PROTOCOLO DE REVISIÓN SISTEMÁTICA DE LITERATURA

TITULO:	Diseño de un modelo de gobierno y gestión corporativo de TI para la gestión de la Ciberseguridad en el sector retail.
AUTORES:	Benitez James Pinedo Elías
RESUMEN:	Evaluar las publicaciones realizadas en los últimos 8 años sobre el tema en el título para determinar nivel de profundidad, opciones de complementariedad y estrategias de diferenciación para el trabajo de grado para optar por el título de maestría en gobierno de tecnologías de la información.
INICIO	Febrero del 2018
CRITERIOS DE SELECCIÓN	Idioma: Inglés, Español Fechas: 2010- 2018 Tipo de referencia: Libros, tesis, revistas, artículos científicos y otras publicaciones de acceso público Adicionales: Prioridad sobre artículos evaluados por expertos
FUENTE:	IEEE, PROQUEST, EMERALD

RELACIÓN DE FILTROS APLICADOS EN LAS FUENTES CONSULTADAS

NRO. BÚSQUEDA	FUENTE	FILTROS	RESULTADOS
1	IEEE	Metadata: (information technology) and (security) and (big data) and (governance); Año: 2012-2018	0
2	IEEE	Metadata y texto completo: (information technology) and (security) and (big data) and (governance) Año: 2012-2018	1.568 Evaluados: 500 más relevantes Seleccionados: 5
3	IEEE	Metadata: (security + it) and (retail or ecommerce) and (big data) Año: 2012-2018	1 Evaluados: 1 Seleccionados: 0
4	IEEE	Metadata y texto completo: (security + it) and (retail or ecommerce) and (big data) Año: 2012-2018	56 Evaluados 56 Seleccionados: 0
5	IEEE	Metadata: ((security) and (retail or	910

		ecommerce) and (governance)) Año: 2010-2018	Evaluados: 250 más relevantes Seleccionados: 13
6	PROQUEST	Metadata y texto completo: (information security) and (retail or ecommerce) and (big data) Año: 2012 - 2018 Evaluación de expertos: Si	5.971 Evaluados: 300 más relevantes Seleccionados: 6
7	PROQUEST	Metadata y texto completo: (corporate governance) and (security or risk) and (retail) Año: 2012 - 2018 Evaluación de expertos: Si	5.220 Evaluados: 300 más relevantes Seleccionados: 3
8	PROQUEST	Metadata y texto completo: (corporate governance) AND (security OR risk) AND (retail) Ubicación: Colombia Año: 2012 - 2018 Evaluación de expertos: No	169 Evaluados: 169 Seleccionados: 2
9	PROQUEST	Metadata y texto completo: (small data) and (security risks) and (retail) Año: 2012 - 2018 Evaluación de expertos: Si	41 Evaluados: 41 Seleccionados: 0
10	EMERALD	Metadata y texto completo: (small data) and (security) and (retail) Año: 2012 - 2018 Artículos y capítulos Evaluación de expertos: Si	3.023 Evaluados: 300 más relevantes Seleccionados: 3
11	PROQUEST	Metadata y texto completo: (information technology) and (retail) Año: 2015 - 2018 Evaluación de expertos:Si	14303 Evaluados: 150 más relevantes Seleccionados: 5

DETALLE DE RESULTADOS SELECCIONADOS

NRO. BÚSQUEDA	TITULO	ISBN / ISSN	RESUMEN
2.1	Understanding Industrial Espionage for Greater Technological and Economic Security Sharad Sinha, 2012	ISSN: 0278-6648	Large and highly successful companies all over the world have to deal with the problem of industrial espionage at one time or another. Encyclopedia Britannica defines Industrial Espionage as “acquisition of trade secrets from business competitors” and goes on to state that “... industrial espionage is a reaction to the efforts of many business to keep secret their designs, formulas, manufacturing processes, research and future plans in order to protect or expand their shares of the market.” Thus we can say that companies spy on other companies to obtain information related to trade secrets and intellectual property that can bring financial payoffs, market leadership, economic growth and, in some cases, political clout to the spying companies. It should be well understood that spying is an illegal and covert activity in almost every country in the world, where laws to deal with it have been enacted. Thus, industrial espionage qualifies as an illegal activity by virtue of its nature itself. Nevertheless, organizations and governments still engage in it because of the benefits it can bring and the fact that legal proceedings are extremely complicated and time consuming. Where specific laws do not exist, legal proceedings can still be initiated by framing charges of theft and unauthorized access. The United States enacted the Industrial Espionage Act of 1996, also called the Economic Espionage Act (EEA) of 1996 to deal with such espionage.
2.2	Cybersecuring Small Businesses Celia Paulsen, 2016	ISSN: 0018-9162	If small businesses collectively embrace cybersecurity, the unique adaptability advantages they have over large organizations could significantly change the dynamics of the cybersecurity landscape and make them leaders in the field.
2.3	Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost Paul P. Tallon, 2013	ISSN: 0018-9162	Finding data governance practices that maintain a balance between value creation and risk exposure is the new organizational imperative for unlocking competitive advantage and maximizing value from the application of big data. The first Web extra at http://youtu.be/B2RlkoNjrzA is a video in which author Paul Tallon expands on his article "Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost" and discusses how finding data governance practices that maintain a balance between value creation and risk exposure is the new organizational imperative for unlocking competitive advantage and

			maximizing value from the application of big data. The second Web extra at http://youtu.be/g0RFa4swaf4 is a video in which author Paul Tallon discusses the supplementary material to his article "Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost" and how projection models can help individuals responsible for data handling plan for and understand big data storage issues.
2.4	Governing Big Data: Principles and practices P. Malik, 2013	ISSN: 0018-8646	As data-intensive decision making is being increasingly adopted by businesses, governments, and other agencies around the world, most organizations encountering a very large amount and variety of data are still contemplating and assessing their readiness to embrace “Big Data.” While these organizations devise various ways to deal with the challenges such data brings, the impact and importance of Big Data to information quality and governance programs should not be underestimated. Drawing upon implementation experiences of early adopters of Big Data technologies across multiple industries, this paper explores the issues and challenges involved in the management of Big Data, highlighting the principles and best practices for effective Big Data governance.
2.5	IT Governance in the Trenches Stephen J. Andriole, 2016	ISSN: 1520-9202	This issue's Spotlight department presents interviews with three past and current CIOs from the business, university, and public transportation sectors. These professionals "in the trenches" present their thoughts about several aspects of the governance process, describe their experiences and the challenges they've faced, and speculate on the future of technology governance.
5.1	Risk in modern IT service landscapes: Towards a dynamic model Nico Rödder; Rico Knapper; Jochen Martin, 2012	ISSN: 2163-2871 ISBN: 978-1-4673-4775-4	The “Cloud Computing” paradigm is gaining ground with new IT service providers and traditional IT out-sourcing providers alike. Customers want to use cloud computing solutions with all their advertised advantages and without the hassle of traditional long term outsourcing migration and contracting. Risk is at the center of attention when dealing with the adoption of cloud services. Because of the security concerns and the consequential reservations towards the acceptance of public cloud computing platforms, a lot has been done to improve security and trust in these environments. However, most of the implementations and research regarding this issue is concerning technical security risks with a focus on preventing perimeter-based attacks. Security and trust issues beyond perimeter based security risks have gained little attention. This paper identifies the need to look beyond technical issues and turns the

			attention to improving compliance and governance in cloud environments. In this process the focus is set on the discontinuity cap between existing methods to identify and evaluate IT risks and the treatment of these risks with Service Level Agreements. To close this cap a model for a dynamic view on current IT risk is proposed to comply with modern IT environments that are composed of an ampleness of different services. The model has a strong corporate context and will help companies to evaluate their current risk exposure and thus make better decisions when choosing their services.
5.2	Strategy for building initial trust in B2C electronic commerce Liefa Liao; Kanliang Wang 2010	ISBN: 978-1-4244-5162-3	This paper analysis the trust building issues and trust information presence which Internet stores provide in order to increase consumer initial trust belief. Based on models of trust from academic literature, the paper develops a research framework that identifies key trust-related factors and organizes them into three categories: self assurance, easy of use and useful of website, and third party information. The framework is applied to six well-known web sites to demonstrate its applicability. The proposed framework will benefit both practitioners and researchers by identifying important issues regarding trust, which need to be accounted for in Internet stores.
5.3	Organisations Capability and Aptitude towards IT Security Governance Tanveer A. Zia, 2015	ISBN: 978-1-4673-6537-6	In today's more digitized world, the notion of Information Technology's (IT) delivery of value to businesses has been stretched to mitigation of broader organisations' risk. This has triggered the higher management levels to provide IT security in all levels of organisations' governance and decision making processes. With such stringent governance, IT security is considered as one of the core business processes with up-to-date policies and procedures to be in placed at all levels of governance. This paper provides IT security practitioners' view on how IT security is managed in their organisations. A close look at some of the IT security governance standards and how these standards are applied in the organisations gives us astonishing results about organisations' capability levels with most practitioners thinking IT security processes are either not fully implemented or fail to achieve its purpose.
5.4	The Risk Study of E-Governance Based on PEST Analysis Model Song Yingfa; Yin Hong 2010	ISBN: 978-1-4244-6647-4	The combination of governance revolution and information and communication technology (ICT) fueled e-governance which make ICT as instrument. E-governance will be new manner of good governance. However, there are several kinds of risk when it develops, such as political, economic, social and technological. They mainly include the plight of

			institution and policy and political deception; the lack of capital; the deficiency of citizen participation, digital divide and negative effect of internet media; information security and innovation. Accordingly, the realization of e-governance needs measurement, such as innovating institution, consummating law system, improving leading competence; breaking funds bottleneck; fostering civil society and shortening digital divide; ensuring information security and promoting information innovation
5.5	A Holistic Governance Framework for e-Business Success Xiaowen Liu; Lihua Wu; Jin Yu; Xiaochun Lei 2010	ISBN: 978-1-4244-8507-9	E-business has made organizations even more reliant on the application of IT. The dependence on new technologies, have increased exposure of businesses to technology-originated threats and have created new requirements for governance. Previous IT governance frameworks, such as those provided by ISO and the IT Governance Institute, Standards Australia, have not given the connection between IT governance and e-business sufficient attention. This paper presents a holistic governance framework for e-business success by integrating IT governance framework with critical success factors (CSFs) of e-business. The framework provided a structured and holistic approach to direct, evaluate and monitor e-business projects and operations.
5.6	IT governance framework planning based on COBIT 5 case study: secured internet service provider company Iffah Kholidatun Nisrina ; Ian Joseph Matheus Edward ; Wervyan Shalannanda 2016	ISBN: 978-1-5090-2649-4	Information technology investment in a company driven by the importance of the information needed by a company. The company seeks to increase the value of IT investments that has been spent on the field. The board of directors of the company has also understood the importance of an effective and efficient IT environment. In the present study, we will plan IT governance framework that will be aligned with one of the companies in Indonesia which has a high level of security. The design of this framework will adopt international standards framework is COBIT 5. The design needs to be done in order to produce effective and efficient governance so that the use of information technology can be optimized
5.7	MAVEN information security governance, risk management, and compliance (GRC): Lessons learned Eduardo Takamura ; Carlos Gomez-Rosa ; Kevin Mangum ; Fran Wasiak 2014	ISBN: 978-1-4799-1622-1	As the first interplanetary mission managed by the NASA Goddard Space Flight Center, the Mars Atmosphere and Volatile EvolutioN (MAVEN) had three IT security goals for its ground system: COMPLIANCE, (IT) RISK REDUCTION, and COST REDUCTION. In a multi-organizational environment in which government, industry and academia work together in support of the ground system and mission operations, information security governance, risk management, and compliance (GRC) becomes a challenge as each component of the ground system has and follows its own set of IT security

			requirements. These requirements are not necessarily the same or even similar to each other's, making the auditing of the ground system security a challenging feat. A combination of standards-based information security management based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), due diligence by the Mission's leadership, and effective collaboration among all elements of the ground system enabled MAVEN to successfully meet NASA's requirements for IT security, and therefore meet Federal Information Security Management Act (FISMA) mandate on the Agency. Throughout the implementation of GRC on MAVEN during the early stages of the mission development, the Project faced many challenges some of which have been identified in this paper. The purpose of this paper is to document these challenges, and provide a brief analysis of the lessons MAVEN learned. The historical information documented herein, derived from an internal pre-launch lessons learned analysis, can be used by current and future missions and organizations implementing and auditing GRC.
5.8	Governance Practices and Critical Success Factors Suitable for Business Information Security Yuri Bobbert ; Hans Mulder 2015	ISSN: 2472-7555 ISBN: 978-1-509 0-0076-0	Information Security (IS) is increasingly becoming an integrated business practice instead of just IT. Security breaches are a challenge to organizations. They run the risk of losing revenue, trust and reputation and in extreme cases they might even go under. IS literature emphasizes the necessity to govern Information Security at the level of the Board of Directors (BoD) and to execute (i.e. Plan, build, run and monitor) it at management level. This paper describes explorative research into IS-relevant Governance and Executive management practices. Answering the main research question: "Which practices at the level of Governance are relevant for Business Information Security Maturity" The initial phase of this research consists of a review of academic and practice-oriented literature on these relevant practices. This list of practices is then examined and validated through expert panel research using a Group Support System (GSS). The paper ultimately identifies a list of 22 core principles. This list can function as frame of reference for Boards of Directors and Management Teams in order to increase their level of Business Information Security (BIS) Maturity.
5.9	Information system security governance: Technology intelligence perspective Mounia Zaydi ; Bouchaib	ISBN: 978-1-509 0-6227-0	In recent years, the majority of studies and scientific research has primarily focused on the technical perspective of information system security (algorithms, tools, hardware, and infrastructure) which is part of a reactive approach. Over the time, this approach has succeeded, more or less, in

	Nasserddine 2016		managing the information technology (IT) concerns. However, the new technological trends and the new work organizations generate excessively rapid changes in the landscape of information security without forgetting the rapid changes in the society, the interconnected economies and computer networks that are increasing exponentially complicate the security of the constantly evolving information systems issues. In this context, our paper focuses on the fact that Information system also consists of a functional parts (human factor, procedures, politics...etc.) which imply the introduction of a proactive approach and adopting a vision of governance in order to align IT goals with organization strategy. This article is a review of literature on the existing approaches to secure information systems, initiate a reflection on the limits of traditional visions adopted, stress the importance of information systems security governance (ISSG) as a holistic approach, provide an overview of the actual IS security issues while criticizing the model GRC (Governance, Risk Management, Compliance) and proposing a new vision of the ISSG under the Technology intelligence(TI) perspective in order to pursue the emergence of technology and the sudden change of business objectives. Finally, we schematize the new Meta model that we named GRCI-TI. In addition to a fruitful discussion of the research contributions and the forthcoming research, directions are presented.
5.10	Identifying gaps in IT retail Information Security policy implementation processes Ileen E. van Vuuren ; Elmarie Kritzinger ; Conrad Mueller 2015	ISBN: 978-1-4673-6988-6	With a considerable amount of support in literature, there is no doubt that the human factor is a major weakness in preventing Information Security (IS) breaches. The retail industry is vulnerable to human inflicted breaches due to the fact that hackers rely on their victims' lack of security awareness, knowledge and understanding, security behavior and the organization's inadequate security measures for protecting itself and its clients. The true level of security in technology and processes relies on the people involved in the use and implementation thereof [1]. Therefore, the implementation of IS requires three elements namely: human factors, organizational aspects and technological controls [2]. All three of these elements have the common feature of human intervention and therefore security gaps are inevitable. Each element also functions as both security control and security vulnerability. The paper addresses these elements and identifies the human aspect of each through current and extant literature which spawns new human-security elements. The purpose of this research is to provide evidence that the IT sector of the South African retail industry is

			vulnerable to the human factor as a result of the disregard for human-security elements. The research points out that the IT sector of the South African retail industry is lacking trust and does not pay adequate attention to security awareness and awareness regarding security accountability. Furthermore, the IT sector of the South African retail industry is lacking: 1) IS policies, 2) process and procedure documentation for creating visibility, and 3) transparency necessary to promote trust. These findings provide support that the identified gaps, either directly or indirectly, relate to trust, and therefore, might be major contributing factors to the vast number of breaches experienced in the South African retail industry. These findings may also provide valuable insight into combatting the human factor of IS within the IT sector, irrespective of industry, which choose to follow an IS model built on the foundation of trust.
5.11	Evaluation of information technology governance using COBIT 5 framework focus AP013 and DSS05 in PPIKSN-BATAN Suryo Suminar ; Fitroh dan Suci Ratnawati 2014	ISBN: 978-1-4799-7975-2	Utilization of Informatics and Center for Nuclear Strategic Area (PPIKSN) based Perka BATAN No. 14 In 2013 served in the utilization and development of nuclear informatics to support the research, development, and application of nuclear science and technology scientific information. One of the fields of Computer and Communication Network Management Data (PJKKD) tasked to manage computer networks and data communications. The problems that exist on the web is the large PPIKSN BATAN unit hacked, the absence of SOPs and special security units and the lack of information for the evaluation of information security. PPIKSN implement audit function based on the guidelines of BATAN, so the need for appropriate evaluation of IT governance standards COBIT 5. This study focuses on the Manage Security (AP013) and Manage Security Service (DSS05). Stages of evaluation in this study is based on the COBIT 5 Process Assessment Activities. The results of this study are PJKKD on PPIKSN for value as is AP013 worth 1.96 and 1.71 DSS05 worth or both at the level of capability 2. That is, the process has been done DSS05 AP013 and manageable manner. As for the AP013 to be worth 2.96 and 2.71 DSS05 worth or both at level 3 capabilities, in other words on AP013 and DSS05 PPIKSN has a gap that is 1.
5.12	The risk control model in corporate governance —Based on conditional random fields based security risk evaluation for IT systems Jing Tang ; LePing Shen	ISBN: 978-1-4244-5540-9	Reducing the risk of IT governance often get a lot of attention. Journal and newspaper articles abound, and professional books have been written on the subject. this article presents a Conditional Random Fields (CRF) based risk assessment model .We first analyzed and evaluated the existing information security risk assessment methodology, and described control processes of information systems and risk

	2010		levels summarily. After that, CRF model was introduced into information system security assessment, which can improve model-based information security risk assessment method (CORAS). this article taking web-based electronic banking system for an example, we quantify the risk indicators of a given task sequence, by formal description and modeling of system flow and risk levels. The experiments demonstrate the feasibility of CRF model, which laid the foundation for information system risk assessment and IT governance security.
5.13	Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC) Perdana Kusumah; Sarwono Sutikno; Yusep Rosmansyah 2014	ISBN: 978-1-4799-6322-5	Management of information without regard to risk the achievement of enterprise goals can have an impact on organizational performance, financial loss or organization's credibility. The risk control for the negative effects and utilization of chance in achieving enterprise goals is called information security. Information security are generally solved by partial and limited. It also happens to INTRAC that apply only management area of information security by adopting ISO/IEC 27001:2009 and ISO/IEC 27002:2005. This study aims to develop process assessment model that support the implementation of information security governance on an organization. The method used in this study is qualitative method. Based on the validation by expert judgment, information security governance model has been prepared in accordance with the requirements of information security, particularly in the INTRAC.
6.1	Privacy, E-Commerce, and Data Security Voss, W Gregory; Woodcock, Katherine; Corbet, Rob; Dhont, Jan; McDonald, Bruce A; Eleftheriou, Demetrios; Hay, Emily; Chung, Cecil Saehoon; Park, Jae Hyun 2013	ISSN: 00207810	This article reviews important legal developments during 2012 in the fields of privacy, e-commerce, and data security. A special focus has been made on European developments, in light of changes around a new proposed privacy framework
6.2	The rise of cyberinfrastructure and grand challenges for eCommerce Winter, Susan J 2012	ISSN: 16179846	Advances in ICT have enabled the transformation of commerce into eCommerce. The eCommerce revolution is well under way, but what grand challenges are on the horizon? This paper extrapolates from the past to understand the forces that shape the future. It focuses on cyberinfrastructure growing out of the Cold War and highlights the role of government, Big Science and of the National Science Foundation in that story. Big Science and

			eCommerce will continue to shape Web activities and to react to advances in ICT. Both are involved in the co-evolution of physical, social, organizational, economic and legal factors and face analogous issues arising from similarly disruptive transformations, though the manifestations of these transformations differ in their surface features. Each may lead in addressing a particular issue at a given time, but can learn from the other. Finally, this paper identifies three Extreme Grand Challenges for Big Science and eCommerce that represent important steps toward an even brighter future for both
6.3	Small data in the era of big data Kitchin, Rob; Lauriault, Tracey P 2015	ISSN: 03432521	Academic knowledge building has progressed for the past few centuries using small data studies characterized by sampled data generated to answer specific questions. It is a strategy that has been remarkably successful, enabling the sciences, social sciences and humanities to advance in leaps and bounds. This approach is presently being challenged by the development of big data. Small data studies will however, we argue, continue to be popular and valuable in the future because of their utility in answering targeted queries. Importantly, however, small data will increasingly be made more big data-like through the development of new data infrastructures that pool, scale and link small data in order to create larger datasets, encourage sharing and reuse, and open them up to combination with big data and analysis using big data analytics. This paper examines the logic and value of small data studies, their relationship to emerging big data and data science, and the implications of scaling small data into data infrastructures, with a focus on spatial data examples.
6.4	Security and privacy in business networking Wohlgemuth, Sven; Sackmann, Stefan; Sonehara, Noboru; Tjoa, A Min 2014	ISSN: 10196781	Business networking relies on application-specific quantity and quality of information in order to support social infrastructures in, e.g., energy allocation coordinated by smart grids, healthcare services with electronic health records, traffic management with personal sensors, RFID in retail and logistics, or integration of individuals' social network information into good, services, and rescue operations. Due to the increasing reliance of networking applications on sharing ICT services, dependencies threaten privacy, security, and reliability of information and, thus, innovative business applications in smart societies. Resilience is becoming a new security approach, since it takes

			dependencies into account and aims at achieving equilibriums in case of opposite requirements. This special issue on 'Security and privacy in business networking' contributes to the journal 'Electronic Markets' by introducing a different view on achieving acceptable secure business networking applications in spite of threats due to covert channels. This view is on adapting resilience to enforcement of IT security in business networking applications. Our analysis shows that privacy is an evidence to measure and improve trustworthy relationships and reliable interactions between participants of business processes and their IT systems. The articles of this special issue, which have been accepted after a double-blind peer review, contribute to this view on interdisciplinary security engineering in regard to the stages of security and privacy requirements analysis, enforcement of resulting security requirements for an information exchange, testing with a privacy-preserving detection of policy violations, and knowledge management for the purpose of keeping business processes resilient
6.5	An information security risk-driven investment model for analysing human factors Alavi, Reza; Islam, Shareeful; Mouratidis, Haralambos 2016	ISSN: 20564961	The purpose of this paper is to introduce a risk-driven investment process model for analysing human factors that allows information security managers to capture possible risk-investment relationships and to reason about them. The overall success of an information security system depends on analysis of the risks and threats so that appropriate protection mechanism can be in place to protect them. However, lack of appropriate analysis of risks may potentially results in failure of information security systems. Existing literature does not provide adequate guidelines for a systematic process or an appropriate modelling language to support such analysis. This work aims to fill this gap by introducing the process and reason about the risks considering human factors.
6.6	Organizational information security policies: a review and research framework Cram, W Alec 1 ; Proudfoot, Jeffrey G 1 ; John D'Arcy 2 2017	ISSN: 0960085X	A major stream of research within the field of information systems security examines the use of organizational policies that specify how users of information and technology resources should behave in order to prevent, detect, and respond to security incidents. However, this growing (and at times, conflicting) body of research has made it challenging for researchers and practitioners to comprehend the current state of knowledge on the formation, implementation, and effectiveness of security policies in organizations. Accordingly, the purpose of this paper is to synthesize what we know and what remains to be learned about organizational information security policies, with an eye toward a holistic understanding of this research stream and the

			identification of promising paths for future study. We review 114 influential security policy-related journal articles and identify five core relationships examined in the literature. Based on these relationships, we outline a research framework that synthesizes the construct linkages within the current literature. Building on our analysis of these results, we identify a series of gaps and draw on additional theoretical perspectives to propose a revised framework that can be used as a basis for future research.
7.1	Applying IT governance balanced scorecard and importance-performance analysis for providing IT governance strategy in university Jairak, Kallaya; Prasong Praneetpolgrang 2013	ISSN: 09685227	Purpose - The purpose of this paper is to identify the current situation and the future improvement for IT governance and controls in developing country like Thailand. Design/methodology/approach - Thai universities were selected and used as subjects for capturing the perception of IT executives on IT governance performance measures. In the first step, a global IT governance perspective was drawn from the literature review. In the second step, the important-performance analysis was applied to the metrics of IT governance balanced scorecard with collected survey data from 64 IT executives. Findings - From a global perspective, the critical points that need to be concerned before implementing IT governance have been illustrated. From a regional perspective, the paper generated the strategic IT governance guidance for Thai universities. Practical implications - This paper is beneficial for chief information officers, executive managers, IT managers, and academics. They will gain more knowledge and understanding about the mixed method of using metrics in IT governance balanced scorecard and importance-performance analysis in order to identify the current situation of IT governance and controls in their organizations. Additionally, the practical idea with this method can be applied to draw IT governance strategy in their contexts. Originality/value - This paper specifies the critical points and directions of IT governance for Thai universities. The analysis covers global and regional viewpoints. This paper also provides the method for applying IT governance balanced scorecard metrics and importance-performance analysis to contribute IT governance strategy.
7.2	IT Governance-An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Improved Effectiveness	ISSN: 15435962	The issues, opportunities and challenges of effectively managing and governing an organization's Information Technology (IT) demands, investments and resources has become a major concern of the Board and executive management in enterprises on a global basis. A rapidly growing number of organizations have become increasingly dependent

	Selig, Gad J 2016		on a broad array of technologies to manage and grow their businesses. IT is an integral part of most organizations today and will certainly become more critical in the future. This paper proposes a comprehensive and integrated IT governance framework and roadmap which identifies the appropriate current and emerging best practices methodologies for each of the major IT Governance components that must be addressed in any approach and is critical for companies to achieve more effective alignment and management of IT. The framework can serve as a guideline for any organization to select and customize the appropriate approach applicable to its environment, plans, priorities, capabilities and available resources. The findings and implications are based on extensive primary and secondary research and are grounded in a review of current and emerging industry and government best practices and select case studies of leading global and regional organizations based on the recently published book by the author entitled, "Implementing Effective IT Governance and IT Management," published by Van Haren Publishers, 2015.
7.3	Antecedents and Consequences of Board IT Governance: Institutional and Strategic Choice Perspectives Jewer, Jennifer; McKay, Kenneth N 2012	ISSN: 15369323	In spite of the potential benefits of board IT governance and the costs of ineffective oversight, there has been little field-based research in this area and an inadequate application of theory. Drawing upon strategic choice and institutional theories, we propose a theoretical model that seeks to explain the antecedents of board IT governance and its consequences. Survey responses from 188 corporate directors across Canada indicate that both board attributes and organizational factors influence board involvement in IT governance. The results suggest that proportion of insiders, board size, IT competency, organizational age, and role of IT influence the board's level of involvement in IT governance. The responses also indicate that board IT governance has a positive impact on the contribution of IT to organizational performance. Overall, the results support the integration of strategic choice and institutional theories to explain the antecedents to board IT governance and its consequences, as together they provide a more holistic framework with which to view board IT governance
8.1	Colombia Information Technology Report - Q4 2015 Business Monitor International 2015	ISSN: 17564794	The depreciation of the Colombian peso against the US dollar in 2015 is a drag on growth by raising the cost of imported devices and solutions and resulting in deferred purchases and substitution for lower cost alternatives. This negatively impacted our forecast, which we revised down again in the Q4 2015 update and now forecast a contraction of 20% in US dollar

			terms in 2015. However, with our in-house Country Risk team envisaging a stabilisation of the peso from 2016, we maintain a bright medium-term outlook, with strong economic performance and a supportive policy environment meaning it is expected to make Colombia a regional outperformer.
8.2	Almacenes Exito S.A. : Retailing - Company Profile, SWOT & Financial Analysis Progressive Digital Media 2016	ISSN: 1840874545	Almacenes Exito S.A. (Exito) is a multi-format retailer based in Colombia. Its product portfolio includes food and non-food products such as packed foods, fresh fruit and vegetables, groceries, dairy products, confectioneries, apparel, consumer electronics, baby products and home decor products, among others. The company operates hypermarkets, supermarkets and proximity stores under various banners including Éxito, Carulla, Surtimax, Super Inter, Viva, Devoto, Disco and Geant. It is involved in offering credit facilities, real estate property services, insurance services, travel agency services and fuel supplies. The company also retails its merchandise through e-commerce websites www.exito.com, www.carulla.com and www.cdiscount.com. It operates in Colombia and Uruguay through the company-owned and leased stores. Exito is headquartered in Envigado, Colombia.
	Gobierno de la información principios y prácticas en big data	ISBN 0738439592	El crecimiento de los datos en los últimos cinco años ha sido asombroso, sin embargo será la base de los volúmenes de datos que se pronostican para los próximos cinco años. La variedad de datos sigue creciendo mucho más allá de las bases de datos tradicionales y hojas de cálculo para abarcar una gran variedad de fuentes de sensores, blogs de redes sociales y tweets, grabaciones de video, registros de llamadas, registros operacionales y muchas más formas de datos. Este volumen y variedad de datos viene a un ritmo cada vez más rápido velocidad. El volumen, la variedad y la velocidad son las tres "V" originales de Big Data, que son datos que se espera que transformen organizaciones individuales e industrias enteras a través de nuevos conocimientos. Todos estos grandes datos respaldan el análisis de múltiples fuentes a lo largo de múltiples dimensiones para encontrar correlaciones inesperadas. A su vez, estos nuevos conocimientos analíticos cambiar los modelos comerciales, ya sea apoyando una próxima mejor acción o una oferta a un cliente, identificando rápidamente el fraude, detectando patrones o sistemas de delincuencia urbana amenazas de red, administración de tráfico y logística, o predicción de necesidades de mantenimiento de antemano para

			evitar el tiempo de inactividad. Big Data es visto por las organizaciones como un recurso natural recurso que impulsa la ventaja competitiva y genera ingresos y valor. Al mismo tiempo, todos estos grandes datos presentan riesgos crecientes para cualquier organización. Los la velocidad y el volumen de llegada impiden la revisión humana de la mayoría de los contenidos. La variedad de datos abre la posibilidad de encontrar correlaciones que se pueden utilizar para perjudicar propósitos, tales como el robo criminal a gran escala de información privada del cliente. Los las fuentes de big data a menudo están fuera del control de la organización y, a menudo lo suficientemente complejo como para plantear preguntas sobre la veracidad de la información, como el origen o el sesgo de los datos, o la calidad general de los datos en sí misma o en Combinación con otros datos. El gobierno de la información está destinado a ayudar a las organizaciones a abordar estos riesgos y alcanzar el valor deseado de todos los datos, ya sean datos estructurados tradicionales o las fuentes emergentes de big data no estructurado. Al usar un marco que se centra en los resultados y los principios básicos que respaldan los estrategias, el gobierno de la información mapea a las personas, los procesos y disciplinas, con arquitectura y tecnología de referencia, que son necesarias para abordar estos desafíos.
10.1	Information security in supply chains: a management control perspective Sindhuja P N; Anand S. Kunnathur 2015	ISSN: 2056-4961	Purpose – This paper aims to discuss the need for management control system for information security management that encapsulates the technical, formal and informal systems. This motivated the conceptualization of supply chain information security from a management controls perspective. Extant literature on information security mostly focused on technical security and managerial nuances in implementing and enforcing technical security through formal policies and quality standards at an organizational level. However, most of the security mechanisms are difficult to differentiate between businesses, and there is no one common platform to resolve the security issues pertaining to varied organizations in the supply chain. Design/methodology/approach

			– The paper was conceptualized based on the review of literature pertaining to information security domain. Findings – This study analyzed the need and importance of having a higher level of control above the already existing levels so as to cover the inter-organizational context. Also, it is suggested to have a management controls perspective for an all-encompassing coverage to the information security discipline in organizations that are in the global supply chain. Originality/value – This paper have conceptualized the organizational and inter-organizational challenges that need to be addressed in the context of information security management. It would be difficult to contain the issues of information security management with the existing three levels of controls; hence, having a higher level of security control, namely, the management control that can act as an umbrella to the existing domains of security controls was suggested.
10.2	How strategists use “big data” to support internal business decisions, discovery and production Thomas H. Davenport 2014	ISSN: 1754-4408	Purpose This study aims to construct mechanisms of big data-driven business model innovation from the market, strategic and economic perspectives and core logic of business model innovation. Design/methodology/approach The authors applied deductive reasoning and case analysis method on manufacturing firms in China to validate the mechanisms. Findings The authors have developed an integrated framework to deduce the elements of big data-driven business model innovation. The framework comprises three elements: perspectives, business model processes and big data-driven business model innovations. As we apply the framework on to three Chinese companies, it is evident that the mechanisms of business model innovation based on big data is a progressive and dynamic process.

			Research limitations/implications The case sample is relatively small, which is a typical trade-off in qualitative research. Practical implications A robust infrastructure that seamlessly integrates internet of things, front-end customer systems and back-end production systems is pivotal for companies. The management has to ensure its organization structure, climate and human resources are well prepared for the transformation. Social implications When provided with a convenient crowdsourcing platform to provide feedback and witness their suggestions being implemented, users are more likely to share insights about their use experience. Originality/value Extant studies of big data and business model innovation remain disparate. By adding a new dimension of intellectual and economic resource to the resource-based view, this paper posits an important link between big data and business model innovation. In addition, this study has contributed to the theoretical lens of value by contextualizing the value components of a business model and providing an integrated framework.
10.3	A retail perspective on the shopping behavior, cultures and personalities for China, United Arab Emirates, Belgium, India, Germany and America Taylor Thomas; Charles E. Carraher 2014	ISSN: 1746-8779	Purpose – This study aims to examine the shopping behaviors (online and in store), cultures and personalities of consumers within China, Belgium, India and Germany, and compares them to American shopping behaviors and to each other. Design/methodology/approach – The data were collected through literature research and personality, cultural and shopping behavior research was assessed via surveys, while customer service oriented behaviors were measured through direct observation and survey methods using structured questionnaires and other approaches for data collection. Findings – The findings showed implications of anticipating

			consumer's behavioral responses, as well as the cultural and personality differences. The findings may help retailers with strategic business strategies to assess what attracts consumers the most and the least and then use this advantage to become successful internationally. Originality/value – The current study is original, in that it uses multiple methods to collect data allowing for comparison across shopping industry groups including retail managers and even consumers themselves. Primary data of this type are difficult to obtain in China. This study contributes to the literature by showing that different industries may have different requirements in terms of the relationship between personalities and customer service levels among managers
11.1	Innovative information technologies and their impact on the performance of the entities which activate in the retail industry Dumitru, Valentin-Florentin; Jinga, Gabriel; Mihai, Florin; Stefanescu, Aurelia 2015	ISSN: 15829146	The use of innovative information technologies can represent an advantage for the companies in the retail industry. This research is based on the results of an empirical study. The research was built under the auspices of the diffusion of innovations theory. Using the questionnaires collected we could establish correlations between the variables included into three categories (company's size, the information technologies used for retail, the impact of information technologies on the company) and we developed two original econometric models. The turnover is considered an endogenous variable (underlying the impact of the information technologies on its value) as well as exogenous (the existence of a unique computers network within the company depending on the turnover as a development factor). The models show that there is a negative correlation between the total turnover and the percentage of the turnover obtained through online sales, respectively the existence of a unique computers network is influenced by the existence of the online retail within the company. The conclusions underline the research limits and the necessary future developments.
11.2	Information and communication technologies as a source of marketing innovations in retail - trends	ISSN: 17321948	Economic growth in modern retail trade is determined by the development of resources, especially knowledge and innovation. The aim of this paper is to demonstrate that retailers use innovative

	Reformat, Beata 2016		solutions, which are based on new information and communication technologies. Their manifestation is the development of marketing innovations. The investigation is aimed at answering the following questions: What are the possibilities for creating marketing innovations in trade based resources and potential of ICT? What trends can be observed in the creation of marketing innovations to trade based on knowledge acquired through ICT tools?
11.3	Analysis of the cost impact of the new technologies in e-tail Drumea, Cristina 2015	ISSN: 20652194	The impact of new technologies on retail is studied in terms of costs. Starting from the idea that reducing costs should have a significant effect of the new technologies in retail, it is investigated the possibility that it actually constitutes the basis of a new facette of the cost leadership generic strategy. Exploratory research tracks some automation effects on transaction costs and labour costs in retail. General business models in the field are analysed, with a focus on some concrete ways of implementation in retail, particularly as e-tail. In the background we grasp and discuss the aspects of the financial flows related to trade. Even when those issues may prevail, one cannot elude discussing the cultural and ethical standards associated to the trade new features induced by e-tail and the new technologies.
11.4	Retail innovation technologies Dinu, Vasile 2015	ISSN: 15829146	Commerce, as an important industry of any national economy, is a socially important complex of activities, which has to correspond to the general level of development and civilization of the community it serves. Considering this, the essential priorities commercial activity will turn to are represented by the increased power that consumers get through better informing, the assurance of a better connection between retail and innovation, more equitable and sustainable commercial relationships along the purchase chain, the improvement of retail services accessibility, the creation of a better work environment through the better correlation between employers' needs and employers' competences.

11.5	Cnalyzing customer service technologies for online retailing: a customer service life cycle approach Ayanso, Anteneh; Lertwachara, Kaveepan 2015	ISSN: 08874417	In this research, we examine the implementation of customer service functionalities on the top 500 online retailers in the U.S. Our analysis is performed through the lens of the Customer Service Life Cycle (CSLC) theory which defines customer services into four stages: Requirements, Acquisition, Ownership, and Retirement. Our study aims to determine the relationship between retailers' CSLC scores and their performance in website traffic and online sales.

PROTOCOLO DE REVISIÓN SISTEMÁTICA DE LITERATURA: ESTÁNDARES

TITULO:	Diseño de un modelo de gobierno y gestión corporativo de TI para la gestión de la Ciberseguridad en el sector retail.
AUTOR:	Benitez James Pinedo Elías
RESUMEN:	Identificar y seleccionar los estándares aplicables para desarrollo del trabajo de grado planteado en el ***título***.
INICIO	Febrero del 2018
CRITERIOS DE SELECCIÓN	Idioma: Inglés, Español Fechas: 2010 - 2018 Tipo de referencia: Estándares
FUENTE:	ISACA, ISO, NIST