Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Diseño de una metodología de gestión de riesgos de seguridad de la información para entidades financieras

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTORES

Luz Angélica MONTOYA ANGULO

Michael Alexander LÓPEZ MARTÍNEZ

ASESOR

Walter Pedro CONTRERAS FLORES

Lima, Perú

2011

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DISEÑO DE UNA METODOLOGIA DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION PARA ENTIDADES FINANCIERAS

Autores: MONTOYA ANGULO, Luz Angélica
LÓPEZ MARTÍNEZ, Michael Alexander
Asesor: CONTRERAS FLORES, Walter Pedro

Titulo: Tesina, para optar el Título Profesional de Ingeniero de Sistemas
Fecha: Julio del 2011

RESUMEN

El crecimiento acelerado de los mercados financieros y la evolución de la bancarización[1], ha significado que los ciudadanos acudan a las instituciones financieras en busca de un servicio de ahorro para sus recursos financieros y en la oportunidad de poder acceder a un crédito en forma oportuna y eficaz. Dicho crecimiento financiero ha generado también un uso creciente de tecnologías de información y comunicaciones, la cual conlleva a una mayor dependencia hacia ella y por lo tanto, los riesgos asociados se transfieren a los procesos del negocio; lo cual, involucra una responsabilidad de la Alta Dirección respecto a la gestión de dichos riesgos, ya que el no hacerlo podría poner en riesgo la seguridad de su

[1] Por bancarización entendemos que es el grado de utilización del sistema bancario por parte del público y por lo tanto la bancarización no es más que el conjunto de actividades que permiten que todos puedan acceder al sistema financiero.

información y la continuidad de sus operaciones, generando incuantificables pérdidas financieras y hasta la desaparición de la Entidad.

Es por ello, que tanto organizaciones internacionales como gubernamentales de nuestro País emitieron una serie de normas, estándares y mejores prácticas como: COBIT **"**Objetivos de Control para la información y Tecnologías relacionadas: PO9 Evaluar riesgos de TI", ISO 27002:2005 "Código para la práctica de la gestión de la seguridad de la información", COSO-ERM "Gestión de Riesgos Corporativos", MAGERIT V2.0 "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", OCTAVE "Metodología de Análisis y Gestión de Riesgos", Mehari "Método de Gestión y Análisis de Riesgos, NIST SP 800-39 "Gestión de Riesgos de los Sistemas de Información, una perspectiva organizacional", AS/NZS 4360:2004 "Norma de Gestión de Riesgos", NIST SP 800-30 "Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información", y la Circular S.B.S Nº G-140 "Gestión de Seguridad de la Información ", que permiten a las Entidades Financieras poder hacer frente al desafío de lograr una adecuada gestión de los procesos, las personas, la tecnología y los eventos externos en forma efectiva y sustentable, bajo un adecuado ambiente de control interno.

Para el éxito de la gestión de los riesgos de seguridad de la información es necesario el liderazgo de la Alta Dirección y el compromiso de todos los miembros de la organización, hacia una cultura de control interno y prevención del riesgo, basado en los diferentes lineamientos, marcos de referencia, estándares y regulaciones vigentes, adaptado a las necesidades y requerimientos de cada Entidad, buscando la seguridad de la información y la continuidad del negocio; de tal manera, que se agregue valor y ventaja competitiva a las operaciones que realizan.

Es necesario que las entidades financieras diseñen, implementen y mejoren una metodología de gestión de riesgos con la finalidad de garantizar la seguridad de la información y la continuidad de las operaciones.

La presente tesina, busca diseñar una metodología de gestión de riesgos de seguridad de la información que busque proteger los activos de información de la organización tomando como referencia los lineamientos y principios de ISO 27002:2005, COSO-ERM, NIST SP 800-39 y MAGERIT V 2.0.

El punto de partida de la metodología, es la identificación y tasación de los activos de información, identificación de las amenazas más potenciales así como las vulnerabilidades más importantes a las que puedan estar expuestos dichos activos. Seguidamente se debe realizar el análisis y evaluación de riesgos, considerando la probabilidad, impacto y relevancia para cada vulnerabilidad y amenaza asociada a cada uno de los activos de información. Finalmente se desarrolla, se seleccionan e implementan controles que minimicen el riesgo y contribuyan a garantizar la seguridad de los activos de información.

En el sistema financiero proteger la información ante cualquier riesgo se ha convertido en un tema de gran trascendencia, habiendo pasado a ocupar un lugar prioritario en las agendas de los reguladores, de los supervisores, de las entidades, de los investigadores y de todos los interesados en el sector financiero, puesto que garantiza su competencia en el mercado y el desarrollo exitoso del negocio.

Palabra claves: Seguridad de la Información, Gestión de Riesgos de Seguridad de la Información, ISO 27002:2005, COSO-ERM, NIST SP 800-39, MAGERIT V 2.0, Entidad Financiera.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADEMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DESIGN OF A METHODOLOGY FOR RISK MANAGEMENT OF INFORMATION SECURITY FOR FINANCIAL INSTITUTIONS

Authors: MONTOYA ANGULO, Luz Angélica
LÓPEZ MARTÍNEZ, Michael Alexander

Advisor: CONTRERAS FLORES, Walter Pedro

Title: Tesina, para optar el Título Profesional de Ingeniero de Sistemas

Date: July 2011

ABSTRACT

The rapid growth of financial markets and the evolution of banking have meant that people go to financial institutions in search of savings for their financial resources and the opportunity to access credit in a timely and effective manner. This financial growth has also generated an increasing use of information technologies and communications, which leads to greater dependence on them. Therefore, the risks are transferred to the business process, which involves a responsibility of senior management, because failure to do so could jeopardize the security of their information and the continuity of its operations, generating not quantifiable financial losses and even the disappearance of the institution.

Therefore, both international and governmental organizations of our country issued a set of rules, standards and best practices such as: COBIT "Control Objectives for Information

and Related Technologies: PO9 Assess risks of IT", ISO 27002:2005 "Code of practice for the management of information security", COSO-ERM "Enterprise Risk Management", MAGERIT V2.0 "Methodology for Analysis and Risk Management for Information Systems", OCTAVE "Methodology for Analysis and Risk Management", Mehari "Method of Risk Analysis and Management", NIST SP 800-39 "Risk Management of Information Systems, an organizational perspective", AS / NZS 4360:2004 "Risk Management Standard", NIST SP 800-30"Risk Management Guide of Information Technology systems", and the SBS Circular No. G-140 "Managing Information Security", which allow financial institutions to cope with the challenge of ensuring proper management of processes, people, technology and external events in an effective and sustainable manner, and in a proper internal control environment.

For the successful of risk management of information security, it is required the leadership of senior management and the commitment of all members of the organization towards a culture of internal control and risk prevention, based on different guidelines, frameworks, standards and regulations, suited to the needs and requirements of each entity. And seeking the information security and business continuity, in order to add value and competitive advantage to the operations they perform.

It is necessary for financial institutions to design, implement and improve a risk management methodology in order to ensure the information security and continuity of operations.

This thesis seeks to design a risk management approach to information security that protect the information assets of the organization by reference to the guidelines and principles of ISO 27002:2005, COSO-ERM, NIST SP 800-39 and MAGERIT V 2.0.

The starting point of the methodology is the identification and valuation of information assets, identifying of potential threats and the most important vulnerabilities to which these assets may be exposed. Then, it must be perform the analysis and the risk assessment, considering the probability, impact and relevance for each vulnerability and threat associated with each of the information assets. Finally, it is developed; selected and implemented controls that minimize the risk and help ensure the security of information assets

In the financial system, to protect the information from any risk has become a topic of great importance, an essential topic on the agendas of regulators, supervisors, agencies, researchers and all stakeholders in the financial sector.

Keys Words: Information Security, Risk Management of Information Security, ISO 27002:2005, COSO-ERM, NIST SP 800-39, MAGERIT V 2.0, Financial Institutions.