Article **Journal-Public Economy**
December, 2022 Vol.6 No.11 1-11

IT Governance and risks

Gobierno y riesgos de TI

SOLARES-SOTO, Pedro†*

Universidad Iberoamericana, México.

ID 1st Author: *Pedro, Solares-Soto*

DOI: 10.35429/JPE.2022.11.6.1.11 Received July 10, 2022; Accepted December 30, 2022

Abstract

The term "governance" describes the ability of an organization to control and regulate their own performance in order to avoid conflicts of interest, related to the division between the beneficiaries and the IT Governance actors. Derived from Corporate Governance, and mainly on the relationship between business and IT management of an organization. Highlight the import of matters concerning IT in modern organizations and recommends that strategic IT decisions are made by the highest level of directives. The Institute of Information Technology Governance (ITGI) was established in 1998 by the Audit Association and Control Information Systems (ISACA) in order to advance international thinking and standards in directing and controlling the information technology companies. According to ITGI IT governance is regarded as critical and as a management discipline within public or private companies. Effective IT governance helps to supports the business goals, maximizes business investment in IT, and appropriately manages IT-related opportunities and risks. These risks include legal and financial consequences for non-compliance with financial corporatives laws. The main objectives of IT Governance are: (1) ensuring that investments in IT generate business value and (2) mitigate the risks associated with IT. This is achievable through the implementation of an organizational structure with well-defined roles for information functions, business processes, applications, infrastructure, etc.. They have several best practices, standards, certifications and government IT risks.

Government, Risks, IT

Resumen

El término "gobernanza" describe la capacidad de una organización para controlar y regular su propia actuación con el fin de evitar conflictos de intereses, relacionados con la división entre los beneficiarios y los actores de la Gobernanza de TI. Derivado de la Gobernanza Corporativa, y principalmente sobre la relación entre el negocio y la gestión de TI de una organización. Destaca la importancia de las cuestiones relativas a las TI en las organizaciones modernas y recomienda que las decisiones estratégicas en materia de TI sean tomadas por las directivas del más alto nivel. El Instituto de Gobernanza de las Tecnologías de la Información (ITGI) fue creado en 1998 por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) con el fin de hacer avanzar el pensamiento y las normas internacionales en materia de dirección y control de las empresas de tecnologías de la información. Según el ITGI, el gobierno de las TI se considera fundamental y una disciplina de gestión dentro de las empresas públicas o privadas. Un gobierno eficaz de las TI contribuye a apoyar los objetivos empresariales, maximiza la inversión empresarial en TI y gestiona adecuadamente las oportunidades y los riesgos relacionados con las TI. Estos riesgos incluyen consecuencias legales y financieras por incumplimiento de las leyes corporativas financieras. Los principales objetivos del gobierno de TI son: (1) garantizar que las inversiones en TI generan valor para el negocio y (2) mitigar los riesgos asociados a las TI. Esto se consigue mediante la implantación de una estructura organizativa con roles bien definidos para las funciones de información, los procesos de negocio, las aplicaciones, la infraestructura, etc. Disponen de varias buenas prácticas, normas, certificaciones y riesgos de TI gubernamentales.

Gobierno, Riesgos, TI

Citation: SOLARES-SOTO, Pedro. IT Governance and risks. Journal-Public Economy. 2022. 6-11:1-11.

† Researcher contributing as first author.

Introduction

An important concept for the alignment of Information Technology (IT) with the Business is IT Governance. Governance is based on the Latin word 'gubernare' (to direct or lead), hence it is the set of responsibilities and practices exercised by the board and executive management with the goals of providing strategic direction, ensuring that objectives are achieved, determining that risks are appropriately managed, and verifying that enterprise resources are allocated and leveraged responsibly.

IT Governance is defined as a discipline relating to the way in which the top management of organisations directs the evolution and use of information technology. It is considered a part of "Corporate Governance", focusing on the performance, risk and control of Information Technology.

ISACA's IT Governance Institute describes: "IT Governance as the responsibility of the Board of Directors and senior management. It is an integral part of corporate governance and consists of leadership, organisational structures and processes to ensure that IT underpins and extends the organisation's objectives and strategies "15 . IT governance is therefore primarily concerned with the ability to make decisions, oversee and control information technology.

IT Governance Institute, [Online]. Available from http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx; Internet; accessed 1 April 2014.

IT Governance

Currently, IT Governance systems are successfully implemented in other sectors (banking, insurance, industry, etc.) reaching a maturity of 2.67 out of 5 on the scale proposed by the IT Governance Institute (ITGI). Universities around the world are also incorporating IT governance, and according to the study carried out by Yanosky and Borreson (2008) they have already reached a maturity of 2.30 out of 5, which means that universities are still in an incipient situation and in the process of maturing.

The elements that support effective IT governance are often not structural or procedural but people-related: managerial support, personal skills and capabilities, and the participation and involvement of all stakeholders.

IT management is becoming increasingly complex but at the same time growing in importance; according to Dahlberg and Kivijarvi (2006), some of the reasons for this are:

- Management would like to improve the cost-effectiveness of the use of its IT resources. They want to ensure that IT investments provide value to their business and are aligned with the achievement of the organisation's other objectives.

- You demand reports that set out what the improvement is in relation to IT and you need IT to meet the new management needs of the organisation.

- Corporate governance and performance measurement actions have led the call that IT should be managed with practices similar to those used for other functions, such as the Balanced Scorecard (BSC) or reliance on suppliers in relation to the organisation's strategy.

- IT service providers and their users must measure and manage the service levels, costs, risks, etc., of IT services.

IT Governance best practices are: ISO 38500, COBIT (Control Objectives for IT) 5.0 and CGEIT Certification.

ISO 38500

ISO/IEC 38500 defines IT Governance as The system by which the current and future use of information technology is directed and controlled. Authors Peter Weill and Jeanne Ross, in their book IT Governance, mention the following definition: "Specification of the decision-making capabilities and accountability framework to encourage the most appropriate behaviour in the use of information technology" 16.

ISSN 2524-2016

Based on the definition, the standard starts by making it clear that IT governance is not an isolated element but -is a system‖, made up of different elements -strategies and policies‖, each of which has value in its own right and the value of the system that integrates them is greater than the value of the sum of their parts (systems thinking).

Peter D. Weill and Jeanne W. Ross, IT Governance. Harvard Business Review Press. U.S.A. 2004.

IT governance is about -directing and controlling‖, the former being understood as making decisions and planning their implementation and the latter as monitoring and evaluating the results.

- It refers to the current and future use of IT because the organisation's managers must ensure that they control the systems in place but must not forget to have a plan for their future operation and for integrating new technologies. IT plans should support the organisation's business plan and their goal should be to achieve the established objectives or, in other words, to seek alignment with business objectives‖17.

For the implementation of IT Governance, the ISO/IEC 38500 standard published in June 2008 is recommended, with the -main objective of providing a framework of principles for business management to evaluate, direct and monitor the use of Information Technologies; its principles are‖18:

- Accountability. Everyone needs to understand and accept their responsibilities for the supply or demand of IT.

- Strategy. The organisation's business strategy takes into account current and future IT capabilities.

- Investment. IT acquisitions are made for valid reasons, based on appropriate and continuous analysis, with clear and transparent decisions.

- Performance. IT is sized to support the organisation, providing services of adequate quality to meet current and future needs.

- Compliance. The IT function complies with all applicable legislation and standards.

- Human Conduct. IT policies, practices and decisions demonstrate respect for human conduct, including the current and emerging needs of all people involved.

- Establishing accountability. Competent decision-makers.

- Alignment. of IT with the organisation's strategic objectives.

- Investment. In appropriate IT assets.

- Procurement. IT acquisitions are made for valid reasons, based on appropriate and continuous analysis, with clear and transparent decisions.

- Compliance. The IT function complies with all applicable laws and regulations. Policies and practices are clearly defined, implemented and enforced.

ISO 38500. [Online]. Available at http://www.iso.org/iso/pressrelease.htm?refid=Ref1135, accessed on 30 April, 2014

IBÍDEM.

In the same way, this standard applies to the governance of information technology management processes in all types of organisations that use (today almost 100%), providing the basis for the objective assessment of IT governance.

- -ISO 38500 IT Governance Principles Adapted from ISO 38500 2008.

- Responsibility. Establishing the responsibilities of each individual or group of people within the organisation in relation to IT.

- Strategy. The potential of IT must be taken into account when designing the organisation's current and future strategy.

- Procurement. IT acquisitions should be made after proper analysis and decision making based on clear and transparent criteria. There must be an appropriate balance between benefits, opportunities, cost and risks, both in the short and long term.

- Performance. IT must support the organisation by delivering services at the level of quality required by the organisation.

- Compliance. IT must comply with all laws and regulations and internal policies and procedures must be clearly defined, implemented and supported.

- Human factor. Established policies and procedures must include the utmost respect for the human component, incorporating all the needs of the people who are part of the IT processes.

The standard emphasises the fundamental role of management in establishing policies and strategies as well as in monitoring the management of compliance with existing internal and external legislation and standards and the performance of the resources used.

The standard also recognises that there is no great expectation that managers will have a high degree of technical expertise, so their decisions will be based on advice from their executives and from external sources. Where IT is critical to the organisation, it would be feasible for management to obtain independent opinions in the same way that financial auditing is a routine activity for many organisations.

Business Framework for the Governance and Management of Enterprise IT: COBIT 5.0

COBIT Control Objectives for Information-Related Technologies 5.0 provides a comprehensive framework that helps companies achieve their objectives for the governance and management of corporate IT. Simply put, it helps companies create optimal value from IT while maintaining the balance between generating benefits and optimising risk levels and resource usage.

COBIT 5 enables IT to be governed and managed in a holistic enterprise-wide manner, encompassing the entire end-to-end business and functional areas of IT responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or public sector‖19.

- COBIT 5.0 is a unique and integrated framework because‖20:

- It aligns with other standards and frameworks allowing it to be used as the overall integrating framework for management and governance.

- It is comprehensive in its coverage of the enterprise, providing a basis for effectively integrating other frameworks, standards and practices used.

- Provides a simple architecture for structuring guidance materials to produce a consistent set.

- It integrates all the knowledge previously dispersed in the different ISACA frameworks.

COBIT 5 offers globally accepted principles, practices, analytical tools and models to help business and IT managers maximise confidence in the value of their information and technology assets.

Businesses around the world need guidance to govern, manage and ensure that they derive value from the vast amounts of information they manage and the rapidly changing technologies they employ. COBIT 5 provides a guide for enterprises to make effective decisions, taking into account the needs of different stakeholders.

COBIT 5 is adaptable to all business models, technology environments, industries, geographies and corporate cultures. It can be applied to:

- Information security.

- Risk management.

- Corporate governance and enterprise IT management.

ISSN 2524-2016

- Review and assurance activities.

- Legal and regulatory compliance.

- Processing of financial data or CSR information.

COBIT 5 equips practitioners with the definitive tools and techniques to govern corporate IT with a business focus. The COBIT 5 framework simplifies the challenges facing corporate governance with just five principles and seven families of drivers. It also integrates other approaches and models, such as TOGAF, PMBoK, Prince2, COSO, ITIL, PCI DSS,

Un marco de negocio para el gobierno y la gestión de las TI de la empresa, [En línea]. Disponible en http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf, accesado el 29 de abril de 2014.

Un recorrido por COBIT 5.0, [En línea]. Disponible en http://www.isacacr.org/archivos/UN%20RECORRIDO%20POR%20COBIT%205%20%2019-06-13.pdf, accesado el 29 de Abril de 2014.

Sarbanes-Oxley Act and Basel III.

IT Governance Certification

The CGEIT accreditation is aimed at professionals involved in the Corporate Governance of ICT in Enterprises [and other bodies/entities]. IT Governance has always defended the borderline nature of Corporate Governance of IT: it is a responsibility of the governing bodies and senior management of organisations; but IT managers and specialists play a fundamental role in its development and implementation. Taking this statement as a starting point, the CGEIT certification is aimed at the boards of directors or senior management teams of companies or organisations.

At the time of its creation, ISACA stated that CGEIT is aimed at both business and IT people to understand the contribution that IT makes to generating value for organisations. The contents in the -CGEIT body of knowledge are: (1) frameworks for Corporate Governance of IT, (2) strategic alignment of IT with the business, (3) IT value delivery, (4) IT risk management, (5) IT resource management and (6) performance measurement of the IT function itself.

The contents allow us to define the CGEIT certification as a professional certification related to the CIO and his -circle of trust‖ team of collaborators; that is, a professional certification that is perfectly adapted to the professional profiles of those individuals involved in the smooth running of IT Corporate Governance, from the supply side: CIO, members of CIO offices, those in charge of IT strategic planning, IT portfolio management, management of corporate risks derived from the use of IT, those in charge of IT marketing, etc.

- The CGEIT programme supports the growing demands and recognises the wide range of professionals whose knowledge and application of IT Governance principles are key to the success of a management programme. Certification is synonymous with excellence and offers a number of benefits both professionally and personally, constituting a -competitive advantage for‖22:

Companies and Organisations:

- Establish a standard of best practice, adding credibility and recognition.

- Provide an orientation to technology and business risk management.

- Upgrade staff competencies.

- Facilitate access to a global network of industry and subject matter experts.

The Practitioners:

- Demonstrate knowledge of IT governance.

- Link with a professional programme that has worldwide acceptance.

- Improve their career opportunities and financial stability.

- To distinguish oneself as a qualified professional.

- Certification is currently considered as a recognition that the professional who has obtained it has the necessary theoretical and practical knowledge to perform adequately.

5.5 IT Risks

The definition of Information Security Risks based on the international standard ISO/IEC 27005:2011 is: -the potential for a certain threat to exploit vulnerabilities of an asset or group of assets and thus cause damage to the organisation‖23.

Risk management enables an organisation to identify what it needs to protect, how it needs to protect itself and how much protection it needs, and thus to invest its efforts and resources effectively. In order to identify risks, it is necessary to determine: assets, threats, existing controls, vulnerabilities, consequences and impacts.

There are various risk frameworks, some of them are:

- ISO 31000
- IEC/DIS 31010
- ISO/D Guide 73
- BS 31100
- ISO/IEC 27005
- ITGI - The Risk IT Framework
- Basel III
- OCTAVE
- NIST SP800-30
- CRAMM
- MAGERIT
- TRA Working Guide
- Microsoft - SRMG
- BS 7799-3
- AIRMIC, ALARM, IRM - ARMS - UNE 71504
- AS/NZS 4360

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition, [En línea]. Disponible enhttp://www.iso27001security.com html 27005.html ; accesado el 25 de abril de 2014.

The most in demand are: ISO 31000 and ITGI - The Risk IT Framework. Each is described below.

ISO 31000

The variety, complexity and nature of risks are likely to be very diverse and the International Standard developed by the IOS (International Organisation for Standardisation) proposes generic guidelines on how to manage risks in a systematic and transparent way.

The design and implementation of risk management will depend on the diverse needs of each organisation, its specific objectives, context, structure, operations, operational processes, projects, services, etc.

The approach is structured around three key elements for effective risk management24:

- The principles for risk management.
- The supporting structure.
- The risk management process.
- -ISO 31000 is designed to help companies to25:
- Increase the likelihood of achieving objectives.
- Encourage proactive management.
- Be aware of the need to identify and address risk throughout the enterprise.

ISSN 2524-2016

- Improve in the identification of opportunities and threats.
- Comply with relevant legal and regulatory requirements as well as international standards.
- international standards.
- Improve financial reporting.
- Improve governance.
- Improve stakeholder confidence.
- Establish a reliable basis for decision-making and planning.
- Improve controls.
- Allocate and effectively use resources to address risk.
- Improve operational effectiveness and efficiency.
- Improve health and safety and environmental protection.
- Improve loss prevention and incident management.
- Minimise losses.
- Improve organisational learning.
- Improve business resilience.
- -For greater effectiveness, risk management based on ISO 31000 in a company is likely to take into account the following principles26:
- Create value. Helping to achieve objectives and improve aspects such as occupational health and safety, legal and regulatory compliance, environmental protection, etc.
- It is integrated into a company's processes. It should not be understood as an isolated activity but as part of the main activities and processes of an organisation.
- It is part of decision-making. It assists decision making by evaluating information about different options.
- It deals explicitly with uncertainty. Addresses those aspects of decision-making that are uncertain, the nature of that uncertainty and how it can be dealt with.
- It is systematic, structured and appropriate. Contributes to efficiency and reliable results.
- It is based on the best available information. The inputs to the process are based on sources of information such as experience, observation, forecasts and expert opinion.
- It is tailor-made. It is aligned with the company's external and internal context and risk profile.
- It takes into account human and cultural factors. Recognises people's capabilities, perceptions and intentions, which are likely to facilitate or hinder the achievement of objectives.
- Is transparent and inclusive. Appropriate and timely involvement of stakeholders and decision-makers at all levels ensures that risk management remains relevant and up-to-date.
- It is dynamic, iterative and responsive to change. The enterprise should ensure that risk management detects and responds to business changes.
- Facilitates continuous business improvement.

ITGI - El marco informático del riesgo

- The RISK IT framework is intended for a broad audience, as risk management is a global practice and a strategic requirement in any organisation. The target audience includes‖27:
- Senior executives and board members who need to set direction and monitor risk at the organisational level.
- IT and business department managers who need to define the risk management process.

- Risk management professionals who need specific direction regarding IT risks.

- External stakeholders.

The RISK IT framework is based on organisational risk management (ERM) principles, standards and frameworks such as COSO ERM 2 and AS/NZS43603, and provides information on how to apply these principles to IT. RISK IT applies the generally accepted concepts of the main standards and frameworks, as well as the main concepts of other IT risk management related standards.

Although RISK IT aligns with the main ERM frameworks, the presence and application of these frameworks is not a prerequisite for the adoption of RISK IT. By adopting RISK IT in organisations, all ERM principles will automatically apply. In the event that ERM is present in some form in the organisation, it is important to leverage the strengths of the existing ERM programme as this will help the organisation to adopt risk management, save time and money and avoid misunderstandings about specific IT risks that can lead to increased business risk.

RISK IT is defined and based on a set of guidelines for effective IT risk management. These guidelines are based on commonly accepted ERM principles that have been applied in the IT domain. The IT risk process model is designed and structured to make it feasible for organisations to put the principles into practice and benchmark their results.

- -The RISK IT framework is based on IT risks. In other words, organisational risk is related to the use of IT. The connection to the organisation is based on the principles on which the framework is built, i.e. effective governance of the organisation and management of IT risks, Some of them are‖28:

- Always align with organisational objectives.

- Align IT management with organisational risk related to total ERM.

- Balance the costs and benefits of IT risk management.

- Promote open and fair communication of IT risks.

- Setting the right tone from a top-down approach, defining and enforcing staff accountability with well-defined and acceptable tolerance levels.

- -Through IT risk management, a process model has been developed that will be familiar to COBIT and Val IT users. Guidance is provided on key activities within each process, responsibilities for the process, information flows between processes and process performance management. The model is divided into three domains: risk governance, risk assessment and risk response, each with three -processes‖29:

- Risk Governance (RM)

- Establish and maintain a common risk view.

- Integrate with ERM.

- Make risk-aware decisions for the business. Risk assessment (RE)

- Collect data.

- Analyse risks.

- Maintain risk profile.

- Risk response

- Articulate risk

- Manage risks

- React to events

Risk Certification

Introduced in 2010, the Certificate in Risk and Control Information Systems (CRISC) is a new certification offered by ISACA and is based on the association's intellectual property, independent market research and input from subject matter experts around the world.

ISSN 2524-2016

The certification is designed for IT and business professionals who identify and manage risk by developing, implementing and maintaining appropriate systems of information controls.

- -The CRISC designation is designed for‖30:
- IT professionals.
- Risk professionals.
- Economic analysis.
- Project managers.
- Compliance professionals.
- -The CRISC designation focuses on‖31:
- Identification, assessment and evaluation of responses to risks.
- Risk monitoring.
- It is control design and implementation.
- It is monitoring, control and maintenance.

CRISC prepares IT professionals for future professional growth by linking IT risk management with enterprise risk management. Professionals from a wide range of functions including IT, security, audit and compliance have achieved CRISC certification since it was established in April 2010. To date, more than 16,000 professionals are CRISC certified. Of these professionals, more than 1,200 are CIOs, CISOs and compliance, risk and privacy managers.

Each company has to select the methodology that meets its requirements and objectives. However, if a structured and systematic process to manage risk is to be specified.

Within Corporate Governance, IT-related Risk Management is being addressed and understood as a key aspect of business and IT Governance is becoming increasingly important as it is integral to the success of the enterprise by ensuring measurable, efficient and effective improvements of business-related IT processes.

Conclusions

IT governance is an integral part of corporate governance, understood as a set of practices and responsibilities exercised by the board of directors and board of management of the corporation, with the objective of providing strategic direction, ensuring that objectives are achieved, facilitating that risks are properly managed and verifying that the organisation's resources are used in a responsible manner, taking into account the demands of different stakeholders, and the continuously evolving corporate environment. In this context, IT governance comprises the leadership, organisational structures and processes that ensure that the organisation's IT underpins and extends the organisation's objectives and strategies.

IT governance is the responsibility of senior management to ensure that information technology supports business objectives and strategies. IT Governance is a simplified, schematic and conceptual representation that provides a framework for:

- Align IT objectives with the business.
- Generate and sustain value.
- Manage risks to an acceptable level.

IT governance guides how to generate value for the organisation and its stakeholders, and minimise risks, by aligning strategy, managing the necessary resources, and developing tools for measuring and communicating the different facets of performance. Efficient and effective use of IT is likely to generate value for the organisation.

ISSN 2524-2016

The standard tools and certifications available to organisations to achieve alignment of IT strategy with the organisation's overall business strategy (and how this alignment generates value), for the construction of appropriate measures and indicators to guide managers and executives in the control and implementation of IT strategy, and for the proper coordination of the resources that an organisation has or can afford to acquire.

All organisations, regardless of size or sector, are exposed to a number of threats that make them vulnerable and are likely to hinder the successful achievement of their objectives, such as operational accidents, illness, fire or other natural disasters.

IT governance is the responsibility of the members of the Management Committee and the senior management of the organisation.

This is an important issue, which derives from the inclusion of IT governance within corporate governance, and which suggests that we are not talking about the management of an IT department or the simple provision of IT services in organisations.

Boards typically lack adequate information on IT strategy as well as IT management. But as Boards become more involved in the

But as Boards become more involved in IT decisions, understand their roles and delve deeper into the definition of strategy, IT becomes more effective in supporting the business.

In IT Governance, a key role of both the Chief Executive Officer (CEO) and the Chief Information Officer (CIO) develops, especially the latter, which requires new competencies, knowledge and managerial skills. Business executives are as responsible for the successful use and management of IT and the delivery of business value as the CIO.

The main objective of IT governance is to achieve alignment between business strategy and IT strategy. This process is essential for IT governance to fulfil its primary function of delivering value to stakeholders while minimising risk.

IT governance includes strategies, policies, responsibilities, structures and processes for the use of IT in an organisation. The inclusion of present and future operational and strategic elements is an essential aspect of IT governance, and guides the development of management and administration tasks. Governance and management or administration should not be confused, because the former establishes the systems and policies that guide and control the latter.

For IT governance, alignment implies more than strategic integration between the (future) IT organisation and the future business organisation. It also implies that IT operations are aligned with ongoing business operations. Of course, IT alignment is difficult to achieve when the business model is not clearly integrated and shared across the different units and areas that make up the organisation.

Organisations have to manage the risk that at any given point in time may affect and negatively impact their activities and processes, thereby jeopardising the achievement of their objectives. In the IT domain, it is necessary to analyse how to preserve business value through the security provided by IT in order to protect their assets, maintain continuity of services and recover from a disaster. But in designing their future strategies they must also assess the new risks that arise from the incorporation of IT into the organisation's processes and strategies.

From a strategic point of view, proper risk management means preserving the ability of the business to deliver results in the medium and long term. The organisation's management is responsible for using and/or equipping itself with the capabilities and competencies it requires to deploy its strategy and achieve the ultimate goals embodied in its mission.

Another fundamental aspect of risk management is to ensure continuity of operations that will secure the organisation's performance and preserve its ability to achieve its objectives in the medium and short term. To this end, it is feasible to use ISO 31000 and CRISC and other business continuity management mechanisms to identify potential accidents that threaten the organisation and to formulate and implement viable continuity strategies.

ISSN 2524-2016

References

AEC-ISO 31000, [En línea]. Disponible en http://www.aec.es/web/guest/centro-conocimiento/iso-31000, accesado el 15 de mayo de 2014.

CRISC, [En línea]. Disponible en http://www.isaca.org/chapters7/Madrid/Certification/Pages/Page4.aspx, accesado el 27 de abril de 2014.

Dahlberg, T. y Kivijarvi, H. (2006).An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. Proceedings of the 39th Hawaii International Conference on System Sciences. IEEE Computer Society.

Fernández Martínez, Antonio y Faraón Llorens Largo. Gobierno de las TI para universidades, En línea .

Disponible en http://www.crue.org/Publicaciones/Documents/Gobierno%20TI/gobierno_de_las_TI_para_universidades.pdf, accesado el 5 de mayo de 2014.

Fernando, Solares Valdes, Tesis-. Instrumentación de Gobierno de Tecnología de Información en una Institución Pública, Universidad La Salle Pachuca. 2010.

ISACA, CGEIT - Certified in the Governance of Enterprise IT, [En línea]. Disponible en http://www.ucertify.com/l/es/exams/ISACA/CGEIT.html, accesado el 9 de mayo de 2014

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition, [En línea]. Disponible en http://www.iso27001security.com/html/27005.html; accesado el 25 de abril de 2014.

ISO 31000 Risk Management | BSI Group, [En línea]. Disponible en http://www.bsigroup.com/en-GB/iso-31000-risk-management/, accesado el 6 de mayo de 2014.

ISO 31000 - Risk management – ISO, [En línea]. Disponible en http//www.iso.org/iso/iso31000. Accesado el 4 de Mayo de 2014.

ISO 38500. ISO/IEC 38500:2008 Corporate Governance of Information, [En línea]. Disponible en Technology. http://www.iso.org/iso/pressrelease.htm?refid=Ref1135, accesado el 30 de abril de 2014.

IT Governance Institute, [En línea]. Disponible en http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx; Internet; accesado el 1 de Abril de 2014.

Marco de Riesgos de TI, [En línea]. Disponible en http://www.info.unlp.edu.ar/uploads/docs/risk_it.pdf, accesado el 11 de mayo de 2014

Peter D. Weill and Jeanne W. Ross, IT Governance. Harvard Business Review Press. U.S.A. 2004.

Un marco de negocio para el gobierno y la gestión de las TI de la empresa, En línea . Disponible enhttp://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf, accesado el 29 de abril de 2014. Turban, E., Leidner, D., McLean, E., Wetherbe, J. (2008). Information Technology For Management: Transforming Organizations In The Digital Economy, 6th Ed. Wiley.

Yanosky, R. Y Borreson Caruso, J. (2008).Process and Politics: IT Governance in Higher Education. ECAR Key Findings. EDUCASE, [En línea]. Disponible en http://net.educause.edu/ir/library/pdf/ekf/EKF0805.pdf, accesado el 9 de Mayo del 2014