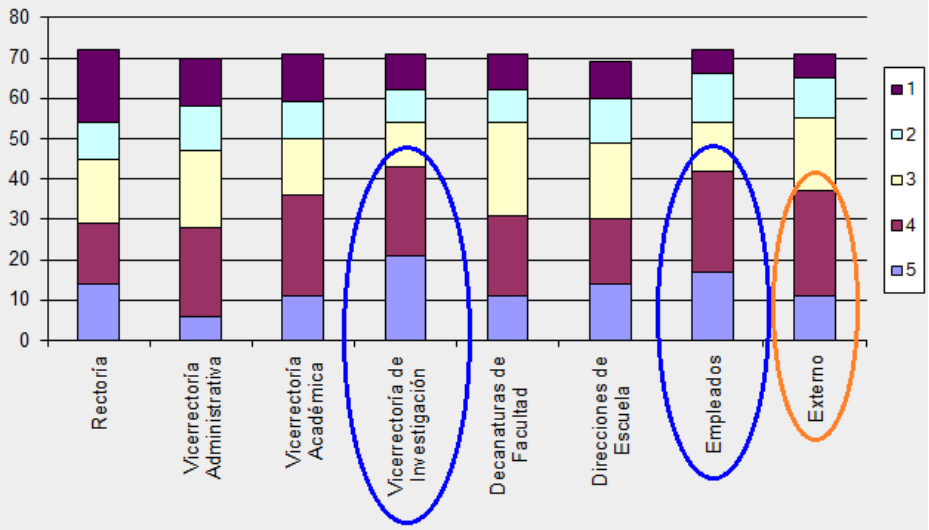
una sobrecarga de datos e información[181], pero no cuentan con activos de conocimiento claramente identificados, definidos y valorados.

Respecto a las responsabilidades, el 45.71% de las instituciones coincidieron en que la responsabilidad principal para capturar el conocimiento obedece a cada persona implicada, mientras que el 42.86% opina que esta responsabilidad debe recaer sobre los jefes de proceso o unidad, un 7,14% considera que debe ser responsabilidad de los especialistas en tecnologías de información y finalmente un 4,29% concluyó que no debe ser responsabilidad de nadie. Esto da por entendido que la mayoría de las instituciones tiene claro que el conocimiento debe contar con la participación activa de todos los empleados, pero además de esto, para que el conocimiento sea correctamente capturado debe existir una persona o grupo que tenga clara la responsabilidad de hacer este trabajo, encargado de iniciar, desarrollar y coordinar los programas de gestión del conocimiento de modo que se logre formar una estructura orientada al conocimiento y el monitoreo del mismo. No obstante, los resultados, aunque bajos de quienes consideran que no debe ser responsabilidad de nadie, sugiere que aún hay brechas que solucionar en cuanto a políticas o lineamientos de la gestión que debe hacerse del conocimiento. Asimismo, que sólo un 7,14% considere que debe ser responsabilidad de los especialistas en tecnologías de información, evidencia que aunque hay instituciones conscientes del empleo de las TIC, es un porcentaje muy bajo, y puede intuirse que se están subutilizando los sistemas de información, por lo cual se debe trabajar en esta falencia, ya que, según el modelo de Minakata[182] las tecnologías de la información y la comunicación son el principal apoyo de la gestión del conocimiento, al analizar esto desde el contexto educativo, se entiende que las TIC facilitan la elaboración de modelos mentales, e instrumentos que ayuden al fortalecimiento del aprendizaje.

[181] SÁNCHEZ AGUILAR, Antonio. Implicaciones de las Tecnologías de Información: Manejo del conocimiento. [Diapositivas]. LANIA, Xalapa. Septiembre, 2004. 37 diapositivas. (Consultado: 19 de agosto de 2015) http://www.slideshare.net/radarik/implicaciones-de-las-tecnologas-de-informacin-manejo-del-conocimiento (asanchez@mail.udlap.mx)

[182] Minakata, A (2009). Gestión del conocimiento en educación y transformación de la escuela. Revista Electrónica Sinéctica, 32.

Ilustración 8. Conocimiento importante proveniente de las siguientes Unidades o áreas en las IES



Fuente: Autora

Con relación al grado de obtención de conocimiento tácito, la mayor fuente de obtención de conocimiento tácito por parte de las instituciones se da mediante entrevistas, discusiones informales y discusiones formales, puesto que más del 70% de las respuestas ubican estos términos en un rango entre 3 y 5. El escenario que menos representa obtención de conocimiento tácito para las instituciones son las entrevistas de salida, ya que casi el 50% de las respuestas obedecieron a calificaciones entre 1 y 2, y es precisamente otro punto por mejorar, puesto que, la persona que no comparte sus conocimientos dentro de la organización puede representar una pérdida para esa organización, sobre todo en el momento de su salida o traslado a otra institución, ya que el conocimiento es creado por el individuo quien es el principal repositorio de conocimiento[183] [184].

[183] Mírian Oliveira, Carla M.M. Curado, Antonio C.G. Maçada, Felipe Nodari, Using alternative scales to measure knowledge sharing behavior: Are there any differences?, Computers in Human Behavior, Volume 44, March 2015, Pages 132-140, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2014.11.042.

[184] Ma, Z., Qi, L., & Wang, K. (2008). Knowledge sharing in Chinese construction project teams and its affecting factors. Chinese Management Studies, 2(2), 97–108.

Importancia y asignación de recursos que da la institución a los procesos de gestión del conocimiento

Respecto a los recursos financieros facilitados por las instituciones para el proceso de compartir el conocimiento, el cual va más allá de la entrega de un manual e implica la comunicación, reproducción y conversación en equipos multidisciplinarios[185], el 15.63% de las respuestas obtenidas coinciden en que la institución si facilita los medios y/o asigna los recursos financieros para compartir el conocimiento, mientras que el 35,94% opinan que son aceptables. Por su parte, un 48,86% opina que la institución invierte poco, muy poco o no está ni facilitando los medios ni asignando los recursos financieros para compartir el conocimiento.

De lo anterior se revela que casi la mitad de las instituciones encuestadas aun no son conscientes de la importancia de definir y potenciar las ventajas competitivas de la organización a partir de la gestión del conocimiento, dado estas entidades encuestadas reconocen no estar adelantando iniciativas de gestión del conocimiento. Esto en parte podría explicarse, teniendo en cuenta que este estudio estuvo dirigido a instituciones del sector público, y aunque DataQuest estima que los gobiernos gastan en el diseño de las iniciativas de gestión de conocimiento alrededor del 30% del total de presupuesto en gestión de conocimiento; el sector privado, por su parte, invierte un porcentaje mayor de recursos en este tipo de iniciativas[186].

[185] SÁNCHEZ AGUILAR, Antonio. Implicaciones de las Tecnologías de Información: Manejo del conocimiento. [Diapositivas]. LANIA, Xalapa. Septiembre, 2004. 37 diapositivas. (Consultado: 19 de agosto de 2015) http://www.slideshare.net/radarik/implicaciones-de-las-tecnologas-de-informacin-manejo-del-conocimiento (asanchez@mail.udlap.mx)

[186] Morrissey, S. (2005). *The Design and Implementation of Effective Knowledge Management Systems.* Philadelphia: The Wharton School.

Papel de las TIC en la gestión del conocimiento

Acerca de los canales de transferencia de conocimiento más importantes en las instituciones de servicio más del 65% definen que son el internet y los cursos de formación (internos y externos), seguidos de las reuniones internas periódicas con un 60% de respuestas en las calificaciones 4 y 5. El canal que menos es utilizado para la transferencia de conocimiento en las instituciones encuestadas son las reuniones externas, las cuales son un espacio para la generación de redes. A esto, por tanto, se debe prestar suma importancia, dado que se ha documentado que las organizaciones con vínculos de comunicación eficientes tienen mejores flujos de información, transferencia de conocimiento, cooperación, resolución de problemas y productividad; adicionalmente, cuando se logran desarrollar redes se produce un aprendizaje más rápido, mejor resolución de problemas, no hay duplicación de esfuerzos y nuevas iniciativas para la transferencia de conocimiento[187].

Sumado a lo anterior, el porcentaje de satisfacción de las instituciones encuestadas por la forma en que la alta dirección fomenta la cultura de trabajo colaborativo e intercambio de conocimiento y la manera en cómo se da el flujo horizontal de información es del 31.51%, Por su parte el porcentaje de insatisfacción con estos aspectos es del 21.87%.

Por otro lado, un 40.63% de las instituciones que respondieron esta pregunta afirman no sentirse ni satisfechos ni insatisfechos, por lo que se infiere que existe desinformación con respecto al tema en estas instituciones, o hace falta compromiso y responsabilidad por parte de la alta dirección y de cada uno de los miembros de la organización, para el desarrollo de prácticas de promoción para suscitar la colaboración. Por otra parte, respecto al flujo de información muestra que este en gran parte no es horizontal sino jerárquico, es decir, existen nociones de

[187] Morrissey, S. (2005). Op. Cit.

mando y autoridad para que los miembros de las instituciones se vean limitados a trabajar con la información que requieren para el ejercicio de sus funciones y no sean vistos como consumidores, procesadores y generadores de información y de conocimiento.

Seguridad del conocimiento y las buenas prácticas de seguridad de la información

En cuanto al grado de responsabilidad en la gestión de la seguridad de la información y el conocimiento, los resultados evidencian que, en orden, los encuestados consideran que es la gente dentro de la organización y los usuarios finales de la información, con un 63,34% y un 58,33% correspondientemente, seguidos de los especialistas en TI con un 55%, la fuerza propia de la tecnología con un 45% y finalmente, los proveedores o consultores con un 35%. De lo anterior se puede decir que el tema de seguridad de la información no le compete sólo a unos cuantos, sino que debe tomar parte toda la organización.

Lo anterior, se relaciona con la gobernanza de un sistema de gestión en este caso de seguridad de información y conocimiento. Se inicia por el liderazgo y compromiso que debe demostrar la alta dirección, asegurando según la norma ISO/IEC 27001:2013:

a. Que sea establecida una política alineada a los objetivos de la institución y que estos sean compatibles con la dirección y planeación estratégica (Ver Anexo 9. Políticas de gestión de seguridad de la información y el conocimiento para la UIS). Las políticas deben ser generadas de acuerdo con las necesidades y expectativas de las partes interesadas, no obstante, se recomienda hacer una revisión previa de políticas en organizaciones similares (Ver Anexo 13. Ejemplos de políticas existentes en Instituciones de Educación superior).

b. La integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización, lo que implica una caracterización de los procesos
c. Que los recursos necesarios para el SGSI estén disponibles y promoviendo la mejora continua.

Según Basie von Solms y Rossouw von Solms[188], uno de los pecados mortales en un plan de gobierno o un plan corporativo de seguridad de la información es no darse cuenta de que la seguridad de la información es un asunto de negocios y no un problema técnico, de esta manera se entiende porque menos de la mitad de las respuestas consideran que la tecnología tenga un grado de responsabilidad alto (4 o 5). La consecuencia, por tanto, de delegar del todo este tema a los departamentos técnicos, podría resultar no sólo en dinero malgastado sino, además, quedarse con una solución arcial, y no lograr nunca una solución total o integral.

Asimismo, se tiene también claro que, aunque con un menor grado de responsabilidad, los proveedores o consultores, quienes también aportan a la gestión de seguridad de la información y el conocimiento. Según la norma ISO/IEC 27001:2013 uno de los 14 dominios es precisamente el A.15 relaciones con los proveedores que implica acordar políticas de accesos de proveedores a los activos de la organización, documentar y llevar la trazabilidad de los conocimientos que se intercambian; además de, establecer y acordar todos los requisitos de seguridad pertinentes para que cada proveedor, contratista o consultor pueda tener acceso, procesar, almacenar, comunicar o suministrar no sólo componentes de infraestructura de TI para la información y conocimiento de la organización, sino también atendiendo a acuerdos de confidencialidad y de propiedad intelectual, se logre una interacción y flujo seguro de la información y el conocimiento, que

[188] Basie von Solms, Rossouw von Solms, The 10 deadly sins of information security management, Computers & Security, Volume 23, Issue 5, July 2004, Pages 371-376, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2004.05.002.

contribuya a su vez con la visión de innovación abierta en una economía del conocimiento, que requiere una aproximación distinta del concepto de capital, es decir, es necesario el establecimiento de políticas diseñadas para obtener del entorno talento y novedad, más que insumos o maquinaria[189].

En lo que respecta a los métodos y herramientas que apoyan el intercambio de conocimiento, para las organizaciones las que mayor aporte o contribución significan en cuanto a crear y/o compartir el conocimiento y la información, son en primer lugar con un 68% las lecciones aprendidas de los trabajos en equipo; seguido con un 65% están las prácticas de mentoring, coaching y tutorías; continuo con un 62% están las reuniones planeadas formalmente cara a cara, y con este mismo porcentaje están las capacitaciones y entrenamientos; por último, con un 60% se considera también importante con una calificación de 4 o 5 las herramientas tecnológicas colaborativas (sharepoint, directorio activo, correo). Lo anterior, según el Comité Europeo De Normalización (CEN) se explica porque, aunque la actividad de compartir conocimiento puede tener lugar de muchas maneras, y el conocimiento puede estar almacenado en bases de datos o distribuido a través de documentos, lo cual se conoce como "enfoque de stock"; la mayor parte del conocimiento puede ser transferido de una persona a otra a través de la interacción directa, a través de la colaboración, talleres, coaching, aprendizajes, etc. Esta transferencia de conocimiento directamente entre personas puede llamarse el "enfoque de flujo".

En lo relativo a la importancia de los planes a futuro para las instituciones en relación con la gestión sistemática de la seguridad del conocimiento y la información, las respuestas indican que todos los planes a futuro indicados en la Tabla 10 son importantes, ya que todos ellos tienen una calificación en el rango de 4 a 5 de más del 60% de las instituciones, a excepción de “Aumentar y compartir el conocimiento con proveedores” cuyo porcentaje en dicho rango es el 41%.

[189] COLOMBIA. UNIVERSIDAD MANUEL BELTRÁN. [base de datos en línea]. [consultado 10 abr.2016]. Disponible en< http://www.umb.edu.co/>

Tabla 10. Perspectivas futuras acerca de la gestión de la seguridad del conocimiento y la información

Términos	1 a 2	3	4 a 5
Aumentar y compartir el conocimiento con proveedores	28%	31%	41%
Aumentar y compartir el conocimiento con usuarios (Mejorar el aprendizaje organizativo)	10%	21%	69%
Desarrollar acuerdos de implementación de tecnología	12%	23%	65%
Mejorar los medios para compartir la información con los empleados	16%	5%	79%
Mejorar la eficacia/rendimiento de los procesos o unidades	10%	17%	72%
Mejorar los servicios prestados	12%	12%	76%
Reducir los costos de operación	16%	17%	67%
Fomentar la innovación y alcanzar nuevos mercados	14%	9%	78%

Fuente: Autora

El instrumento de investigación también indago acerca de las políticas de seguridad de la información, ya que son una base necesaria de los programas de seguridad organizacional[190]. En este aspecto, el 50.94% de las instituciones afirman que, si cuentan con una política documentada y actualizada de protección y acceso a la información y el conocimiento, mientras que un 33.96% de ellas no la tienen. Un 15.09% no sabe si la organización la tiene o no. Los resultados muestran que aún existe un amplio número de instituciones con dificultades en la planificación y coordinación de todos los recursos relacionados con el conocimiento, tanto tácito como explícito. Esto indica que gran parte de estas instituciones no podrían garantizar que los riesgos de la seguridad de la información sean conocidos, gestionados y minimizados por la organización de una forma documentada, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

[190] Kenneth J. Knapp, R. Franklin Morris Jr., Thomas E. Marshall, Terry Anthony Byrd, Information security policy: An organizational-level process model, Computers & Security, Volume 28, Issue 7, October 2009, Pages 493-508, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2009.07.001.

No obstante, tener una política establecida no garantiza necesariamente la seguridad de la información[191]. El mal cumplimiento de las políticas de seguridad de la información por parte de los empleados es un problema perenne para muchas organizaciones. Se ha demostrado que aproximadamente la mitad de todas las infracciones de seguridad causadas son accidentales[192] [193]. Por lo anterior, una forma de mitigar este incumplimiento de la política es evaluar la forma como se comunica la misma dentro de la organización. El análisis permitió determinar que en el 30.19% de las organizaciones participantes la política se comunica por medio de correo electrónico, en igual proporción (30.19%) otras respondieron que esta política se comunica por medio de actividades de capacitación (charlas, conferencias, seminarios, etc.), un 20.75% afirma que se informa por medio del manual de seguridad, un 24.53% lo hace a través de la página institucional, y una pequeña parte de ellas (5.66%) lo hace mediante folletos.

Por otra parte, existe un gran porcentaje de ellas (32.08%) que a pesar de contar con una política de protección y acceso a la información y el conocimiento afirman que esta política no se comunica. Lo cual obstaculiza aún más la distribución acertada la información a todas las áreas de la organización.

Sumado a lo anterior, y teniendo en cuenta que los empleados en una organización no son homogéneos[194], Stahl et al.[195] sugieren que las políticas de seguridad de la

[191] Fredrik Karlsson, Karin Hedström, Göran Goldkuhl, Practice-based discourse analysis of information security policies, Computers & Security, Volume 67, June 2017, Pages 267-279, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.12.012.
[192] ENISA threat landscape 2014. Overview of current and emerging cyber-threats
European Union Agency for Network and Information Security (2014) Technical Report
[193] Cheryl Vroom, Rossouw von Solms, Towards information security behavioural compliance, Computers & Security, Volume 23, Issue 3, 2004, Pages 191-198, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2004.01.012.
[194] Beautement, A; Becker, IF; Krol, K; Parkin, S; Sasse, MA; (2016) Productive Security: A scalable methodology for analysing employee security behaviours. [Dataset]. Twelfth symposium on usable privacy and security (SOUPS 2016)
[195] Bernd Carsten Stahl, Neil F. Doherty, Mark Shaw (2012). Information security policies in the UK healthcare sector: a critical evaluation. En: Information Systems Journal, vol. 22, No. 1, pp. 77–94. doi:10.1111/j.1365-2575.2011.00378.x

información sean "orientaciones orientadas a los empleados" y que "los contenidos técnicos para audiencias especializadas" estén en apéndices. Esto contribuiría al fomento de un ambiente que favorece la seguridad de la información o del conocimiento gestionado o transferido, y aunque más del 50% de las organizaciones participantes afirmaron que, si se fomentan estos ambientes, existe también un alto porcentaje de estas que no lo hace, ya sea por falta de apoyo de la alta dirección o porque aún no es muy claro y genera confusiones toda la temática. Entonces, se sugiere dado que el primer objetivo de control de la norma ISO/IEC 27001:2013 son las políticas de seguridad de la información, adaptar estas políticas a las prácticas laborales de los empleados, de esta manera, hay menos necesidad de soluciones alternativas[196]. Además, los empleados no se quedan con la decisión de priorizar entre la seguridad de la información y su práctica laboral[197]. En consecuencia, aliviaría la carga de los empleados para cumplir con las políticas de seguridad de la información, que según Adams y Sasse[198], también aumentaría la motivación de la seguridad de la información.

Ordenando de mayor a menor, se presentan a continuación en la Tabla 11 los aspectos que para las instituciones deben estar incluidos en la política de seguridad de la información y el conocimiento de la Institución.

Tabla 11. Aspectos que deben estar incluidos en la política de seguridad de la información y el conocimiento

Aspecto de la política	%
Roles y responsabilidades en seguridad de la información	**79,25%**

[196] Fredrik Karlsson, Karin Hedström, Göran Goldkuhl, Practice-based discourse analysis of information security policies, Computers & Security, Volume 67, June 2017, Pages 267-279, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.12.012.
[197] KIRLAPPOS, Iacovos; BEAUTEMENT, Adam y SASSE, M. Angela (2013). “Comply or Die” Is Dead: Long Live Security-Aware Principal Agents. Financial cryptography and data security – FC 2013 workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Lecture Notes in Computer Science, vol 7862. Springer-Verlag, Berlin Heidelberg, pp. 70–82.
[198] ADAMS, Anne y SASSE, Martina Angela (1999). Users are not the enemy. En: Communications of the ACM, Volume 42 Issue 12, Pages 40-46. DOI: 10.1145/322796.322806

Aspecto de la política	%
Clasificación de la información (pública, confidencial, restringida...)	66,04%
Objetivos de seguridad de la información	62,26%
Monitoreo de amenazas relacionadas con el entorno	56,60%
Registro de eventos, incidentes, debilidades y lecciones aprendidas	56,60%
Acceso a la infraestructura tecnológica, redes y servicios de red	54,72%
Programas de sensibilización, formación o educación	50,94%
Gestión de contraseñas y autenticación de usuarios	50,94%
Procesos disciplinarios en caso de fuga de información o conocimiento sensible	49,06%
Estructura de la evaluación y gestión del riesgo	45,28%
Protocolo de conexión remota o teletrabajo	43,40%
Instalación de software o sistemas operativos	43,40%
Requerimientos estatutarios, reguladores y contractuales relevantes	43,40%
Uso de controles criptográficos	39,62%
Registro, revisión y cancelación del registro de usuarios y los derechos de acceso	37,74%
Manejo de los dispositivos móviles y medios removibles	37,74%
Mantenimiento, reutilización y disposición final segura de los equipos	33,96%
Control de acceso a las instalaciones físicas	28,30%
Asignación de activos	26,42%

Fuente: Autora

Dentro de los aspectos más importantes que consideran los encuestados que deben estar incluidos en la política de seguridad de la información y el conocimiento de la institución se encuentran: roles y responsabilidades en seguridad de la información (79,25%), clasificación de la información como pública, confidencial, restringida, etc., (66,04%), objetivos de seguridad de la información (62,26%), monitoreo de amenazas relacionadas con el entorno (56,6%). es decir, para los encuestados lo principal es que cada persona por medio de un conjunto de directrices previamente definidas tenga claro su rol en el proceso, de forma tal, que se garantice el buen uso

de la información y por tanto una adecuada gestión de los activos de conocimiento, ya que la premisa para la gestión del conocimiento es que, entre muchos otros factores, el comportamiento efectivo e inteligente depende de tener un entendimiento apropiado además de estar informado[199].

En cuanto a los controles de seguridad de la información y conocimiento que se encuentran implementados actualmente en la instituciones, las respuestas obtenidas muestran que el control de seguridad usado por la mayoría (80,77%) son las copias de seguridad de la información, seguido con un 59,62% los acuerdos de confidencialidad o de no divulgación, luego con un 57,69% cada uno, están los controles de seguridad de la red interna (intranet) y los control de acceso a equipos, software e información. todos los demás controles estaban implementados en menos de la mitad de las organizaciones participantes. los controles menos implementados son el inventario de activos, las responsabilidades o roles definidos, el registro de lecciones aprendidas y el procedimiento para el tratamiento de incidentes de seguridad con externos. si se comparan las respuestas con mayor porcentaje, con las menos seleccionadas, se puede entrever que los controles seguridad de la información y conocimiento son más de seguridad informática más no de seguridad de la información, y menos de asegurar el conocimiento.

También se evalúo la importancia dada en cada unidad o proceso de las organizaciones participantes a cada uno de los temas o aspectos presentados en la Tabla 12. Los resultados obtenidos son alarmantes, ya que en ninguno de los aspectos se obtuvo un porcentaje cercano a 100% en el rango 4 a 5, es decir, no hay conciencia o no se dan cuenta del papel importante de las prácticas para la gobernanza de la seguridad de la información, y por ende, tienen en poco las amenazas a la seguridad de la información y la conservación del conocimiento, y

[199] Karl M. Wiig, (2002) "Knowledge management in public administration", Journal of Knowledge Management, Vol. 6 Issue: 3, pp.224-239, doi: 10.1108/13673270210434331

por tanto, a la materialización de los riesgos y su impacto ya sea sistémico, financiero, en los objetivos o en la imagen institucional.

Tabla 12. Importancia dada en la unidad o proceso a cada uno de los aspectos de seguridad de información

Términos	1 a 2 Nula/Poca	3 Media	4 a 5 Alta/Muy Alta
Seguridad de la información	12%	22%	66%
Rol desempeñado por cada integrante en la seguridad de la información	16%	32%	52%
Responsabilidad que usted tiene en la seguridad de la información	12%	30%	58%
Clasificación de la información	14%	32%	54%
Reporte de eventos que constituyan un incidente de seguridad de la información	26%	34%	40%
Usos autorizados de los activos	22%	26%	52%

Fuente: Autora

En este orden de ideas, también se indagó sobre los procedimientos que se llevan a cabo cuando ingresa un nuevo funcionario o persona a la unidad o proceso de la institución, y se obtuvo que en el 70% de las organizaciones se hace una presentación del equipo de trabajo, pero sólo en el 50% se firma un acuerdo de confidencialidad y se asignan sus activos de información, físicos, y tecnológicos. Aún más preocupante, en el 24% se imparte un programa de sensibilización o educación sobre seguridad de la información y en el 16% de los casos se socializa la normatividad sobre el tema. Por tanto, podría concluirse que dentro de las organizaciones participantes los procesos de nuevo ingreso se basan en ayudar al empleado a integrarse al proceso, pero se deja de lado motivar al empleado desde el inicio a cumplir con un conjunto de reglas y políticas relacionadas con el acceso y el uso de los activos de información y conocimiento de la organización.

No obstante, se podría aprovechar el interés de hacer sentir integrado a los nuevos funcionarios, dado que, por el trabajo en grupo o equipo, el comportamiento u opiniones de los empleados probablemente son influenciados entre ellos, se podría intentar influir tanto en las normas personales como en las normas sociales. Es decir, gracias a que las normas sociales, basadas en las interacciones sociales entre los individuos, definen ampliamente reglas de comportamiento basadas en creencias comunes sobre cómo las personas deben actuar en una situación particular, se podría promover indirectamente el conjunto de sub-políticas de apoyo de seguridad de información y conocimiento. Por otro lado, las normas personales son normas privadas e internalizadas basadas en las creencias y valores propios[200], sin embargo, se podría a través de las normas sociales afectar el comportamiento de un individuo y que las acepte e internaliza como normas personales, y de esta manera probar la hipótesis propuesta por Yazdanmehr y Wang[201], quienes afirman que las normas personales relacionadas con la seguridad de la información y el conocimiento tienen una influencia positiva en el cumplimiento del conjunto de reglas o directrices de la política de seguridad.

En este sentido, se valoró finalmente las prácticas que los participantes consideraban sobresalen dentro de las organizaciones participantes, y se encontró que las organizaciones consideran importante la labor del empleado; sus empleados tienen clara la estrategia, misión, valores, objetivos y normas; consideran importante estar en contacto continuo con todo el entorno y desarrollar redes de comunicación; tienen definidos los puestos de trabajo y las líneas de mando así como cuentan con manuales y documentos y, tienen en cuenta los conocimientos e ideas de los empleados en la organización. Por el contrario, las

[200] P.C. Stern, T. Dietz, T. Abel, G.a. Guagnano, L. Kalof. A value-belief-norm theory of support for social movements: the case of environmentalism. Human Ecology Review, 6 (1999), pp. 81–97

[201] Adel Yazdanmehr, Jingguo Wang, Employees' information security policy compliance: A norm activation perspective, Decision Support Systems, Volume 92, December 2016, Pages 36-46, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2016.09.009.

prácticas que los participantes consideran que las organizaciones no fomentan son, la opinión subjetiva en ocasiones no es permitida en todos los niveles, cometer errores no son considerados oportunidades de aprendizaje, no se cuenta con constante actualización de los procesos dentro de la organización y no se considera apropiada la actitud de los que toman riesgos.

3.3.2 Análisis de la tendencia en materia de gestión y seguridad del conocimiento y la información en Latinoamérica

De acuerdo con los resultados obtenidos por la Asociación Colombiana de Ingenieros en Sistemas (ACIS), el Centro de Atención de Incidentes de Seguridad Informática y Telecomunicaciones – ANTEL de Uruguay, el Capítulo Buenos Aires de ISACA y la organización ISACA de Perú, a continuación se presentan apartes relevantes sobre los resultados de la encuesta latinoamericana de seguridad de la información que se viene realizando año a año desde el 2009, en la cual Colombia siempre ha presentado el porcentaje más alto de participación (42,22%), frente a los demás países participantes, seguido de Perú (15%), Argentina (23,33%), y otros países: Chile, Costa Rica, México, Uruguay, Paraguay, Cuba, Ecuador, Panamá, Portugal, Puerto Rico, y Venezuela[202].

Inversión en seguridad

En el periodo comprendido entre el 2009 y el 2012 los temas en los cuales las organizaciones concentraban la inversión en seguridad de la información eran: protección de la red, proteger los datos críticos de la organización, seguridad de la información y proteger el almacenamiento de datos de clientes. Aunque a lo largo de los años estas asignaciones han marcado la pauta de inversión en seguridad de la información al interior de las organizaciones, a partir del 2012 es posible apreciar incrementos marcados en cuanto al monitoreo de seguridad informática 7x24,

[202] CANO, M. Jeimy J.; SAUCEDO, Meza, Gabriela María (2012). IV Encuesta Latinoamericana de Seguridad de la Información, Tendencias 2012.

evaluaciones de seguridad internas y externas, y desarrollo y afinamiento de la seguridad de las aplicaciones. Adicional, en el año 2013 surgieron cuatro nuevos rubros de inversión: Desarrollo de políticas y procedimientos de seguridad, estrategias de protección para dispositivos móviles, protección de los datos en la nube y el cumplimiento de exigencias legales y corporativas en cuanto a seguridad de la información.

Presupuesto de la inversión

En cuanto a la cantidad de dinero que las organizaciones destinan para mantener en óptimo estado el aseguramiento de los activos de información, aproximadamente el 50% destinan un presupuesto inferior a USD$50.000, en promedio un 17% destina entre los USD$50.000 y USD$70.000 y un 15% destinan más de USD$130.000. A pesar de lo anterior, el porcentaje de organizaciones que cuentan con un presupuesto asignado para la seguridad de la información (SI) ha venido disminuyendo en los últimos años[203], lo anterior se evidencia en que para los años 2011 y 2012 más del 70% de las organizaciones tenían un presupuesto asignado para SI, a partir del 2013 este porcentaje ha estado por debajo del 60%, y en 2016 llegó a ser del 55%.

Fallas de Seguridad

Desde el año 2009 hasta la actualidad, las principales fallas en seguridad se han presentado por: virus/caballos de troya, instalación de software no autorizado y accesos no autorizados a la web. Sumado a esto, existen otro tipo de fallas como lo son los accesos no autorizados a la web, pérdida de la integridad de la información y la manipulación de aplicaciones de software, sin embargo, estas fallas han venido disminuyendo desde el año 2013, mientras que han aumentado desde el año 2012 las fallas como el Phishing.

[203] CANO, M. Jeimy J.; SAUCEDO, Meza, Gabriela María (2012). VIII Encuesta Latinoamericana de Seguridad de la Información, Nuevos horizontes para América Latina.

Notificación de Incidentes

Hasta el año 2011 los incidentes eran notificados en su mayoría al equipo de atención de incidentes o no eran notificados. Sin embargo, a partir de este año se empezó a evidenciar un notable aumento en el porcentaje de organizaciones que notificaban los incidentes a los directivos de la organización pasando de un 0% de notificaciones en el periodo comprendido entre el 2009 y el 2010 a un 44,76% en el 2011 y posteriormente a un 57,1% en el 2015, lo cual indica que es clara la participación e interés que se denota por parte de los directivos quienes se involucran en los sucesos e implicaciones de los incidentes informáticos. Por otra parte, también se observa que la tendencia a no denunciar ha venido disminuyendo, pasando de un 39.30% en 2009 a un 15% referido durante los años 2015 y 2016. Según el 25% de las organizaciones participantes, el motivo por el cual no denuncian se relaciona con la publicación de noticias desfavorables en los medios, lo cual ocasiona pérdida de la imagen empresarial ante la sociedad. En cuanto a los involucrados en realizar los reportes de incidentes, en su mayoría son los empleados o el análisis de registros de auditorías/Sistema de archivos/Registros Firewall.

Políticas de Seguridad

Respecto al desarrollo de políticas de seguridad se ha avanzado paulatinamente, desde el año 2011 las empresas que cuentan con una política formal, escrita, documentada e informada a todo el personal superan el 40% lo cual refleja el esfuerzo de las organizaciones, la preparación de los responsables de esta buena práctica y la concientización que hasta el momento se ha logrado. De acuerdo con la VIII encuesta latinoamericana de seguridad de la información, para el 2016 el 41,54% de las grandes empresas realizan evaluaciones de seguridad de la información, el sector con mayor número de evaluaciones es el gobierno/Sector público con un 32,31%. Los resultados también muestran que el 47% de las empresas desarrollan procesos de evaluación de riesgos y el 87% cuentan con metodologías de gestión de riesgos, dentro de las cuales se destacan: la ISO 31000

(23%), la ISO 27001 (22%), GRC (Governance, Risk & Compliance) (13%) y Magerit (12%). Uno de los motivos por los cuales existen empresas que no cuentan con una metodología para la gestión de riesgos corresponden a no tener un proceso formal de gestión de riesgos ni corporativo ni de información.

Obstáculos para la seguridad

Para el año 2015, los principales obstáculos para la seguridad de la información seguían siendo la Falta de colaboración entre áreas/departamentos, la falta de apoyo directivo, poca visibilidad del tema a nivel ejecutivo, poco entendimiento de la seguridad de la información y falta de tiempo. Aunque estos disminuyeron para el año 2016, surgieron nuevos obstáculos, entre los que se encentran, la ausencia de una cultura de la seguridad de la información y la escasa formación en gestión de la seguridad de la información.

Responsabilidad de la SI

Durante los años 2012, 2013 y 2014 en más del 30% de las empresas la responsabilidad de la seguridad de la información recaía sobre el director del departamento de sistemas/tecnología, un 16% en promedio a un cargo no especificado, un 13% a otros cargos (Consultores, abogados, docentes, fraud managers) y en sólo un 25% de estas empresas, se contaba con un director de seguridad de la información (SI). A partir del 2015, cambia el panorama, y se hace más fuerte la presencia en las organizaciones de una persona encargada de la seguridad de la información. Lo cual explica porque para el año 2016 en el 43% de las empresas se contaba con un director de SI. Sumado a esto, disminuyó el porcentaje de empresas donde el encargado de la seguridad de la información era principalmente el director del departamento de sistemas/tecnología que pasó de un porcentaje superior al 30% en el periodo 2012-2014, a un 13,7% y 16% en los años 2015 y 2016 respectivamente. Por tanto, como lo menciona la IV encuesta nacional sobre seguridad informática, se observa que dentro de las organizaciones ha crecido la necesidad de cuidar el valioso activo “Información”.

3.3.3 Medición del nivel de madurez del proceso de seguridad de la información en la UIS

En la actualidad, la Universidad Industrial de Santander -UIS- cuenta con un sistema de gestión integrado NTCGP 1000:2009 – NTC ISO 9001:2008 – NTC ISO 14001:2004 – NTC OHSAS 18001:2007 (Ver Anexo 14), y adelanta actualmente el proyecto de “Implementación del Sistema de Gestión Integrado en las actividades de docencia, investigación y extensión, y en los procesos de apoyo al cumplimiento de su misión institucional”, con el objetivo de contribuir a la calidad de sus productos y servicios, la salud en relación a enfermedades profesionales y accidentes de trabajo, y, al desarrollo sostenible y el cumplimiento de las normas legales aplicables. Adicional, se encuentra en el proceso de acreditación por la Comision Nacional del Servicio Civil – CNSC, el cual dentro de los tres criterios que evalúa, está incluida la variable infraestructura tecnológica y soporte profesional y esta variable exige como evidencia que la institución tenga Implantado un Sistema de Gestión de Seguridad de la Información (SGSI), con acciones de mantenimiento y mejora, donde se evidencie el cumplimiento en un 60% por cada uno de los once (11) dominios[204].

En este orden de ideas, es la División de Servicios de Información o “DSI” como se conoce en el ámbito de la UIS, la unidad administrativa que se encarga de Gestionar y administrar todos los recursos y servicios donde las tecnologías de información están involucradas. La forma en que desarrolla estas actividades de gestión, administración y proyección es mediante la modernización de la infraestructura de los servicios informáticos institucionales, el adecuado uso de los recursos y la innovación tecnológica, apoyando la consecución de los objetivos estratégicos y

[204] GUÍA TÉCNICA DE ACREDITACIÓN DE UNIVERSIDADES PÚBLICAS Y PRIVADAS, INSTITUCIONES UNIVERSITARIAS E INSTITUCIONES DE EDUCACIÓN SUPERIOR. Disponible en: https://www.cnsc.gov.co/index.php/normatividad/category/3-guia-de-acreditacion?download=1:documentacion

misionales de la Universidad.[205] Con apoyo de la DSI, se realizó la evaluación de cumplimiento de los 11 dominios de la ISO/IEC 27001:2005, y como resultado se encontró que la UIS tiene un porcentaje de cumplimiento del 66% a Julio de 2015 (Ver Anexo 7. Evaluación 11 Dominios ISOIEC 27001:2005 en la UIS).

Sumado a lo anterior, la Universidad Industrial de Santander ha venido ejecutando su plan estratégico mediante proyectos que buscan alcanzar los objetivos estratégicos planteados desde el Plan de Desarrollo Institucional 2008 – 2018. Para poder realizar todos los planes, la UIS ha construido un mapa de procesos que desarrolle las actividades necesarias para llevar a buen término todos los planes y objetivos. El mapa de procesos se puede observar en la ilustración 9.

Existen 4 grupos de procesos a saber: Procesos estratégicos, Procesos de Evaluación, Procesos Misionales y Procesos de Apoyo. La DSI se encuentra dentro de los procesos de apoyo, lo cual hace que sus procedimientos estén enmarcados solo en lo operativo y no en lo estratégico. De hecho, hoy día, la propia dinámica de la Universidad ha venido conviniendo que la DSI participe más activamente en el campo estratégico y mejorando el campo operacional. Esto es un cambio positivo, sin embargo, se hace necesario revisar los procedimientos que actualmente operan en la DSI para que no solo cubra los aspectos operativos, si no que estén enfocados en términos estratégicos.

[205] Universidad Industrial de Santander, «Sitio Web de la DSI,» 20 10 2015. http://www.uis.edu.co/webUIS/es/administracion/serviciosInformacion/presentacion.jsp.

Ilustración 9. Mapa de Procesos de la Universidad Industrial de Santander

Fuente: Universidad Industrial de Santander, «Pagina de Calidad,» 2010: https://www.uis.edu.co/intranet/calidad/calidad.jsp.

Actualmente, la UIS no cuenta con procesos y procedimientos articulados que desde la operación de sus sistemas de información sean realmente operativos según los procesos estratégicos, es decir, según los procedimientos escritos en la Oficina de Calidad difieren de los procedimientos que se siguen desde los sistemas de información. Esta desarticulación implica que existan reprocesos en sus operaciones y el desperdicio de tiempo y recursos como papel sean evidentes. El problema que se pretende resolver con este trabajo de aplicación es que la DSI establezca sus procedimientos de tal forma que den apoyo real a los procesos de las unidades y que de esta forma se analice cada procedimiento desde una perspectiva estratégica, disminuyendo los desperdicios antes mencionados. Esto implica no solo un conjunto de proyectos que resuelvan problemas inmediatos de información para la toma de decisiones, sino que, por el contrario, se planteen procedimientos y procesos que busquen siempre el planteamiento de que tanto los

proyectos que se emprendan desde la DSI están realmente alineados con la estrategia de la Universidad y que de la misma forma se puedan establecer los lineamientos necesarios para priorizar dichos proyectos.

3.3.4 Medición del nivel de madurez de los procesos de Gestión de Conocimiento en la UIS

El primer modelo de madurez, denominado *Capability Maturity Model* (CMM por sus siglas en inglés), describe cinco niveles, cuyos nombres varían de acuerdo con el autor, sin embargo, sus características enmarcan la evolución de los procesos evaluados y las áreas claves en las que deben implementarse un conjunto de prácticas o focalizarse los cambios en aras de consolidar los mejoramientos [206] [207].

La literatura de GC revela que al igual que el CMM, la mayoría de modelos de madurez de gestión de conocimiento, MMGC, basados o no en CMM, identifican cinco niveles de madurez. El modelo propuesto denominado MGMGC adaptó cinco niveles de madurez de CMM llamados inicial, conciencia, definido, gestionado y de optimización. Similar a la mayoría de modelos de madurez de GC basados o no en CMM, el MGMGC sigue una estructura por etapas y tiene tres componentes principales, llamados niveles de madurez, áreas de proceso clave o KPA por sus siglas en ingles *Key Process Areas* y características comunes [208] [209].

---

[206] DURANGO, Carlos. Arias, J.. Madurez de los procesos y tecnologías de gestión del conocimiento en empresas industriales de Antioquia. Atizapán, México: Memorias ACACIA 2012.

[207] DURANGO YEPES, Carlos Mario. EVALUATION OF TECHNOLOGIES FOR MANAGING KNOWLEDGE. Evaluación de las tecnologías para la gestión del conocimiento, Revista Dimensión Empresarial, vol. 13, núm. 2, p. 205-217 JEL: C380, M150 DOI: http://dx.doi.org/10.15665/rde.v13i2.537

[208] DURANGO, Carlos. Arias, J. Madurez de los procesos y tecnologías de gestión del conocimiento en empresas industriales de Antioquia. Atizapán, México: Memorias ACACIA 2012.

[209] DURANGO YEPES, Carlos Mario. EVALUATION OF TECHNOLOGIES FOR MANAGING KNOWLEDGE. Evaluación de las tecnologías para la gestión del conocimiento, Revista Dimensión Empresarial, vol. 13, núm. 2, p. 205-217 JEL: C380, M150 DOI: http://dx.doi.org/10.15665/rde.v13i2.537

Al aplicar este modelo de medición, se obtiene la puntuación final con la cual se puede identificar el nivel de madurez en GC de la organización. Dicho nivel consta de cinco sub-niveles, los cuales pueden variar de un nivel de "reacción", que es el más bajo, al nivel de "madurez", que es el más alto[210]. Estos cinco niveles empleados ordenados de menor a mayor en este análisis fueron: i) la reacción; ii) la iniciación; iii) la introducción (expansión); iv) el refinamiento; y v) la madurez[211]. Los significados de los cinco niveles de madurez en GC fueron plasmados en el Anexo 11. Conceptos generales de los niveles de madurez. Las situaciones descritas en cada uno de estos niveles se relacionan con la presencia, ausencia o debilidad de la GC respecto a 7 criterios relacionados con los agentes facilitadores de la GC (liderazgo, tecnología, personas y procesos), los procesos de GC y los resultados finales de la institución reflejados en el aprendizaje y la innovación[212].

Para el caso de la Universidad Industrial de Santander, se identificó que la institución se encuentra en un nivel de ***refinamiento*** en GC, justificado en las respuestas obtenidas a un total de 42 preguntas que evaluaban los 7 criterios mencionados a través de la herramienta de autoevaluación de madurez en gestión del conocimiento adaptada de la guía asiática APO[213] (Ver Anexo 12). En la Ilustración 10 se puede observar el estado de la UIS por cada criterio evaluado.

[210] Fabio Ferreira Bautista, Modelo de Gestión de Conocimiento para la Administración Pública Brasilera, Como implementar la Gestión de Conocimiento para producir resultados benéficos en los ciudadanos. Para el Instituto de Pesquisa Económica Aplicada IPEA. Rio de Janeiro 2012
[211] Op. Cit
[212] Op. Cit.
[213] APO - ASIAN PRODUCTIVITY ORGANIZATION (2009). Knowledge management: facilitator´s guide. Disponible en: <http://www.apo-tokyo.org/00e-books/IS-39_APO-KM-FG.htm>

Ilustración 10. Grafico radial de las puntuaciones por criterio de evaluación de la GC

Fuente: Elaboración Propia

Estos resultados obtenidos con respecto a la Universidad Industrial de Santander, evidencia que ya existe dentro de la Institución un conocimiento del proceso de gestión de conocimiento y un reconocimiento de la importancia que tiene para alcanzar su estrategia basada en 5 dimensiones a saber: Dimensión Académica, Dimensión Talento Humano, Dimensión Bienestar Universitario, Dimensión Universidad Frente a la comunidad regional, nacional e internacional y Dimensión Administrativa y Financiera[214]. Dentro de estas dimensiones se despliegan los objetivos estratégicos, programas y subprogramas, los cuales representan el norte para los proyectos que se deben proponer. El planteamiento de estos objetivos estratégicos está perfectamente alineado con la razón de ser de una Institución de Educación Superior en Colombia, y la operación de la UIS, mediante sus procesos y procedimientos están a su vez alineados con los programas estratégicos.

[214] Universidad Industrial de Santander, Plan de Desarrollo Institucional 2008 - 2018, Bucaramanga: UIS, 2007

3.3.5 Análisis del nivel de riesgo del proceso de gestión de conocimiento en la UIS de acuerdo con las vulnerabilidades y amenazas de los activos identificados

En esta parte del estudio se identifican, valoran y priorizan los riesgos a los que está expuesto el proceso de gestión de conocimiento en la UIS y cuál de los principios de seguridad de la información se ven afectados, para posteriormente identificar y asignar el conjunto más adecuado de controles preventivos que permitan disminuir el impacto y/o la probabilidad. En este sentido, el análisis de riesgos consiste en el proceso de identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto[215]. A su vez, la valoración de riesgos consiste en la determinación del nivel de riesgo inicial, a partir de las medidas existentes, y calcular el nivel de riesgo final luego de la valoración de la efectividad de los controles.

Una vez obtenidas las cuantificaciones de probabilidad e impacto para cada riesgo, se procede a utilizar la matriz de riesgos, en la que se relacionan estas dos medidas, y de donde se obtiene el nivel de riesgo, clasificado en niveles bajo, moderado, alto y extremo. En el Anexo 17, se muestra la matriz de identificación, clasificación y valoración de riesgos, así como las fichas de tratamiento de cada uno de los riesgos; y en la Tabla 13, se relaciona un resumen de los cinco riesgos identificados del proceso, y por cada uno de ellos se describen las causas, las consecuencias, su calificación inicial y final y las respectivas medidas de control que permitan mitigar los riesgos.

[215]SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security. 2009, p. 726.

Tabla 13. Matriz de riesgo del proceso de gestión de conocimiento

Principio de SGSI afectado	Código N°	FACTORES DE RIESGOS	IDENTIFICACIÓN DE RIESGOS		Calificación inicial	Descripción	Calificación final
		Causa: (Factores Internos y Externos, Agente Generador)	Riesgo	Efectos o Consecuencias			
Integridad	RGC-1	Errores en la digitación	Conocimiento, Información o Datos misionales no confiables	No contar con conocimiento e información útil para la toma de decisiones	20 Extremo	Estadísticas de control a la calidad del dato capturado,	12 Extremo
		Errores en la recolección atribuibles a falta de competencias técnicas, comportamentales y de gestión					
		Fallas en el aseguramiento de los datos e información				Hacer uso de TIC que permiten almacenar el conocimiento con estructuras cronológicas y facilitan el acceso simultáneo, estructurado y controlado al conocimiento a distintos usuarios tantas veces como sea necesario.	
Disponibilidad	RGC-2	Demora y desconocimiento del procedimiento de recolección y digitación, además de desconocer espacialmente donde reside el conocimiento dentro de la Universidad y fuera de esta	Conocimiento, Información o datos no oportunos	La extemporaneidad en la digitación implica la inoportunidad de información misional útil, afecta la calidad de los análisis y por tanto en las decisiones institucionales.	16 Extremo	Uso de TIC que permiten identificar el stock de conocimiento e inventariarlo, describiendo donde se encuentra, personas o grupos de trabajo, fuentes externas a la Universidad, etc.	9 Alto
		Concentración primordial en acciones misionales dejando en un segundo lugar a las acciones transversales como registro de información en el sistema por parte de los proyectos.				Actualizar los procedimientos de recolección y digitación, seguimiento y calidad del dato y registro extemporáneo de información misional.	
		Errores en la actualización				Brindar capacitación continua	

Principio de SGSI afectado	Código N°	FACTORES DE RIESGOS	IDENTIFICACIÓN DE RIESGOS		Calificación inicial	Descripción	Calificación final
		Causa: (Factores Internos y Externos, Agente Generador)	**Riesgo**	**Efectos o Consecuencias**			
		No se cuenta con la capacitación suficiente para operar adecuadamente el procedimiento.				Socializar y autoevaluar los procedimientos y documentos asociados del proceso de gestión del conocimiento	
Disponibilidad	RGC-3	Ausencia de criterios para la definición de la información que debe ser analizada	No contar con el análisis de acuerdo con la información que se tiene	Toma de decisiones inadecuadas Conocimiento inexistente	16 Extremo	Establecer los criterios para la definición de la información que debe ser analizada para la toma de decisiones	9 Alto
Disponibilidad	RGC-4	No estandarización de metodologías de distribución de conocimiento	Conocimiento distribuido ineficazmente	No se cierra el ciclo del proceso de gestión de conocimiento, por tanto, las decisiones que se toman no van a impactar en el cumplimiento del objetivo institucional.	12 Extremo	Generar canales de divulgación del conocimiento producido en la UIS	6 Moderado
		Confiar excesivamente en la tecnología				Generar política de incentivos para que los empleados compartan sus experiencias, lecciones aprendidas y en general el conocimiento organizativo del proceso en el cual participan	
		Dificultad en el acceso al conocimiento, su difusión y aplicación consecuente en contextos				Hacer uso de TIC que facilitan la comunicación personal formal e informal, ya sea temporal o continua, con independencia de las estructuras jerárquicas y de la departamentalización funcional facilitando la adaptación mutua y la flexibilidad organizativa.	

Principio de SGSI afectado	Código N°	FACTORES DE RIESGOS	IDENTIFICACIÓN DE RIESGOS		Calificación inicial	Descripción	Calificación final
		Causa: (Factores Internos y Externos, Agente Generador)	Riesgo	Efectos o Consecuencias			
						Comenzar con un proyecto piloto en una de las UAA de la UIS que permita medir con claridad los resultados en un lapso de un año; y a través de él sensibilizar frente al trabajo en equipo y transferencia de información	
		Insular la información y conocimiento del proceso y convertirlo en dominio de unos pocos				Evaluar el tipo de conocimiento que posee cada uno de los empleados y cuál es el adecuado para la transformación del proceso	
						Mirar la disponibilidad de fuentes de conocimiento calificadas similares que pueden reemplazar rápidamente la fuente perdida	
						Participación de la gerencia y el ejercicio del liderazgo constituyen elementos fundamentales de éxito.	
Confidencialidad	RGC-5	Ausencia de conciencia en los empleados sobre los riesgos de la fuga de información confidencial	Fuga de conocimiento o información confidencial y Divulgación del "know	Exposición de la imagen de la universidad	12 Extremo	Hacer cumplir los acuerdos de no divulgación (NDA, por sus siglas en inglés) e incluir un lenguaje más fuerte y específico en los contratos de trabajo sobre estos tópicos	8 Alto

Principio de SGSI afectado	Código N°	FACTORES DE RIESGOS	IDENTIFICACIÓN DE RIESGOS		Calificación inicial	Descripción	Calificación final
		Causa: (Factores Internos y Externos, Agente Generador)	Riesgo	Efectos o Consecuencias			
		Ingeniería social	how" de la Universidad			Desarrollo de un “firewall humano” dentro de la Universidad, que incluya responsabilidades de seguridad bien articuladas para cada empleado por medio de entrenamiento sobre concienciación de la seguridad	
						Promover el conocimiento entorno a los efectos del robo de propiedad intelectual debe ser parte integral de la formación de la conciencia de seguridad entre los trabajadores de la organización.	
						Aplicación de estándares de seguridad en todas sus relaciones con terceros	

Fuente: Autora a partir de Alcaldía Mayor de Bogotá [216], Manhart y Thalmann[217], Massaro, Dumay y Garlatti[218] , Santos y Barcellos[219]

[216] Alcaldía Mayor de Bogotá (2015): proceso seguimiento y control de gestión del conocimiento. Modulo Riesgos Gestión del conocimiento. Disponible en: http://intranetsdis.integracionsocial.gov.co/modulos/contenido/default.asp?idmodulo=1225

[217] Markus Manhart, Stefan Thalmann, (2015). Op. Cit.

[218] Maurizio Massaro, John Dumay, Andrea Garlatti, (2015) "Public sector knowledge management: a structured literature review", Journal of Knowledge Management, Vol. 19 Issue: 3, pp.530-558, https://doi.org/10.1108/JKM-11-2014-0466 Permanent link to this document: https://doi.org/10.1108/JKM-11-2014-0466

[219] Luciana Emirena Santos CARNEIRO y Maurício Barcellos ALMEIDA (2013). En: revista eletrônica de biblioteconomia e ciência da informação, v. 18, n. 37, p. 175-202, mai./ago. ISSN 1518-2924. DOI: 10.5007/1518-2924.2013v18n37p175

3.4 MODELO DE GESTIÓN DE SEGURIDAD DEL CONOCIMIENTO PARA LOS PROCESOS ADMINISTRATIVOS EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

Los modelos son esquemas que simulan parcialmente una realidad, se reconocen como vehículos que permiten aprender sobre fenómenos complejos del mundo en situaciones particulares. Un modelo da cuenta de las características de un fenómeno, establece relaciones y simula los diferentes efectos que emergen de dichas relaciones para entender, hasta cierto punto, la complejidad del fenómeno original[220].

Sin embargo, un modelo solo representa parte de la totalidad de un sistema original, es decir, un modelo establece un razonamiento sustituto de la realidad[221] y permite, en la mayoría de casos, predecir teóricamente lo que acontece al sistema; por esto es importante establecer una relación de realidad entre el sistema analizado y el modelo construido. Según Turner[222] citado por Pacheco, Gómez y Barrero (2009) "existen modelos icónicos, análogos y simbólicos. Los primeros establecen propiedades morfológicas (maquetas) de la realidad de un sistema; los segundos representan a través de convenciones formales (mapas) un sistema y los últimos son abstracciones de un objeto real mediante operaciones matemáticas (geometrías o estadísticas).

[220] Pacheco, J. Gómez, G. y Barrero, G. (2009). El desafío de las comunidades artesanales rurales: una propuesta ecotecnológica para una artesanía sostenible. Cuadernos de Desarrollo Rural. Departamento de Diseño Facultad de Arquitectura y Diseño, Pontificia Universidad Javeriana de Colombia, Santafé de Bogotá. Citado por: URIBE URAN, Adriana (2011). Caracterización del sector artesanal Latinoamericano, Estudios realizados sobre la artesanía en países de América Latina. Red Iberoamericana de Investigación y Transferencia de Tecnología para el Fortalecimiento Artesanal financiada por CYTED. Barranquilla, Colombia. Disponible en: http://www.ritfa.net/artesanos/templates/rifta/Libros/No_7_Libro_digital_Caracterizacion_del_Sector_Artesanal_Latinoam.pdf (Consultado 21 de abril de 2017)

[221] Swoyer, C. 1991. Structural representation and surrogative reasoning. Synthese 87:449-508.

[222] Turner, J. 1994. Matemática moderna aplicada. Probabilidades, estadística e investigación operativa. Madrid: Alianza Editorial.

Las ciencias sociales han utilizado modelos frecuentemente desde la segunda guerra mundial: La teoría de juegos, la modelación de agentes y la teoría de *graphos*, entre otros, han planteado la correspondencia entre relaciones teóricas, datos empíricos y razones matemáticas. Como cualquier otra actividad empresarial, la gestión de la seguridad de la información está supeditada a cambios de la era del conocimiento, lo que exige por parte de los responsables modelos que consideren factores claves como la gestión de este conocimiento, experiencia e información debería ser una alta prioridad tanto en las empresas de gran escala como en las de pequeña escala[223].

El modelo propuesto para la Universidad Industrial de Santander que permita la gestión de seguridad del conocimiento de tal manera que asegure la continuidad de las operaciones institucionales está fundamentado con base en los componentes Identificados en la revisión de la literatura sobre sistemas de GC, así como en los modelos, instrumentos de evaluación y guiones de implementación de GC utilizados

[223] METTAS, Adamantios; ROCK, David. Intellectual capital: utilizing the Web for knowledge management and data utilization in reliability engineering. En: Reliability and Maintainability Symposium, 2002. Proceedings. Annual. IEEE, 2002. p. 379-385.

por organizaciones públicas, como el propuesto por Batista[224] [225] [226], Wiig[227], Massaro, Dumay y Garlatti[228], Lopera y Quiroz[229], Bonilla[230], Rodríguez[231].

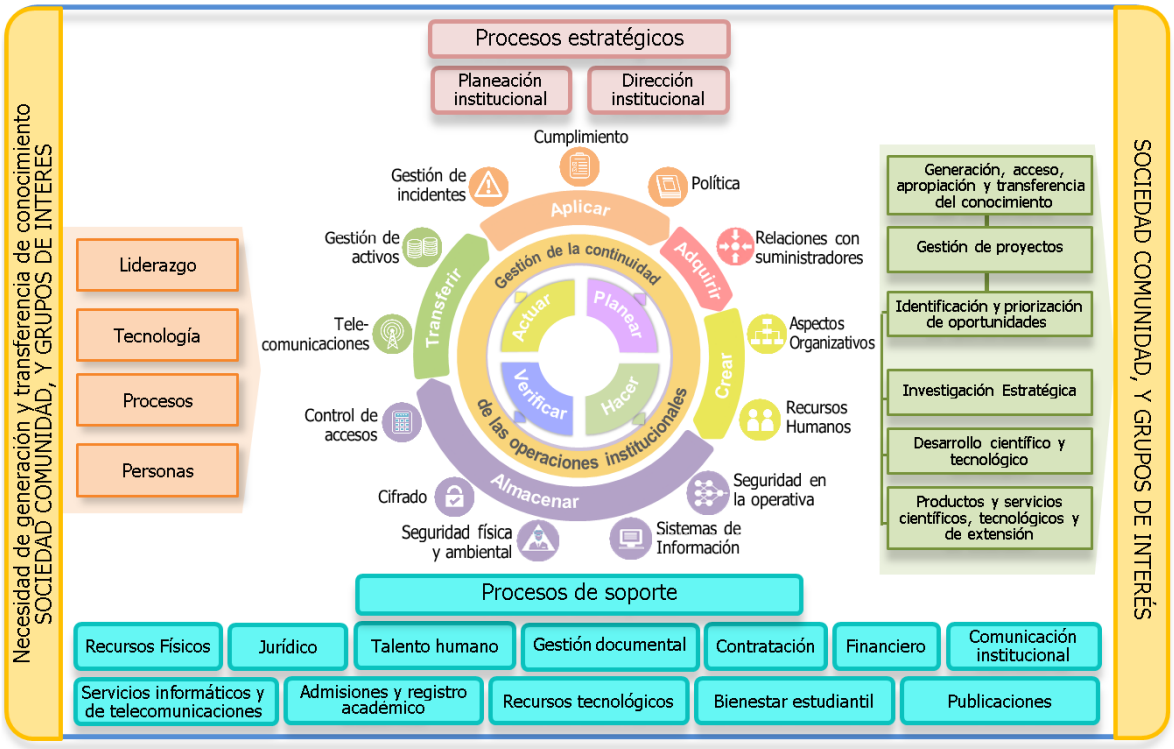
La ilustración 11 presenta los ocho componentes del modelo: i) procesos estratégicos, responsabilidad de planeación institucional y dirección institucional; ii) procesos de soporte iii) viabilizadores: liderazgo, tecnología, personas y procesos; iv) ciclo de GC: crear, adquirir, almacenar, transferir y aplicar; v) ciclo de mejoramiento: PHVA; vi) dominios de seguridad de la información; vii) gestión de continuidad de las operaciones viii) resultados de GC

El primer componente que corresponde a los procesos estratégicos, incluye la dirección institucional y la planeación institucional -es decir, la visión de futuro, la misión institucional, los objetivos estratégicos y las metas-, y sirve de fundamento para el modelo, puesto que, estos procesos están relacionados con la definición, difusión y establecimiento de políticas y estrategias académicas, financieras y administrativas, así como la fijación de objetivos y el aseguramiento de la

[224] BATISTA, F. F. Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2012.
[225] BATISTA, F. F. et al. Casos reais de implantação do modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2014. (Texto para Discussão, n. 1941).
[226] BATISTA, Fábio Ferreira (2008). Proposta de um modelo de Gestao do conhecimento com foco na qualidade. Tesis de doctorado en Ciencias de la información, Departamento de ciencias de la información y la documentación de la Universidad de Brasilia, 287 p.
[227] Wiig, Karl M. (2002) "Knowledge management in public administration", Journal of Knowledge Management, Vol. 6 Issue: 3, pp.224-239, doi: 10.1108/13673270210434331
[228] MASSARO, Maurizio, DUMAY, John y GARLATTI Andrea (2015). Public sector knowledge management: a structured literature review. Journal of Knowledge Management, vol. 19, No. 3.
[229] LOPERA LONDOÑO, Maria Eugenia y QUIROZ GIL, Nora Ledis (2013). Caracterización de un modelo de gestión del conocimiento aplicable a las funciones universitarias de investigación y extensión: Caso Universidad CES. Tesis de maestría en dirección, Universidad CES – Universidad del Rosario, Medellín.
[230] BONILLA MURIEL, Maria Jimena (2004). Diseño de un modelo de gestión del conocimiento para la Universidad Industrial de Santander. Trabajo de grado de la Escuela de Estudios Industriales y empresariales de la Facultad de Ingenierías Físico-Mecánicas de la Universidad Industrial de Santander, 188 p.
[231] RODRÍGUEZ DÍAZ, Miryam Teresa (2013). Characterization and measuring the level of knowledge management research groups in public and private universities from the department of Boyacá, Colombia. En: Cuadernos Latinoamericanos de Administración, Vol. 9, No. 17, Págs. 86-105

disponibilidad y distribución apropiada de los recursos que contribuyen al logro de la misión institucional[232], adicional, por el tamaño de la UIS, la naturaleza de sus actividades y la madurez de sus procesos, la implantación de ISO 27001 puede implicar una inversión considerable de recursos que requiere del compromiso de la dirección institucional[233].

Ilustración 11. Modelo de gestión de seguridad del conocimiento en los procesos administrativos de la UIS



Fuente: Autora

Por otra parte, los procesos de soporte o de apoyo son el segundo componente del modelo, y son conceptuados como básicos o claves. Este conjunto de procesos

[232] Universidad Industrial de Santander, Dirección Institucional (2007). Manual de gestión integrado procesos de la Universidad Industrial de Santander. Disponible en: https://www.uis.edu.co/intranet/calidad/documentos/direccion%20institucional/MANUAL%20DE%20CALIDAD/MDI.01.pdf

[233] MOOKHEY, K. K. y JITHRA, Khushbu (2006). Estrategias clave para la implantación de ISO 27001. En: ITAudit, vol. 9.

relacionados con la ejecución de las políticas y estrategias académicas, financieras y administrativas, tienen la finalidad de contribuir al logro de las actividades misionales de la Universidad, y aunque resultan de gran importancia para el intercambio de conocimiento en el interior de la institución, generalmente las acciones desde estos procesos son esporádicas y no alcanzan a cumplir su objetivo en el nivel deseable[234]. Por tanto, es esencial para la implementación de este modelo, no sólo alinear los procesos de planeación institucional y dirección institucional con la GC, los principios de seguridad de la información y los dominios de la ISO/IEC 27001:2013, sino además que la gestión de los recursos institucionales (tangibles e intangibles) que soportan el desarrollo de la institución sirvan como instrumento para alcanzar los resultados de una gestión de seguridad del conocimiento y la información.

Por otra parte, considerando que el conocimiento está ligado a los individuos y que el conocimiento es creado únicamente por los individuos a través de los procesos sociales algunos autores, como Nonaka[235], Lam y White[236], Capurro[237] formulan la siguiente hipótesis: "*El conocimiento en sí no puede ser manejado, lo que hay que manejar son los seres humanos y las condiciones bajo las cuales tienen lugar los procesos sociales"*. En este sentido, las organizaciones deben proporcionan un contexto en el cual los individuos sean apoyados en su proceso de creación de conocimiento[238]. Más concretamente, el diseño y la configuración específicos de este contexto son de suma importancia para el intercambio, la transferencia y el desarrollo de los conocimientos, haciendo así necesaria la identificación y consideración de los principales impulsores y facilitadores del proceso de creación

[234] BRUDNY, Paula (n.d.). Gestión del conocimiento en universidades. Examen de admisión al doctorado. Facultad de Ciencias Económicas – Orientación Administración.
[235] NONAKA, I.; TAKEUCHI, H.: Die Organisation des Wissens – Wie japanische Unternehmen eine brachliegende Ressource nutzbar machen. Campus-Verlag. Frankfurt, New York, pp. 68-87, 1997.
[236] LAM, Long W. y WHITE, Louis P. (1998). Human resource orientation and corporate performance. En: Human resource development quarterly. Volume 9, Issue 4, Winter 1998. Pages 351–364
[237] CAPURRO, R.: Grundfragen des Wissensmanagements, 1999. (WWW-site 30.11.2000). Disponible en: http://v.hbi-stuttgart.de/WM/bausteine.htm#Grundfragen
[238] WILLKE, H.: Systemisches Wissensmanagement. Lucius & Lucius Verl. Stuttgart, pp. 41-46, 1998.

de conocimiento[239]; por tanto, los factores críticos de éxito o viabilizadores de la GC[240] constituyen el tercer componente del modelo. Estos son: i) liderazgo; ii) tecnología; iii) personas; y iv) procesos[241].

En cuanto al liderazgo, este desempeña un papel relevante para la implementación de la GC. En resumen, corresponde a:

(a) Presentar y reforzar la visión, los objetivos y las estrategias de GC;

(b) Establecer la estructura de gobernanza institucional que permita formalizar los proyectos de GC llevados a cabo bajo prácticas de seguridad de la información, según las sugieren los estándares ISO/IEC 27001, NTC ISO 31000, ISO/IEC 20000 (ITIL)[242], ISO/IEC 22301. Como ejemplos de tales ajustes, se pueden citar, entre otros: una unidad central de coordinación y gestión de la información y del conocimiento; Un jefe de gestión de la información y del conocimiento; y la creación de equipos de GC y comunidades de práctica, o en su defecto asignar las responsabilidades de GC a alguna UAA existente.

Por ejemplo, para el caso de la UIS, se sugiere encargar a la División de servicios de información responsable del proceso de servicios informáticos y de telecomunicaciones cuyo objetivo es gestionar y administrar los recursos y servicios de tecnologías de la información y comunicación – TIC- que según la ISO/IEC 27000:2016 son a menudo un elemento esencial en la

[239] VON KROGH, G., NONAKA, I. & ABEN, M. (2001). Making the most of your company's knowledge: A strategic framework. Long Range Planning, 34:421-439.

[240] Este documento utiliza la siguiente definición para el término GC - Gestión del conocimiento, basada en el trabajo de Wunram (2001), quien afirma que "la gestión del conocimiento es sistemática y su objetivo está orientado a la aplicación de medidas para dirigir, controlar y fomentar los activos de conocimientos tangibles e intangibles de las organizaciones, con el propósito de utilizar los conocimientos existentes dentro y fuera de las organizaciones para permitir la creación de nuevos conocimientos y generar valor, innovación y mejoras para la misma".

[241] BATISTA, F. F. Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2012. Citado por: BATISTA, F. F. et al. Casos reais de implantação do modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2014. (Texto para Discussão, n. 1941).

[242] Marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información, publicada inicialmente en 1989 y actualmente utiliza la versión 3 del 2007. Los estándares de calificación ITIL son gestionados por ICMB.

organización y ayudan a facilitar la creación, procesamiento, almacenamiento, transferencia, protección y destrucción de la información, la cual puede ser digital, material o representada en forma de conocimiento de los funcionarios.

Otra UAA que se podría encargar es la Vicerrectoría de investigación y extensión, dada su responsabilidad de promover los procesos de gestión de conocimiento;

(c) Asignar recursos financieros para viabilizar los proyectos de GC y garantizar la utilización de la GC para mejorar procesos, productos y servicios;

(d) Definir la política de protección del conocimiento;

(e) Ser ejemplo para las demás UAAs en compartir el conocimiento y realizar trabajo colaborativo siguiendo los principios de seguridad de la información.

Otro viabilizador importante de la GC es la tecnología, pues con ésta se hace posible acelerar los procesos de GC, ya que según Pastor[243] y Arboníes[244], posibilitan al usuario compartir, transmitir y difundir su conocimiento, al tiempo que le ayudan en la adquisición de información para una asimilación e integración de la misma y una posterior generación de conocimiento a través de herramientas como por ejemplo: i) mecanismos de búsqueda; ii) repositorios digitales; iii) portales; iv) intranets; v) internet; vi) plataformas virtuales de comunidades de práctica, y viii) gestión

[243] PASTOR SÁNCHEZ, Juan Antonio (2000). Gestión del conocimiento en instituciones universitarias En: Scire, vol. 6, No. 2, pp. 99-120.

[244] ARBONÍES, Angel L. (2000). El conocimiento no se puede gestionar. En: Gestión del Conocimiento, vol. 4. Disponible en: www.sld.cu/galerias/doc/sitios/infodir/el_conocimiento_no_se_puede_gestionar.doc, consultado el 5 de junio de 2017

electrónica de documentos (GED)[245]. Además, Pizzolante[246] indica que el papel de las TIC en la gestión del conocimiento en las universidades y su impacto en las mismas, no se centra sólo en los mecanismos tecnológicos sino también como aparatos culturales que “estructuran los modos de pensamiento, imponen conductas y cohesionan comportamientos”. Entonces, incorporar TIC en la administración de la seguridad del conocimiento posibilita condiciones favorables para el cumplimiento de la misión administrativa de las universidades.

Asimismo, los cambios en la gestión de la información son apoyados por el fuerte uso de TIC. Esta posición se ve reforzada por la afirmación de los autores Shapiro y Varian[247] quienes previenen a los ejecutivos de las organizaciones sobre saber mantenerse al día en el diseño de estrategias competitivas relacionadas con la tecnología ya que la misma cambia el valor y la disponibilidad de la información, y esta a su vez influye en la generación de conocimiento y la toma de decisiones. Según, Tapia y León[248], las TIC son herramientas que han impactado en todo el quehacer humano, sus efectos en el ámbito organizacional son evidentes, al promover la gestión eficiente primero de la información y posteriormente del conocimiento.

Además de las variables tecnológicas involucradas en cualquier tipo de proceso de gestión, también está el aspecto humano. Por esta razón, las personas son otro de los viabilizadores de la GC, dado que captan, crean, almacenan, comparten y

[245] BATISTA, F. F. Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2012. Citado por: BATISTA, F. F. et al. Casos reais de implantação do modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2014. (Texto para Discussão, n. 1941).

[246] PIZZOLANTE, Italo. La Comunicación en el lenguaje de las emociones. En Congreso de Inteligencia Emocional Ejecutiva (1°. 2001: Valencia). Ponencia del I Congreso de Inteligencia Emocional Ejecutiva. Valencia, Venezuela: Asociación de Ejecutivos del Estado Carabobo, 2001

[247] SHAPIRO, Carl; VARIAN, Hal R. A economia da informação: como os princípios econômicos se aplicam à era da Internet. Rio de Janeiro: Campus, 1999.

[248] RANGEL Tapia, Edith y Martínez León, Jorge "Educación con TIC para la sociedad del conocimiento” Revista Digital Universitaria [en línea]. 1 de febrero de 2013, Vol. 14, No.2 [Consultada: 2 de febrero de 2013] Disponible en Internet: [http://www.revista.unam.mx/vol.14/num2/art16/index.html] ISSN: 1607-6079.

aplican conocimiento. En la literatura, se dice que el know-how de los empleados y la cultura organizacional poseen las características de los activos estratégicos de las siguientes maneras; son inimitables, raros, valiosos y no sustituible[249], asimismo, autores como De Hoog y Van Der Spek[250] aseguran que el know-how del empleado es un componente del conocimiento organizacional y un recurso estratégico crucial. En este orden de ideas, es el capital humano una de las principales entradas al modelo, puesto que, el conocimiento no surge con la acumulación de información, sino que surge cuando la información se estructura de forma agregada. Por ello el conocimiento se encuentra repartido entre las mentes de todos los miembros de la comunidad universitaria y entre los sistemas de información de la misma[251].

Lo anterior, teniendo en cuenta un estudio realizado por Wunram et. Al (2002), el cual analizó las barreras de la gestión del conocimiento en 50 empresas de Europa, estas barreras fueron clasificadas en tres categorías: Tecnología, Organización y Personas. Los obstáculos que pueden asignarse a la categoría «Tecnología» podrían resumirse como no tan pertinentes, ya que éstos sólo se referían a problemas de usabilidad o diseño de interfaces. Sin embargo, esto no significa que los autores consideran que esto no es importante - por el contrario - sino el más fácil de resolver. Curiosamente Endres et al. En 1996 llegó a una conclusión similar, lo que refuerza el supuesto que los aspectos humanos parecen ser el centro de la gestión del conocimiento en el contexto interorganizacional, teniendo en cuenta que la gestión del conocimiento comienza mirando al individuo. A pesar de que puede parecer evidente, los autores expresan que sólo el abordaje conjunto y simultáneo de las barreras humanas, organizacionales y tecnológicas conducirá a una gestión exitosa del conocimiento (North, 1998).

[249] MICHALISIN, Michael D.; SMITH, Robert D. y KLINE, Douglas M. (1997). In search of strategic assets. En: The International Journal of Organizational Analysis, vol. 5, No. 4, pp.360-387, DOI: 10.1108/eb028874
[250] DE HOOG, Robert; VAN DER SPEK, Rob. Knowledge management: hope or hype?. En: Expert Systems with Applications, 1997, vol. 13, no 1, p. v-vi. DOI: 10.1016/S0957-4174(97)80026-7
[251] SAORÍN PÉREZ, T. (1997). Ofimática Documental. En: Scire, vol. 3, No. 2, pp. 55-72.

El cuarto componente es el proceso de GC, que permite de manera sistémica movilizar el conocimiento en la institución para alcanzar los objetivos organizacionales. Las cinco actividades de este proceso son: Adquirir, crear, almacenar, transferir y aplicar el conocimiento. Estas fases deben ser puestas en práctica en la gestión de procesos y proyectos, y para ello, se utilizó el ciclo PHVA, el cual es el quinto componente del modelo, y es detallado en el Anexo 10. Caracterización procesos de gestión del conocimiento.

Asimismo, el modelo integra 13 de las 14 categorías de control de la norma ISO 27001:2013 asociándolas a una de cinco actividades del proceso de GC. Estos 13 objetivos de control constituyen el sexto componente del modelo y busca asegurar a través de la lista de controles la actividad de gestión de conocimiento correspondiente. Estas categorías ayudaran a planificar el plan de tratamiento de riesgo de seguridad de la información y del conocimiento en el proceso de gestión de conocimiento. Es importante, que se realice también una declaración de aplicabilidad que contenga los controles necesarios para la UIS, ya que los 114 controles sugeridos por la ISO 27001 en el Anexo A de la esta norma no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.

A continuación, se describe brevemente cada una de las cinco actividades básicas del conocimiento[252] [253], y los objetivos de control que se proponen:

a) **Adquirir:** consiste en definir un propósito e identificar el conocimiento que se requiere para lograrlo. Debe incluir un análisis del conocimiento existente frente al que no se encuentra disponible, el denominado "análisis de brechas". Con el fin de fomentar la reutilización de los conocimientos

[252] CEN. (2004). European Guide to good Practice in Knowledge Management - Part 1: Knowledge Management Framework. European committee for standardization comité européen de normalisation europaisches komitee fur normung, 1-33.
[253] CEN. (2004). Knowledge Management Framework. En CEN, European Guide to good Practice in Knowledge Management-Part 1: Knowledge Management Framework (págs. 1-33). Bruselas, Bélgica: CEN.

existentes, este paso de identificación comúnmente debe realizarse antes de crear nuevos conocimientos. El objetivo de control que apoya este paso es el A.15 relaciones con suministradores e incluye: Supervisión y revisión de los servicios prestados por terceros, Gestión de cambios en los servicios prestados, acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor (entiéndase como consultor, externo, actor del ecosistema de educación, ciencia y tecnología) que puede acceder, procesar, almacenar, comunicar o proporcionar conocimiento o información. Es importante recordar que el conocimiento que se adquiere es resultado en ocasiones del trabajo en red, y esta red debe establecerse con parámetros y políticas claras sobre la seguridad del conocimiento y la información que allí se aporte o comparta.

b) **Crear:** es la capacidad que existe en la organización de añadir nuevo conocimiento a la base ya existente. Hay muchas formas de crear nuevos conocimientos: a nivel personal y de equipo, frecuentemente corresponde al resultado de la interacción social, es decir, a través de la formación, el aprendizaje mediante la práctica, la solución conjunta de problemas o las sesiones de ideación colectiva. Este proceso es desarrollado por los individuos que pertenecen a la organización, a los que se les debe proporcionar un contexto apropiado por medio del desarrollo de comunidades de práctica, una adecuada inversión en I+D, una cultura organizativa, liderazgo orientado a los objetivos de conocimiento y aprendizaje, una mayor autonomía y espacios en donde puedan enfocarse al desarrollo de esta capacidad en la organización. Se propone contar en esta actividad con los objetivos de control A.6 aspectos organizativos y A.7 seguridad ligada a los recursos humanos, con lo cual se busca que ayudar a asignar las funciones y responsabilidades de la seguridad de la información a los individuos desde el momento de su contratación inicia su participación y aporte a esta actividad de GC.

c) **Almacenar:** hace referencia al lugar donde se acumula el conocimiento que ha sido adquirido o creado, con el fin de poderlo utilizar cuando sea requerido. Con el fin de crear activos de conocimiento, el conocimiento debe estar integrado dentro de una organización. Gran parte del conocimiento es almacenado en el cerebro de los individuos y con frecuencia permanecerá allí como conocimiento tácito, o puede ser almacenado en rutinas de equipo o de organización que no han sido descritas explícitamente. Mientras las personas y equipos permanezcan accesibles, se puede decir que su conocimiento es "memorizado" por la organización y está disponible para su uso. Sin embargo, la forma de asegurar el conocimiento es institucionalizarlo en el llamado "capital estructural" dentro de las estructuras, los procesos y la cultura de la organización. Almacenar conocimiento explícito depende de algunas actividades como seleccionar, organizar o categorizar, así como actualizar y eliminar el contenido antiguo. Para ello, se sugiere contar con los objetivos de control A.9 control de accesos, A.10 cifrado, A.11 seguridad física y ambiental, A.12 seguridad en la operativa, y A.14 sistemas de información. Estos controles permitirán limitar el acceso al conocimiento explícito y ayudar a proteger la confidencialidad, autenticidad e integridad del mismo.

d) **Transferir:** el objetivo de este paso es transferir el conocimiento al lugar correcto, en el momento adecuado, con la calidad adecuada, lo cual implica que el conocimiento cumpla con los principios de disponibilidad en integridad de la seguridad de la información. Esto significa que el conocimiento llega al contexto correcto, es decir, donde se crea el valor. Por lo anterior, se recomienda implementar controles relacionados con los objetivos A.8 gestión de activos y A.13 seguridad en las telecomunicaciones, permitiendo mantener la seguridad de los activos de conocimiento previamente

clasificados de acuerdo con su importancia para la institución en el momento de ser transferidos dentro de la institución o con cualquier actor externo.

e) **Utilizar:** es la capacidad que tiene la organización para explotar y usar el nuevo conocimiento en forma de servicios, procesos o mercados que ayuden a generar un sistema innovador. Este proceso puede ser aplicado dentro de la misma organización, generando una diferenciación en el sector y ventajas competitivas sostenibles en el tiempo o puede ser vendido para que sea aprovechado por otras organizaciones por medio de patentes. Esta actividad determina las necesidades de conocimiento y debe servir como punto de referencia para el conocimiento que se va a crear, almacenar y compartir. Al aplicar el conocimiento, se descubren algunas brechas adicionales, así como se adquieren nuevas experiencias que podrían representar nuevos conocimientos para la organización. Según esto, se da por terminado el proceso de GC, por lo cual se tienen recopilados aprendizajes e incluso eventos que hayan favorecido u obstaculizado la seguridad del proceso, por lo que se recomienda establecer controles relacionados con los objetivos A.5 política de seguridad, A. 16 gestión de incidentes y A.18 cumplimiento, ya que son los objetivos que permiten asegurar el nivel de continuidad de la institución y por ende permiten que el proceso de GC se mantenga como un ciclo continuo.

Para lograr mejoras a partir de las actividades básicas de gestión de conocimiento, estas deben alinearse o integrarse a los procesos organizativos y las rutinas organizativas y deben estar alineadas de acuerdo con las especificidades de cada proceso y organización, evitando centrarse sólo en una o dos actividades aisladas, así como, cumplir con los objetivos de seguridad de la información asociados a cada actividad de GC.

El ciclo PHVA se incluyó en el modelo, teniendo en cuenta, que los procesos de mejoramiento continuo están asociados a procesos de aprendizaje organizacional, dado que el paso hacia el mejoramiento se da cuando se toman las medidas necesarias para corregir las desviaciones presentadas, lo cual requiere de una gestión del conocimiento efectiva que involucre a la organización, sus procesos, sus ciclos y sus integrantes. Una organización no es susceptible a mejorar si no se conoce a sí misma, por lo cual uno de los retos dentro de la gestión institucional es lograr la identificación y desarrollo de procesos de aprendizaje, a través de la aplicación de sistemas administrativos estructurados que permitan llevar una trazabilidad de la operación de la institución, además de la utilización del conocimiento colectivo en pro del desarrollo de formas más exitosas de gestión[254].

Sumado a lo anterior, y debido a que la Universidad Industrial de Santander, cuenta con el sistema integrado de gestión, que incluye un Sistema de Gestión de Calidad (SGC). Este modelo propuesto es pertinente a la UIS y cualquier otra institución u organización en la cual se encuentre implementado un sistema de gestión de calidad, ya que se alinea a los requisitos de la norma ISO/IEC 9001:2015 de considerar el conocimiento que la organización necesita y cómo mantenerlo. Para revisar en detalle los requisitos sobre el conocimiento de la organización se debe consultar la cláusula 7.1.6 del estándar ISO/IEC 9001:2015. Hay algunas notas en esta norma que explican lo que es conocimiento de la organización y en lo que se puede basar. En concreto, es el conocimiento específico de la organización, por lo general adquirida por la experiencia, que es utilizada y compartida para alcanzar los objetivos de la organización. Esto puede venir internamente, como la propiedad intelectual, las lecciones aprendidas del fracaso y éxitos, o los resultados de las

[254] CALDAS, Marisol. Editora de Ideas Plus (2017). Publicado en Revista Empresarial y Laboral Edición No. 92. y en Ideas Plus bajo el título El Ciclo PHVA y su Papel Dentro de Procesos Exitosos de Mejoramiento y Aprendizaje. Este artículo está distribuído bajo una Licencia Creative Commons. Disponible en: http://www.ideasplusgve.com/articulo/57-el-ciclo-phva-y-su-papel-dentro-de-procesos-exitosos-de-mejoramiento-y-aprendizaje.html

mejoras; o puede provenir externamente de conferencias, conocimiento de la comunidad, o el conocimiento de proveedores[255].

El séptimo componente del modelo se trata de la integración de la norma ISO/IEC 22301 sobre continuidad de negocio a la universidad, ya que independiente de los controles que se puedan implementar, siempre se tendrá un riesgo residual que puede afectar la continuidad de las operaciones. Entendido, continuidad de una organización como la capacidad estratégica y táctica para planear y responder a incidentes e interrupciones del negocio, garantizando la continuidad de las operaciones a un nivel aceptable predefinido[256]. Por tanto, la Gestión de Continuidad (GC) de las operaciones institucionales es un proceso de gestión integral que identifica los riesgos potenciales de las operaciones de la Universidad y los impactos que éstos podrían causar en caso de materializarse, proporcionando el marco adecuado para construir la resiliencia organizacional y reforzar la capacidad de respuesta efectiva a los riesgos identificados. En este orden de ideas, se propone una herramienta para realizar el diagnóstico del estado actual en el que se encuentra la UIS, frente al estándar o buena práctica, en materia de Continuidad del Negocio: ISO/IEC 22301 (Ver Anexo 19).

Adicional, teniendo en cuenta que la gestión de continuidad del negocio debe estar inmersa en la cultura de la institución como un sistema de gestión, al igual que la gestión de seguridad de la información y la gestión del conocimiento. A continuación, en la Tabla 14 se proponen los roles, responsabilidades y autoridades de acuerdo con las funciones que deben desempeñar los diferentes grupos de interés participantes en el funcionamiento del Sistema de Gestión de Continuidad de las operaciones de la UIS.

[255] ISOTools Excellence. «Cómo gestionar el conocimiento de la organización de acuerdo con la norma ISO 9001 2015». 7. SOPORTE, ISO 9001:2015, 2016. Disponible en: http://www.nueva-iso-9001-2015.com/2016/09/gestion-conocimiento-iso-9001-2015/
[256] Fuente: BS 25999-2:2007

Tabla 14. Matriz RACI del Sistema de Gestión de Continuidad de las operaciones de la UIS

MATRIZ RACI	Dirección Institucional	Dirección de Control Interno y Evaluación de Gestión	Vicerrectoría administrativa	Sistema de Gestión de Calidad	División de servicios de información	Jefes de las UAA	Oficina de Control Interno Disciplinario	Empleados
Política, objetivos, alcance, roles y responsabilidades del SGC	A	A	C	R	I	I	I	I
Normatividad y certificación	A	C	C	R	R	I	I	I
Modelo de madurez	I	A	C	R	C	I	I	I
Definición del modelo de gestión de continuidad	A	A	C	R	I	I	I	I
Identificación de recursos requeridos	I	A	I	R	C, I	R	I	C
Provisión de recursos requeridos	I	A	I	R	R	R	I	C
Mantenimiento de recursos operativos	I	I	A	R	I	R	I	C
Mantenimiento de recursos tecnológicos	I	I	A	I	R	R	I	C
Desarrollo de competencias	I	I	A, C	R	R	R	I	I
BIA y análisis de riesgos	I	I	I	A, C	R	R	I	I
Planes y estrategias de continuidad	I	I	I	A, C	C, I	R	I	I
Pruebas y simulacros	I	I	I	A, C	R	R	I	I
Definición de Indicadores	C, I	C, I	A	R	R	R	I	I
Medición y Seguimiento al SGC	I	I	C	R, A	C	I	I	R
Acciones preventivas, correctivas y de mejora	I	I	C	R, A	R	C	I	R
Capacitación y divulgación	I	I	A, C	R	I	I	I	I
Modelo de madurez integrado	I	I	A, C	R	I	I	I	I

Fuente: Adaptado a partir de Banco de la República (2013). Manual del sistema de gestión de continuidad.

Como se trata de un modelo de gestión de seguridad del conocimiento y la información con foco en resultados, el octavo y último componente es el resultado de la GC de una manera apropiada según las buenas prácticas definidas por la ISO/IEC 27001:2013. Hay dos tipos de resultados esperados con la implementación de la GC: inmediatos y finales. Los resultados inmediatos son el aprendizaje y la innovación. Como consecuencia, hay un incremento de la capacidad de realización del individuo, del equipo, de la organización y de la sociedad en la identificación, la creación, el almacenamiento, la transferencia y la aplicación del conocimiento[257].

Los resultados finales destacados en el modelo son consecuencia de los resultados inmediatos (aprendizaje e innovación, así como el aumento de la capacidad de realización del individuo, de los equipos, de la organización y de la sociedad) y son: aumentar la eficiencia; Mejorar la calidad y el impacto social; y contribuir al desarrollo de la institución[258].

[257] BATISTA, Fábio Ferreira (2012). Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea.
[258] BATISTA, Fábio Ferreira (2012). Op. Cit.

4. CONCLUSIONES

El principal objetivo de la investigación fue diseñar un modelo de gestión de seguridad del conocimiento generado, obtenido y aplicado en los procesos administrativos de la UIS. La utilidad del modelo diseñado está en orientar la forma adecuada de asegurar la generación de valor en los procesos de apoyo y estratégicos de la UIS a partir de la estrategia de gestión de conocimiento, de forma que sirva como una herramienta de gestión tanto para la UIS como para otras Universidades. Adicional, este estudio constituye una contribución para la literatura científica en la que se identificó un gran interés de las instituciones de educación superior por indagar, profundizar y gestionar sus funciones sustantivas, pero según la literatura revisada, son pocas las experiencias identificadas que en el ámbito universitario relacionan las funciones universitarias con la gestión segura del conocimiento atendiendo los principios de confidencialidad, disponibilidad e integridad.

Se propone un modelo no lineal, en el que se tienen en cuenta las etapas definidas en la literatura científica para la gestión del conocimiento y se asocian a cada etapa aquellas dimensiones de la seguridad de la información, así como también las condiciones específicas del ecosistema de las Universidades públicas en Colombia y las características particulares bajo las cuales opera la UIS.

De otra parte, este estudio constituye una iniciativa que, apalancándose en la conceptualización teórica, indagó sobre dos conceptos normalmente tratados de forma aislada, la seguridad de la información y la gestión del conocimiento. Así como también busco integrar los principios de seguridad de la información (confidencialidad, integridad, disponibilidad) a cada etapa de la gestión del conocimiento. Teniendo en cuenta que, por un lado, la seguridad de la información plantea un aumento de la confidencialidad, pero por otro, la gestión del

conocimiento busca eliminar las restricciones en el acceso a la información. Lo anterior, lleva a una conjetura, es que la gestión de la seguridad de la información no se ocupa de las necesidades de conocimiento e información de los empleados, puesto que, si bien uno de los principios es el de disponibilidad, éste lleva implícitas una serie de restricciones según los niveles de confidencialidad que se determinen.

Así mismo, los resultados permitieron identificar como principal limitación del proceso de gestión de seguridad del conocimiento la insuficiente claridad desde la alta dirección en construir y asegurar que la política de seguridad de la información y los objetivos de seguridad de la información sean compatibles no solo con la dirección estratégica de la organización sino además con los objetivos de la gestión del conocimiento. Este no es solo un problema de las Universidades, sino también de otros organismos como: centros de estudio e investigación, centros de apoyo a la tecnología y a la innovación, sociedades de gestión de conocimiento e informática, y la banca financiera. En el caso específico de la UIS, se recomienda continuar el proceso de adaptación de las políticas de seguridad de la información y del conocimiento propuestas en este estudio a las prácticas de trabajo actuales, tanto para favorecer la gestión del conocimiento como para aumentar el acceso seguro a la información y conocimiento de los empleados y el cumplimiento de las políticas. Esto es similar al consejo ofrecido por Stahl et al. (2012), quien afirmó que una política debería "ofrecer asesoramiento específico y accionable".

Respecto del estado actual de la gestión de seguridad del conocimiento explícito (o información) en las Universidades públicas colombianas, los resultados obtenidos evidencian un reconocimiento de su importancia, no obstante, apenas se están empezando a establecer las primeras políticas de seguridad de la información y se están obteniendo los primeros resultados. Lo anterior, debido en parte a los plazos establecidos por el Decreto 2693 de 2012 entre el año 2015 y 2017 para dar cumplimiento a los lineamientos de uno de los 6 componentes del

Modelo de Gobierno en línea, “elementos transversales”, para el cual, según el manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional y territorial de la República de Colombia en su versión 3.1, las entidades del Estado, entre ellas las universidad, deben entre otros objetivos, alcanzar la implementación de un sistema de gestión de tecnologías de información y la implementación de un sistema de gestión de seguridad de la información (SGSI). Con lo anterior, se espera no sólo el fortalecimiento en uso de las TIC de una manera responsable y segura, sino además disfrutar de todos los beneficios potenciales derivados de la adecuada gestión segura del conocimiento dentro de estas instituciones.

Con los resultados obtenidos del cuestionario aplicado en este estudio (Ver Anexo 2), se puede concluir, además que, aunque casi la mitad de las instituciones encuestadas (48,86%) reconocieron no estar adelantando iniciativas de gestión del conocimiento, existe un alto porcentaje de estas instituciones que poco a poco han venido fortaleciendo los procesos que se orientan la generación de conocimiento y la información. Son conscientes, que la gestión de la seguridad del conocimiento y la información son parte del proceso intrínseco de cualquier organización, de lo cual se genera un tratamiento de datos y su correspondiente documentación que depende de su correcto funcionamiento interno.

En general, las instituciones mostraron su interés por mejorar la dinámica de los procesos de creación y difusión del conocimiento puesto que reconocen la importancia del flujo del conocimiento, tanto internamente entre los miembros de la organización como la interacción de ese activo interno con el entorno y viceversa, para lograr una organización flexible a los cambios del ambiente. A pesar de lo anterior, los resultados obtenidos develan que 18 de las organizaciones, es decir, un 33,96% de las instituciones que respondieron a la encuesta, no cuentan con un proceso formalizado de gestión de la seguridad del conocimiento y la información, puesto que es inexistente la política de acceso a la

información, lo cual contribuye a que la distribución acertada de la información a todas las áreas de la organización sea impedimento para llevar correctamente un plan de gestión del conocimiento.

Una característica en común que comparten más del 50% de las instituciones participantes en este estudio, es que, aunque saben que el tema de gestión de la seguridad del conocimiento y de la información debe contar con la participación de todos los empleados, en la práctica, señalaron en una calificación de 3,64 dentro de una escala de 1 a 5, donde 1 indicaba el nivel más bajo (cuando no existen programas o interés de parte de la organización) y 5 el nivel más alto, al fomento en las instituciones de un ambiente que favorezca la seguridad de la información o del conocimiento en los procesos, de modo que es recomendable una mayor apropiación por parte de la alta dirección, para brindar apoyo a los procesos de gestión del conocimiento, partiendo desde la definición de roles, responsabilidades y actuación de cada miembro en el proceso.

Lo anterior está alineado a los resultados de la encuesta latinoamericana de seguridad de la información realizada en 2012 por ACIS, la cual determinó en sus análisis que el área de seguridad de la información depende de la Dirección de Tecnología de Información, aspecto que denota su asociación con aspectos técnicos y de servicio, lo cual limita este tema a una parte de la organización, y se convierte en un obstáculo tanto para desarrollar una cultura de seguridad de la información como una cultura que favorezca la gestión del conocimiento. Entre los motivos señalados por los participantes como principales barreras para la implementación de buenas prácticas se cuentan: la falta de colaboración entre áreas (41.66%), falta de apoyo directivo (35.27%) y poco entendimiento de la seguridad de la información (33.05%).

Otro factor analizado en las instituciones participantes que respondieron al cuestionario fue la tecnología, como medio para facilitar la transferencia de

aprendizaje y diálogo entre los empleados. Las respuestas advierten que el porcentaje de satisfacción de los trabajadores con este aspecto es inferior al 50%, por tanto, o bien se están subutilizando los medios tecnológicos para procesar y difundir todo tipo de información dentro de las instituciones, o quizá estos medios nos son los más apropiados y eficientes, ya sea porque no se está planificando de forma adecuada las necesidades tecnológicas de la organización al momento de incorporar nuevos sistemas de información, o el flujo de información no es horizontal sino jerárquico, lo cual genera que todos los miembros de la organización se vean limitados en la información que requieren para el ejercicio de sus funciones, esto conlleva a que se haga una apuesta a corto plazo de mejorar las habilidades de la alta dirección para entender todo el "negocio" y se entienda la gestión de conocimiento no como una actividad adicional paralela al ejercicio diario de la organización, sino que se trata de una actividad intrínseca al desarrollo del mismo, la cual contribuye de diversas formas: crear memoria institucional, promover el aprendizaje y la mejora continua, generar documentación hacia la ampliación de las dimensiones del proyecto o su transferencia a otros contextos, elaborar productos que apoyen estrategias de visibilidad, de desarrollo de capacidades o de incidencia política, entre otros.

De acuerdo con lo anterior, es fundamental mencionar que la comunicación interna de las organizaciones puede acelerar o detener los procesos de gestión de la seguridad de conocimiento y la información, ya que la estructura de la comunicación organizacional dependen del entendimiento de las políticas y objetivos de las instituciones, la adecuación de rutinas eficientes de trabajos, el sistema de documentación de la organización y el flujo dinámico de información entre los niveles de la organización. Por lo cual, es importante reflexionar sobre dónde está el conocimiento que la actividad, función o proceso necesita, cómo documentar el conocimiento que el proceso va generando, y cómo se transfiere conocimiento y se promueve su adaptación y uso.

En cuanto a lo anterior, los resultados de la fase II y III de este estudio, permitieron también identificar que, aunque el Gobierno ha puesto a disposición la guía para la implementación del SGSI en sus entidades, incluidas las universidades; y el Decreto 2573 de 2014 el cual incluye como componente fundamental de la estrategia de gobierno en línea, la seguridad y privacidad de la información, dando como plazo para la implementación del 100% de este componente el año 2018, las universidades como la UIS se han encontrado en este proceso con dificultades como: la falta de capacitación o experiencia en implementación de SGSI, personal insuficiente para conformar el equipo de trabajo, y falta de acompañamiento por parte del Gobierno en el desarrollo del proyecto de implementación del SGSI.

De lo anterior, en la revisión de la literatura, se identificó que autores como Ezingeard; McFadzean; Birchall (2007), reconocen que la alta dirección necesita tomar algunas decisiones sobre cómo adaptar la seguridad de la información a una organización, sin afectar los procesos de gestión del conocimiento. Es decir, necesita decidir entre las siguientes compensaciones: la necesidad de creatividad e innovación versus el uso de controles de procedimiento para el aseguramiento de la información; la necesidad de confianza entre los empleados frente al control total de la información; la facilidad de hacer en el caso de universidades proyectos de extensión, alianzas, redes, transferencia de conocimiento o comercialización de tecnologías frente a una mayor exposición a las amenazas; suplir las necesidades de la institución haciendo uso del personal interno (Insourcing) versus sub-contratar para aprovechar las ventajas del *outsourcing.* Además, según la investigación realizada en 2013 por McKinsey y el Foro Económico Mundial sobre ciberseguridad, los gerentes de las organizaciones que tienen más éxito en la seguridad de la información, están haciendo lo siguiente: participar activamente en la toma de decisiones estratégicas, impulsar cambios en el comportamiento del usuario, y garantizar una gobernanza y una presentación de informes eficaces.

Respecto al resultado final de este estudio, teniendo en cuenta que se basa en un estudio de caso y los criterios se han validado en un contexto institucional específico, el modelo y las políticas propuestas aún necesitan finalizar su proceso de implementación para conocer el impacto final en la UIS. Por lo anterior, los gestores de seguridad de la información o unidades responsables de la gestión del conocimiento que deseen utilizar estos resultados deben ser conscientes que es necesario llevar a cabo una validación adicional, incluyendo cómo y en qué medida los criterios del modelo y las políticas son transferibles a otros contextos.

Dadas las limitaciones anteriores, existen oportunidades interesantes para futuras investigaciones. En primer lugar, una vía importante para la investigación futura es validar más los elementos del modelo y hacerlos más precisos. Otra tarea es indagar si este modelo es aplicable en otros sectores y, en caso afirmativo, en qué medida. Finalmente, se necesitan investigaciones sobre las implicaciones del uso de este modelo en el diseño de un sistema de seguridad de la información en organizaciones basadas en conocimiento o que tengan por objetivo estratégico generar valor a partir del uso del conocimiento creado, adquirido, compartido o almacenado. Estos hallazgos permitirán comprender mejor las fortalezas y limitaciones del modelo como herramienta práctica en los procesos de diseño y evaluación de las políticas de seguridad de la información y de los diferentes tipos de conocimiento: conocimiento personal, conocimiento organizativo, conocimiento de los proveedores, conocimiento de los aliados, conocimiento de los usuarios. Así como, añadirá que la gestión del conocimiento debe tener como objetivo hacer que todos los interesados sean más conscientes del papel del conocimiento en los procesos de los que son parte, e identificar para estos procesos específicos de agregación de valor los diferentes controles de seguridad requeridos para cumplir con el propósito.

También se reconocen como limitaciones del estudio, el porcentaje de respuesta de instituciones de educación superior, ya que de 303 instituciones de

educación superior reconocidas por el Ministerio de Educación Nacional (SNIES, 2017), se recibieron respuestas de funcionarios de 29 instituciones de educación superior colombianas, es decir, el 9,6% de las IES. No obstante, y aunque no es un porcentaje muy alto, se logró obtener respuesta de algunas de las Universidades más importantes en cuanto a infraestructura y número de personas de su planta de personal en Colombia, por ejemplo, la Universidad de los Andes, la Universidad Nacional de Colombia, la Universidad de Antioquia, la Universidad del Valle y la Universidad Pedagógica y Tecnológica de Colombia. Por tanto, se considera que los resultados obtenidos proporcionan información importante para los análisis y conclusiones de la seguridad de la información y del conocimiento en la UIS, y demás universidades tanto públicas como privadas del país.

Es importante precisar además, que el alcance del modelo se limitó a los procesos administrativos de la UIS, y se considera importante la realización de futuros estudios que consideren la gestión del conocimiento en los procesos de investigación, extensión y académicos, así como la seguridad del conocimiento en estos mismos procesos, de tal manera que la universidad continúe trabajando en pro de responder la pregunta: ¿cómo puede la seguridad del conocimiento y la información ayudar a la universidad a alcanzar los objetivos estratégicos?

Finalmente, con este estudio se llegó a un modelo sistémico que aunque integra los elementos de la GC soportados en controles de seguridad de información que mitigan los riesgos de cada parte del proceso de GC, diseñado específicamente para la UIS liderado desde la División de servicios de Información, es importante su validación a través de un proceso iterativo con los colaboradores, teniendo en cuenta que una sistematización no termina con la descripción de los elementos del modelo, sino que implica un análisis continuo sobre ¿Qué funciona bien y que no funciona?, ¿Cuáles son los factores claves de éxito?, ¿Qué se puede hacer de otra manera y por qué? y ¿cuáles son las recomendaciones derivadas de la práctica?

BIBLIOGRAFÍA

ADAMS, Anne y SASSE, Martina Angela (1999). Users are not the enemy. En: Communications of the ACM, Volume 42 Issue 12, Pages 40-46. DOI: 10.1145/322796.322806

Adel Yazdanmehr, Jingguo Wang, Employees' information security policy compliance: A norm activation perspective, Decision Support Systems, Volume 92, December 2016, Pages 36-46, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2016.09.009.

Advisera, se especializa en brindar apoyo a las organizaciones para implementar las principales normas y marcos referenciales como, por ejemplo, ISO 27001, ISO 9001, ISO 13485, ISO 14001, OHSAS 18001, IATF 16949, AS9100, ISO 20000 e ITIL. Con los años, Advisera se ha convertido en líder mundial en brindar cursos de capacitación y documentación para ISO 27001 (gestión de seguridad de la información) e ISO 22301 (gestión de la continuidad del negocio) a través de Internet. Sus productos son de la más alta calidad y se han implementado en más de 100 países.

ACKOFF, Russell. L. From Data to Wisdom. En: Journal of Applied Systems Analysis. 1989, vol. 16. p. 3-9.

AHMAD, Atif; BOSUA, Rachelle y SCHEEPERS, Rens. Protecting organizational competitive advantage: A knowledge leakage perspective. En: computers & security. Mayo, 2014, vol. 42. p 27-39

Ahmed, F., & Siyal, M.Y. (2005). A novel approach for regenerating a private key using password, fingerprint and smart card. En: Information Management & Computer Security, 13, 1, 39-54.

ALVESSON, Mats. A Review of “Knowledge Work and Knowledge Intensive Firms”. En: Journal of Management & Governance. Enero, 2005, vol. 9 no. 1. p. 101-105.

ANDERSON, Eddse. GATIGNON, Harndol., «Modes of foreign entry: A transaction cost analysis and propositions», Journal of International Business Studies, (1986) vol. 17, pp.1-25.

ANDERSON, J. C. Y GERBING, D. W., «Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach», Psychological Bulletin (1988), vol. 103, núm. 3, págs. 411-423.

ANDERSSON, S. (2004), «Internationalization in different industrial contexts», Journal of Business Venturing, 19, págs. 851-875

Angel León González Ariza, Jean Paul Castro, Mayra Roncallo (2014). Diagnóstico de la gestión del conocimiento en una empresa grande de Barranquilla (Colombia) Una actividad de vinculación Universidad Manuela Beltrán universidad - sector productivo.

Angela Martin, Talent Management: Preparing a “Ready” agile workforce, International Journal of Pediatrics and Adolescent Medicine, Volume 2, Issues 3–4, September–December 2015, Pages 112-116, ISSN 2352-6467, http://dx.doi.org/10.1016/j.ijpam.2015.10.002.

A. Mettas and D. Rock, "Intellectual capital: utilizing the Web for knowledge management and data utilization in reliability engineering," *Annual Reliability and Maintainability Symposium. 2002 Proceedings (Cat. No.02CH37318)*, Seattle, WA, 2002, pp. 379-385.
DOI: 10.1109/RAMS.2002.981671

ARBONÍES, Angel L. (2000). El conocimiento no se puede gestionar. En: Gestión del Conocimiento, vol. 4. Disponible en: www.sld.cu/galerias/doc/sitios/infodir/el_conocimiento_no_se_puede_gestionar.doc, consultado el 5 de junio de 2017

Audrey S. Bollinger, Robert D. Smith, (2001) "Managing organizational knowledge as a strategic asset", Journal of Knowledge Management, Vol. 5 Issue: 1, pp.8-18, doi: 10.1108/13673270110384365

AUSTIN, Robert D. y DARBY, Christopher A.R. The myth of secure computing. En: Harvard Business Review. Junio, 2003, vol. 81, no. 6. p.121–126

BARONI DE CARVALHO, Rodrigo y TAVARES FERREIRA, Marta. Using information technology to support knowledge conversion processes. En: Information Research. 2001, vol. 7, no. 1

Basie von Solms, Rossouw von Solms, The 10 deadly sins of information security management, Computers & Security, Volume 23, Issue 5, July 2004, Pages 371-376, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2004.05.002.

BATISTA, F. F. et al. Casos reais de implantação do modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea, 2014. (Texto para Discussão, n. 1941).

BATISTA, Fábio Ferreira (2012). Modelo de gestão do conhecimento para a administração pública brasileira. Brasília: Ipea.

BATISTA, Fábio Ferreira (2008). Proposta de um modelo de Gestao do conhecimento com foco na qualidade. Tesis de doctorado en Ciencias de la información, Departamento de ciencias de la información y la documentación de la Universidad de Brasilia, 287 p.

Beautement, A; Becker, IF; Krol, K; Parkin, S; Sasse, MA; (2016) Productive Security: A scalable methodology for analysing employee security behaviours. [Dataset]. Twelfth symposium on usable privacy and security (SOUPS 2016)

BENBYA, Hind; PASSIANTE, Giuseppin y AISSA, Nassi. Corporate portal: a tool for knowledge management synchronization. En: International Journal of Information Management. Junio, 2004, vol. 24, no. 3. p. 201-220. Disponible en: <http://choo.fis.utoronto.ca/fis/courses/lis2102/Readings/ benbya.pdf>

Bernd Carsten Stahl, Neil F. Doherty, Mark Shaw (2012). Information security policies in the UK healthcare sector: a critical evaluation. En: Information Systems Journal, vol. 22, No. 1, pp. 77–94. doi:10.1111/j.1365-2575.2011.00378.x

Bierley, P. y Chakrabarti, A. (1996): Generic Knowledge Strategies in the U.S. Pharmaceutical Industry. Strategic Management Journal, vol.17 (winter special issue), págs. 123-135.

BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Julio, 2005, vol. 3, no. 4. p. 49

BLOODGOOD, James M. y SALISBURY, Wm. David. Understanding the influence of organizational change strategies on information technology and knowledge management strategies. En: Decision Support Systems - Knowledge management support of decision making. Mayo, 2001, vol. 31, no. 1. p. 55-69.

BOHMER, R.M. Learning how and learning What: effects of tacit and codified Knowledge on Performance Improvement. Following Technology Adoption, Vol. 34. Pag. 197 - 223.

BONILLA MURIEL, Maria Jimena (2004). Diseño de un modelo de gestión del conocimiento para la Universidad Industrial de Santander. Trabajo de grado de la Escuela de Estudios Industriales y empresariales de la Facultad de Ingenierías Físico-Mecánicas de la Universidad Industrial de Santander, 188 p.

Bontis, N., 1998. Intellectual capital: an exploratory study that develops measures and models, Management Decision, Vol. 36, No. 2, p. 63 – 76.

Bontis, N., Keow, W.C. and Richardson, S., 2000. Intellectual capital and business performance in Malaysian industries, Journal of Intellectual Capital, Vol 1, No. 1, p. 85-100.
BRUDNY, Paula (n.d.). Gestión del conocimiento en universidades. Examen de admisión al doctorado. Facultad de Ciencias Económicas – Orientación Administración.

BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Abril, 1996, vol. 42, no. 4. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Diciembre, 2009, vol. 29, no. 6. p. 449

BUENO, Eduardo. La gestión del conocimiento: nuevos perfiles profesionales. [En línea]. (1999). [Consultado el 6 de agosto de 2012]. Disponible en <http://www .sedic.es/bueno.pdf>

Caldas, Marisol editora de Ideas Plus (2017). Publicado en Revista Empresarial y Laboral Edición No. 92. y en Ideas Plus bajo el título El Ciclo PHVA y su Papel Dentro de Procesos Exitosos de Mejoramiento y Aprendizaje. Este artículo está distribuído bajo una Licencia Creative Commons. Disponible en: http://www.ideasplusgve.com/articulo/57-el-ciclo-phva-y-su-papel-dentro-de-procesos-exitosos-de-mejoramiento-y-aprendizaje.html

CANO, M. Jeimy J.; SAUCEDO, Meza, Gabriela María (2012). IV Encuesta Latinoamericana de Seguridad de la Información, Tendencias 2012.

CANO, M. Jeimy J.; SAUCEDO, Meza, Gabriela María (2012). VIII Encuesta Latinoamericana de Seguridad de la Información, Nuevos horizontes para América Latina.

Capurro, R.: Grundfragen des Wissensmanagements, 1999. (WWW-site 30.11.2000). Disponible en:
http://v.hbi-stuttgart.de/WM/bausteine.htm#Grundfragen

CEN. (2004). Knowledge Management Framework. En CEN, European Guide to good Practice in Knowledge Management-Part 1: Knowledge Management Framework (págs. 1-33). Bruselas, Bélgica: CEN.

Centro de Coordinación Seguridad Informática Colombia, dedicados a la gestión de incidentes de seguridad informática y de telecomunicaciones

Centro de Tecnologías de Información y Comunicación de la Universidad Industrial de Santander

CHENG-YUAN, Ku, MAN-NUNG, Liu y TSUNG-HAN, Yang (2016). An integrated system for information security management with the unified framework. En: Journal of risk research

Cheryl Vroom, Rossouw von Solms, Towards information security behavioural compliance, Computers & Security, Volume 23, Issue 3, 2004, Pages 191-198, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2004.01.012.

COLOMBIA. UNIVERSIDAD MANUEL BELTRÁN. [base de datos en línea]. [consultado 10 abr.2016]. Disponible en< http://www.umb.edu.co/>

CROASDELL, David; JENNEX, Murray; ZHIHONG, Yu; CHRISTIANSON, Tony; CHAKRADEO, Meenal y MAKDUM, Wagas. A meta-analysis of methodologies for research in knowledge management, organizational learning and organizational memory: five years at HICSS. En: System Sciences. Proceedings of the 36th Hawaii intl conf on system sciences, 2003. Disponible en: <http://www.computer.org/csdl/proceedings/hicss/2003/1874/04/187440110a-abs.html>

DAVENPORT, Thomas H. y PRUSAK, Lawrence. Working knowledge: how organizations management what they know. En: Harvard Business School Press, Boston. 1998

DE HOOG, Robert; VAN DER SPEK, Rob. Knowledge management: hope or hype? En: Expert Systems with Applications, 1997, vol. 13, no 1, p. v-vi. DOI: 10.1016/S0957-4174(97)80026-7

DESOUZA, Kevin C. y VANAPALLI, Ganesh K. Securing knowledge in organizations: lessons from the defense and intelligence sectors. En: International Journal of Information Management. Febrero, 2005, vol. 25, no. 1. p. 85-98.

DELOITTE (2009). Protecting what matters. 6th Annual Global Security Survey.

DHILLON, G. and BACKHOUSE, J. Information system security management in the new millennium. En: Communications of ACM. 2000, vol. 43, no. 7, pp. 125-8. Citado por: Chang, Shuchih Ernest y Ho, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

DHILLON, Gurpreet. Principles of Information Systems Security: text and cases. 1 ed. New York: John Wiley and Sons, 2007. 464 p. ISBN 978-0471450566

DIAZ MUÑANTE, Jorge Raúl. Modelo de Gestión del Conocimiento (GC) aplicado a la Universidad Pública del Perú, publicado en el SISBIB “sistema de bibliotecas del Perú”, 2003. 40 p

DÍAZ, Nieves Lidia. Los activos de conocimiento tecnológico en las empresas industriales españolas. 2005

División de Servicios de Información - DSI, «FGD.01 - LMD Internos - Listado Maestro de Procesos,» Bucaramanga, 2015.

Dogson, M. (1993): Organizational Learning: A Review of Some Literatures. Organization Studies, vol.14, nº3, págs. 375-394.

DOHERTY, Neil Francis; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: A critical study of the content of university policies. En: International Journal of Information Management. 2009, vol. 29, no. 6. p. 449–457

DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Octubre, 2003, vol. 41, no. 1. p. 50

DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. 1988, vol. 66, no. 1. p. 47

DURANGO, Carlos. Arias, J.. Madurez de los procesos y tecnologías de gestión del conocimiento en empresas industriales de Antioquia. Atizapán, México: Memorias ACACIA 2012.

DURANGO YEPES, Carlos Mario. EVALUATION OF TECHNOLOGIES FOR MANAGING KNOWLEDGE. Evaluación de las tecnologías para la gestión del conocimiento, Revista Dimensión Empresarial, vol. 13, núm. 2, p. 205-217 JEL: C380, M150 DOI: http://dx.doi.org/10.15665/rde.v13i2.537

DUTTA, A. y MCCROHAN, K. MANAGEMENT’S role in information security in a cyber economy. En: California Management Review. 2002, vol. 45, no. 1, pp. 67-87. Citado por: Chang, Shuchih Ernest y Ho, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

DUTTA, Snider. Conceptualizing and measuring capabilities: methodology and empirical application, Strategic Management Journal, 2005. Pág. 277 – 285

Efthymia Metalidou, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas, Georgios Giannakopoulos, The Human Factor of Information Security: Unintentional Damage Perspective, Procedia - Social and Behavioral Sciences, Volume 147, 2014, Pages 424-428, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2014.07.133. Disponible en: http://www.sciencedirect.com/science/article/pii/S1877042814040440

ENISA threat landscape 2014. Overview of current and emerging cyber-threats

European Union Agency for Network and Information Security (2014) Technical Report

Fabio Ferreira Bautista, Modelo de Gestión de Conocimiento para la Administración Pública Brasilera, Como implementar la Gestión de Conocimiento para producir resultados benéficos en los ciudadanos. Para el Instituto de Pesquisa Económica Aplicada IPEA. Rio de Janeiro 2012

Financiera Comultrasan (2010). Esquema de valoración para el tratamiento de riesgos. En: Sistema de gestión de seguridad de la información NTC/ISO 27001:2005 para Financiera Comuntrasan asesorado por NewNet S.A.

Fredrik Karlsson, Karin Hedström, Göran Goldkuhl, Practice-based discourse analysis of information security policies, Computers & Security, Volume 67, June 2017, Pages 267-279, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.12.012.

GARG Ashish; CURTIS Jeffrey y HALPER Hilary. Quantifying the financial impact of Information technology security breaches. En: Information Management and Computer Security. 2003, vol. 11, no. 2. p. 74–83

GOGAN, Luminita-Maria y DRAGHICI, Anca (2013). A model to evaluate the intellectual capital. En: CENTERIS 2013 - Conference on ENTERprise Information Systems / PRojMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies. Pág. 867 – 875

GOLD, Andrew H.; MALHOTRA, Arvind y SEGARS, Albert H. Knowledge management: an organizational capabilities perspective. En: Journal of Management Information Systems. Summer, 2001, vol. 18, no. 1. p. 185-214

Grant, R.M. (1996): Prospering in Dynamically-Competitive Enviroments: Organizational
Capability as Knowledge Integration. Organization Science, vol. 7, nº4, July/August, págs. 375-387.

GRANT, Robert M. The knowledge-based view of the firm: Implications for management practice. En: Long Range Planning. 1997, vol. 30, no. 3. p. 450-454

Grant, R.M. (1996): Toward a Knowledge-Based Theory of the Firm. Strategic Management Journal, vol.17 (winter special issue), págs. 109-122.

GUÍA TÉCNICA DE ACREDITACIÓN DE UNIVERSIDADES PÚBLICAS Y PRIVADAS, INSTITUCIONES UNIVERSITARIAS E INSTITUCIONES DE EDUCACIÓN SUPERIOR. Disponible en: https://www.cnsc.gov.co/index.php/normatividad/category/3-guia-de-acreditacion?download=1:documentacion

HALLIDAY, S., BADENHORST, K. y VON SOLMS, R.A business approach to effective information technology risk analysis and management. En: LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Diiembre, 2006, vol. 2006, no. 12. p. 17

HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008. Dissertation (Doctor of Philosophy). University of New York. Faculty of the graduate school. p. 9.

Hinson, G. (2003). Human factors in information security. IsecT Ltd. Disponible en: http://www.noticebored.com/NB_White_paper_on_human_factors_v5.pdf [Accessed: 02 August 2012].

HONE, Karin and ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers and Security. Octubre, 2002, vol. 21, no. 5. p. 402–409

HONG, Kwo-Shing, et al. An integrated system theory of information security management. En: Information Management & Computer Security. 2003, vol. 11, no. 5. p. 243

ISOTools Excellence. «Cómo gestionar el conocimiento de la organización de acuerdo con la norma ISO 9001 2015». 7. SOPORTE, ISO 9001:2015, 2016. Disponible en: http://www.nueva-iso-9001-2015.com/2016/09/gestion-conocimiento-iso-9001-2015/

JENNEX, Murray E. (2009). Assessing Knowledge Loss Risk. En: Conference: Proceedings of the 15th Americas Conference on Information Systems, AMCIS 2009, San Francisco, California, USA, August 6-9, 2009. DOI: 10.1109/HICSS.2013.103

JOHANNESSEN, Jon-Arild y OLSEN, Bjørn. Knowledge management and sustainable competitive advantages: the impact of dynamic contextual training. En: International Journal of Information Management. Agosto, 2003, vol. 23, no. 4. p. 278.

Karl M. Wiig, (2002) "Knowledge management in public administration", Journal of Knowledge Management, Vol. 6 Issue: 3, pp.224-239, doi: 10.1108/13673270210434331

Kenneth J. Knapp, R. Franklin Morris Jr., Thomas E. Marshall, Terry Anthony Byrd, Information security policy: An organizational-level process model, Computers & Security, Volume 28, Issue 7, October 2009, Pages 493-508, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2009.07.001.

KHANDELWAL, Vijay y GOTTSCHALK, Petter. Information technology support for interorganizational knowledge transfer: an empirical study of law firms in Norway and Australia. En: Information resources management journal. 2003, vol. 16, no. 1. p. 14-23

KIRLAPPOS, Iacovos; BEAUTEMENT, Adam y SASSE, M. Angela (2013). “Comply or Die” Is Dead: Long Live Security-Aware Principal Agents. Financial cryptography and data security – FC 2013 workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Lecture Notes in Computer Science, vol 7862. Springer-Verlag, Berlin Heidelberg, pp. 70–82.

LABIANO, Javier. Las TIC en la Seguridad y Protección de Datos. [En línea]. Marzo (2009). [Consultado el 10 Junio de 2013]. Disponible en http://www.socinfo.info/contenidos/pdf56mar09/p14-25datos.pdf

LACEY, David. Managing the human factor in information security: how to win over staff and influence business managers. Chichester: John Wiley & Sons, 2009. 384 p. ISBN: 978-0-470-72199-5. p. 15-16.

Lam, Long W. y White, Louis P. (1998). Human resource orientation and corporate performance. En: Human resource development quarterly. Volume 9, Issue 4, Winter 1998. Pages 351–364

LEE, Heeseok y CHOI, Byounggu. Knowledge enablers, processes and organizational performance: An integrated view and empirical examination. En: Journal of Management Information Systems. 2003, vol. 20, no. 1. p. 179-228

LEONARD-BARTON, D. (1995). Wellsprings of knowledge: Building and sustaining the sources of innovation. En: Harvard Business School Press, Boston.

LIM, Kwanghui. The relationship between research and innovation in the semiconductor and pharmaceutical industries (1981–1997). En: Research Policy. Vol. 33 (2004); pág. 287–321 [citado en 10 de octubre de 2015] Disponible en Elsevier Research Databases.

LLORENS, Faraon; JOSE BAYONA, Juan; GOMEZ, Javier y SANGUINO, Francisco.The University of Alicante's institutional strategy to promote the open dissemination of knowledge. En: Online Information Review. (2010)

LOPERA LONDOÑO, Maria Eugenia y QUIROZ GIL, Nora Ledis (2013). Caracterización de un modelo de gestión del conocimiento aplicable a las funciones universitarias de investigación y extensión: Caso Universidad CES. Tesis de maestría en dirección, Universidad CES – Universidad del Rosario, Medellín.

MANURI, Ismail y YAACOB, Raja Abdullah Raja. Perceptions of knowledge creation, knowledge management processes, technology and applications in military organisations. En: Malaysian Journal Of Library & Information Science. (2011)

MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. 2004, vol. 19, no. 1. p. 4.

MARTIN, Angela. Talent Management: Preparing a "Ready" agile workforce, International Journal of Pediatrics and Adolescent Medicine, Volume 2, Issues 3–4, September–December 2015, Pages 112-116, ISSN 2352-6467, https://doi.org/10.1016/j.ijpam.2015.10.002. Disponible en: http://www.sciencedirect.com/science/article/pii/S2352646715001088

MARTIN, Julia, RASTROLLO, Ángeles, The Firm's Internationalization: The Experiential Knowledge as Determinant of Performance in Foreign Markets. Cuadernos de Economía y Dirección de la Empresa. Núm. 39, junio 2009, págs. 123-150, ISSN: 1138-5758

Martínez, Álvaro Javier, Forero, Diana Magally, Pinto Prieto, Laura Patricia y Becerra Ardila, Luis Eduardo. Ponencia titulada: Análisis bibliométrico de la producción científica acerca de técnicas de adquisición y representanción de conocimiento a través del Social Science Citation Index (2001-2013).

MASSARO, Maurizio, DUMAY, John y GARLATTI Andrea (2015). Public sector knowledge management: a structured literature review. Journal of Knowledge Management, vol. 19, No. 3.

Ma, Z., Qi, L., & Wang, K. (2008). Knowledge sharing in Chinese construction project teams and its affecting factors. Chinese Management Studies, 2(2), 97–108.

McPHERSON, P.K. The inclusive value of information. En: International Federation for Information and Documentation – 48th congress. Graz, 1996. p. 41–60.

Michalisin, Michael D.; Smith, Robert D. y Kline, Douglas M. (1997). "In search of strategic assets". En: The International Journal of Organizational Analysis, vol. 5, No. 4, pp.360-387, DOI: 10.1108/eb028874

Minakata, A (2009). Gestión del conocimiento en educación y transformación de la escuela. Revista Electrónica Sinéctica, 32.

Mírian Oliveira, Carla M.M. Curado, Antonio C.G. Maçada, Felipe Nodari, Using alternative scales to measure knowledge sharing behavior: Are there any differences?, Computers in Human Behavior, Volume 44, March 2015, Pages 132-140, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2014.11.042.

MOK, Ka Ho. Fostering entrepreneurship: changing role of government and higher education governance in Hong Kong. En: Research Policy. 2005, vol. 34, no. 4. p. 540

Montuschi, L. (2000). La economía basada en el Conocimiento: importancia del conocimiento tácito y del Conocimiento Codificado. Buenos Aires: CEMA.

Morrissey, S. (2005). *The Design and Implementation of Effective Knowledge Management Systems.* Philadelphia: The Wharton School.

MORTAZAVI, S. Habib y BAHRAMI, Mahdi. Integrated approach to entrepreneurship – knowledge based economy: a conceptual model. En: Procedia – Social and Behavioural Sciences. Vol. 41 (2012); p. 283.

MOOKHEY, K. K. y JITHRA, Khushbu (2006). Estrategias clave para la implantación de ISO 27001. En: ITAudit, vol. 9.

MOORE, Nick. Chapter 20. The information society. En: World Information. Report 1997/98. UNESCO Publishing. , Quétigny (Francia): Yves Courrier. 1997. p. 271-284. ISBN 92-3-103341-7

NEVO, Dorit y CHAN, Yolande E. A Delphi study of knowledge management systems: Scope and requirements. En: Information & Management. Septiembre, 2007, vol. 44, no. 6. p. 583–597.

Nonaka, I. (1994): A Dynamic Theory of Organizational Knowledge Creation. Organization Science, vol.5, nº1, Febrary, págs.14-37.

Nonaka, I. y Takeuchi, H. (1995): The Knowledge Creating Company. Oxford University Press, New York.

Nonaka, I.; Takeuchi, H.: Die Organisation des Wissens – Wie japanische Unternehmen eine brachliegende Ressource nutzbar machen. Campus-Verlag. Frankfurt, New York, pp. 68-87, 1997.

O'DONOGHUE, Nathan y CROASDELL, David T. Protecting knowledge assets in multinational enterprises: a comparative case approach. En: VINE. Octubre, 2009, vol. 39, no. 4. p. 298-318. ISSN: 0305-5728

ORGLAND, Magne y VON KROGH, Georg. Initiating, Managing and Sustaining Corporate Transformation: A case Study. En: European Management Journal. 1998, vol. 16, no. 1. p. 31-38

Orshesky, C. (2003). Beyond technology - The human factor in business systems. En: Journal of Business Strategy, 24, 4, 43-47.

Pacheco, J. Gómez, G. y Barrero, G. (2009). El desafío de las comunidades artesanales rurales: una propuesta ecotecnológica para una artesanía sostenible. Cuadernos de Desarrollo Rural. Departamento de Diseño Facultad de Arquitectura y Diseño, Pontificia Universidad Javeriana de Colombia, Santafé de Bogotá. Citado por: URIBE URAN, Adriana (2011). Caracterización del sector artesanal Latinoamericano, Estudios realizados sobre la artesanía en países de América Latina. Red Iberoamericana de Investigación y Transferencia de Tecnología para el Fortalecimiento Artesanal financiada por CYTED. Barranquilla, Colombia.

PASTOR SÁNCHEZ, Juan Antonio (2000). Gestión del conocimiento en instituciones universitarias En: Scire, vol. 6, No. 2, pp. 99-120.

P.C. Stern, T. Dietz, T. Abel, G.a. Guagnano, L. Kalof. A value-belief-norm theory of support for social movements: the case of environmentalism. Human Ecology Review, 6 (1999), pp. 81–97

P. Dolan, R. Shaw, A. Tsuchiya, A. Williams. QALY maximization and people's preferences: a methodological review of the literature Health Econ., 14 (2) (2004), pp. 197–208

PELUFFO A., Martha Beatriz y CATALÁN CONTRERAS, Edith. Introducción a la gestión del
conocimiento y su aplicación al sector público. Instituto Latinoamericano y del Caribe de Planificación Económica y Social – ILPES. Santiago de Chile, diciembre de 2002, 92 p. Disponible en: http://repositorio.cepal.org/bitstream/handle/11362/5586/S2002617_es.pdf?sequen Disponible en: http://www.ritfa.net/artesanos/templates/rifta/Libros/No_7_Libro_digital_Caracterizacion_del_Sector_Artesanal_Latinoam.pdf (Consultado 21 de abril de 2017)

PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. 2007, vol. 16, no. 1. p. 339

PINTO, R.; GRAWITZ, M. (1967). Analyse de contenu et theorie. En: Méthodes des sciences sociales. Dalloz. Paris. p. 456-499.

PIZZOLANTE, Italo. La Comunicación en el lenguaje de las emociones. En Congreso de Inteligencia Emocional Ejecutiva (1°. 2001: Valencia). Ponencia del I Congreso de Inteligencia Emocional Ejecutiva. Valencia, Venezuela: Asociación de Ejecutivos del Estado Carabobo, 2001

Plan de Incentivos Explorando el Conocimiento. Colombia, Ministerio de Educación Nacional República de. 2011. Bogotá : CETICS, 2011.

PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. 1985, vol. 64, no. 4. p. 149

Prieto Pastor, Isabel María. «Una valorización de la gestión del conocimiento para el desarrollo de la capacidad de aprendizaje en las organizaciones: propuesta de un modelo integrador». Universidad de Valladolid, Facultad de Ciencias Económicas y Empresariales, Departamento de Economía y Administración de Empresas, 2003.

RANGEL Tapia, Edith y Martínez León, Jorge "Educación con TIC para la sociedad del conocimiento" Revista Digital Universitaria [en línea]. 1 de febrero de 2013, Vol. 14, No.2 [Consultada: 2 de febrero de 2013] Disponible en Internet: [http://www.revista.unam.mx/vol.14/num2/art16/index.html] ISSN: 1607-6079.

RENDÓN, Miguel. Relación entre los conceptos: información, conocimiento y valor. Semejanzas y diferencias. En: Ciência da Informação, Brasília. Vol. 34, No. 2 (2005); p. 53.

RICHARDSON, Sandra; COURTNEY, James y HAYNES, John. Theoretical principles for knowledge management system design: application to pediatric bipolar disorder. En: Decision support systems. 2006, vol. 42, no. 3. p. 1321-1337

R.M. Grant. Towards a knowledge-based view of the firm. En: Strategic Management Journal, 17 (1996), pp. 109–122

Rodriguez de Almeida, Reginaldo. «DE LA SOCIEDAD DE LA INFORMACIÓN A LA SOCIEDAD DEL CONOCIMIENTO: LA SOCIEDAD DEL BIT», 2003. http://biblioteca.ucm.es/tesis/inf/ucm-t26909.pdf

RODRÍGUEZ DÍAZ, Miryam Teresa (2013). Characterization and measuring the level of knowledge management research groups in public and private universities

from the department of Boyacá, Colombia. En: Cuadernos Latinoamericanos de Administración, Vol. 9, No. 17, Págs. 86-105

Roos, G., Roos, J., 1997. Measuring Your Company's Intellectual Performance. Long Range Planning, Special Issue on Intellectual Capital, Vol. 30, No. 3, p. 413-426.

SABAU, Gabriela. Know, live and let live: towards a redefinition of the knowledge-based economy – sustainable development nexus. En: Ecological Economics. Vol. 69, No. 6 (Abr. 2010); p. 1193.

SÁNCHEZ AGUILAR, Antonio. Implicaciones de las Tecnologías de Información: Manejo del conocimiento. [Diapositivas]. LANIA, Xalapa. Septiembre, 2004. 37 diapositivas. (Consultado: 19 de agosto de 2015) http://www.slideshare.net/radarik/implicaciones-de-las-tecnologas-de-informacin-manejo-del-conocimiento (asanchez@mail.udlap.mx)

SANTOS OLMO PARRA, Antonio; SANCHEZ CRESPO, Luis Enrique; ALVAREZ, Esther; HUERTA, Monica y FERNANDEZ MEDINA PATON, Eduardo. Methodology for Dynamic Analysis and Risk Management on ISO27001. En: IEEE Latin America Transactions. 2016, vol. 14, No. 6, pág. 2897-2911. DOI 10.1109/TLA.2016.7555273

Saorín Pérez, T. (1997). Ofimática Documental. En: Scire, vol. 3, No. 2, pp. 55-72.

Schultz, E. (2005). The human factor in security. En: Computers & Security, 24, 425-426.

SEGARRA, Mercedes., Configuración del conocimiento como activo estratégico, (2010).

SHAPIRO, Carl; VARIAN, Hal R. A economia da informação: como os princípios econômicos se aplicam à era da Internet. Rio de Janeiro: Campus, 1999.

SHEDDEN, P.; SCHEEPERS, R.; SMITH, W. y AHMAD, A. Incorporating a knowledge perspective into security risk assessment. En: VINE Journal Knowledge Management. 2011, vol. 41, no. 2. p. 152-166.

Sheng, W., Howells, G., Fairhurst, M., Deravi, F., & Chen, S. (2012). Reliable and secure encryption key generation from fingerprints. En: Information Management & Computer Security, 20, 3, 207 – 221.

SHER, Peter y LEE, Vivid. Information technology as a facilitator for enhancing dynamic capabilities through knowledge management". En: Information & management. 2004, vol. 41, no. 8. p. 933-945

SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. 2009, vol. 19, no. 3. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Diciembre, 2009, vol. 29, no. 6. p. 449

SMITH, Adam (1776). Investigación de la naturaleza y causas de la riqueza de las naciones. Tomo I. Disponible en: http://www.marxistsfr.org/espanol/smith_adam/1776/riqueza/smith-tomo1.pdf

SO, M. y SCULLI, D. The role of trust, quality, value and risk in conducting e-business. En: Industrial Management & Data Systems. 2002, vol. 102, no. 9, pp. 503-12. Citado por: Chang, Shuchih Ernest y Ho, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

Steinmueller, E. (2002). Las economías basadas en el conocimiento y las tecnologías de la información y la comunicación. Revista Internacional de Ciencias Sociales OEI. Número 171, 1-17.

Swoyer, C. 1991. Structural representation and surrogative reasoning. Synthese 87:449-508.

TELLIS, Winston. Application of a Case Study Methodology. En: The Qualitative Report. Septiembre, 1997. Vol. 3, No. 3. [En línea]. [Citado 10 Enero, 2012]. Disponible en internet: <http://www.nova.edu/ssss/QR/QR3-3/tellis2.html>.

TESTA, James. (1998) La base de datos del ISI y su proceso de selección de revistas. [versión online] Disponible en: http://www.bvs.sld.cu/revistas/aci/vol9_s_01/sci23100.htm. Consultado en 29 de septiembre de 2016. Trabajo originalmente publicado por el ISI en formato electrónico: (URL: http://www.isinet.com) y presentado en el Seminario sobre Evaluación de la Producción Científica, realizado en São Paulo por el Proyecto SciELO, del 4 al 6 de marzo de 1998.

THOMPSON, E. Dale y KAARST-BROWN, Michelle L. Sensitive Information: a review and research agenda. En: Journal of the American Society for Information Science and Technology. Febrero, 2005, vol. 56, no. 3. p. 245-257

TIMMS, Stephen; POTTER, Chris y BEARD, Andrew. DTI. Information security breaches survey. Department of Trade & Industry; Technical Report. [En línea]. (2004). . [Consultado 25 Mayo de 2014]. Disponible en

<http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf>

Turner, J. 1994. Matemática moderna aplicada. Probabilidades, estadística e investigación operativa. Madrid: Alianza Editorial.

UNESCO. (2005). Hacia las sociedades del conocimiento. Informe Mundial. Ediciones UNESCO. Paris. 2005. 240 p.

UNIRED® es una corporación mixta, sin ánimo de lucro, conformada por instituciones de educación, investigación y desarrollo del oriente colombiano, la cual integra a los departamentos Santander, Boyacá y Norte de Santander (Tomado de: http://www.unired.edu.co/index.php/quienes-somos/que-es-unired).

Universidad Industrial de Santander, Dirección Institucional (2007). Manual de gestión integrado procesos de la Universidad Industrial de Santander. Disponible en:
https://www.uis.edu.co/intranet/calidad/documentos/direccion%20institucional/MANUAL%20DE%20CALIDAD/MDI.01.pdf

Universidad Industrial de Santander, Plan de Desarrollo Institucional 2008 - 2018, Bucaramanga: UIS, 2007

Universidad Industrial de Santander, «Sitio Web de la DSI,» 20 10 2015. http://www.uis.edu.co/webUIS/es/administracion/serviciosInformacion/presentacion.jsp.

VERMEULEN, C. y VON SOLMS, R. The information security management toolbox – taking the pain out of security management. En: Information Management & Computer Security. 2002, vol. 10, no. 2/3, pp. 119-25. Citado por: Chang, Shuchih Ernest y Ho, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

VON KROGH, Georg. Care in Knowledge Creation. En: California Management Review. 1998, vol. 40, no. 3. p. 133-154

Von Krogh, G., Nonaka, I. & Aben, M. (2001). Making the most of your company's knowledge: A strategic framework. Long Range Planning, 34:421-439.

VON SOLMS, B. y VON SOLMS, R. The 10 deadly sins of information security management. En: Computers & Security. 2004, vol. 23, no. 5, pp. 371-6. Citado por: Chang, Shuchih Ernest y Ho, Chienta Bruce. Organizational factors to the effectiveness of implementing information security management. En: Industrial Management & Data Systems. 2006, vol. 106, no. 3. p. 345-361

VON SOLMS, Basie y VON SOLMS, Rossouw. The ten deadly sins of information security management. En: Computers and Security. 2004, vol. 23, no. 5. p. 371–376

VON SOLMS, Bassie. Information Security: the fourth wave. En: Computers & Security. Vol. 25, No. 3 (May. 2006); p. 165.

WARD, John y PEPPARD Joe. Strategic planning for information systems. 3 ed. Chichester: John Wiley & Sons Ltd., 2002. 624 p.

Weisheng, Lu; K. W., Chau; Hongdi, Wang y Wei, Pan. A decade's debate on the nexus between corporate social and corporate financial performance: a critical review of empirical studies 2002-2011. En: Journal of Cleaner Production. 2014. Vol. 79, pp: 195-206. Base de datos: ISI

Willke, H.: Systemisches Wissensmanagement. Lucius & Lucius Verl. Stuttgart, pp. 41-46, 1998.

Wiig, Karl M. (2002) "Knowledge management in public administration", Journal of Knowledge Management, Vol. 6 Issue: 3, pp.224-239, doi: 10.1108/13673270210434331

WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. 2005, vol. 24. p. 17

WUNRAM, Michael; WEBER, Frithjof; PAWAR, Kulwant S. y GUPTA, Abhishek. Proposition of a Human-centred Solution Framework for KM in the Concurrent Enterprise. Proceedings of the 8th International Conference on Concurrent Enterprising – Ubiquitous Engineering in the Collaborative Economy, Rome, Italy, 17th-19th June 2002, pp. 151 – 158

ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Septiembre, 2007, vol. 18, no. 5. p. 751

Z. Ma, L. Qi, K. Wang. Knowledge sharing in Chinese construction project teams and its affecting factors. En: Chinese Management Studies, 2 (2) (2008), pp. 97–108