Tesis de Maestría en Administración de Empresas

María Florencia Gaibazzi[*]

Director:

Antonio Rubulotta

GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA DE LAINFORMACIÓN EN LOS BANCOS[**]

Mención Provincial Honoraria 2010 a Tesis De Maestría[***]

Resumen. La información es un recurso muy importante dentro de los activos de una organización, tiene un valor determinado de acuerdo al grado de criticidad que posea, por consiguiente debe ser debidamente protegida tanto interna como externamente. La seguridad de la información resguarda a la "información" de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la organización.

Con el advenimiento de las nuevas Tecnologías Informáticas y de Comunicación (TIC), la operatoria bancaria se hizo aún más riesgosa porque al utilizar medios electrónicos para la captura, procesamiento de los datos y transmisión de la información es

---

[*] Docente-Investigadora de la Facultad de Ciencias Económicas y Estadística de la UNR.

[**] Defendida en la Facultad de Ciencias Económicas y Estadística de la U.N.R. el 8 de septiembre de 2010.

[***] Otorgado por la Secretaría de Estado de Ciencia, Tecnología e Innovación del Gobierno de la Provincia de Santa Fe, con fecha 18 de julio de 2011 según Resolución Nº 046 de la misma Secretaría.

Contacto: mgaibaz@fcecon.unr.edu.ar

necesario contar con medidas adecuadas a los tiempos que corren para asegurar los tres principios básicos de seguridad: confidencialidad, integridad y disponibilidad de la información.

Por todo lo expresado anteriormente y siendo el B.C.R.A. el ente regulador de la actividad financiera y supervisor de las Entidades Financieras (EF), propone ampliar la normativa vigente sobre Seguridad de la Información, actualizarla y detallar con claridad los requisitos mínimos en cuanto a la gestión, implementación y control de los riesgos relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados con el fin de que las EF implementen las mejores prácticas de control y seguridad, teniendo en cuenta el riesgo de dicha actividad, la criticidad de sus activos y la adopción de la Normativa Internacional vigente.

Palabras clave: Auditoría; Seguridad física; Seguridad lógica.

Abstract. Information is a very important resource of the assets of an organization. Its value is determined by the degree of critical relevance and therefore it should be properly protected both internally and externally. Protection of information safeguards “information” from a wide range of threats in order to ensure business continuity, minimize self damage and maximize return on investment and opportunities.

Protection of information is achieved by implementing a suitable set of controls, which include policies, practices, procedures, organizational structures and software functions.

These controls should be established to ensure that they achieve the specific objectives of the organization’s security.

With the advent of new Information Technology and Communication (ITC), banking operations became even more risky because using electronic means to capture, data processing and transmission of information is necessary to have appropriate measures in time running to secure the three basic principles of security: confidentiality, integrity and availability of information.

Given that the Central Bank of Argentina (Banco Central de la República Argentina) regulates financial activity and supervises Financial Institutions (FI), it seeks to increase existing rules on information security. It also seeks to update and clearly detail the minimum requirements for management , implementation and control of risks associated with Information Technology, Information Systems and Resources Associated with the FI to implement the best practices of control and security, taking into account the risk of that activity, the criticality of assets and adoption of international guidelines.

Key words: Audit, Physical security, Logical security

***Alcance**:* Esta tesis centró su estudio en el análisis del impacto producido en la estructura y funcionamiento organizacional por la aplicación, adopción y puesta en vigencia a partir del 27 de junio de 2007 de la normativa sobre "Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras", según la comunicación "A" 4609 del B.C.R.A. (NGSSI), en bancos que tienen su casa central operando en la ciudad de Rosario a octubre de 2008.

***Objetivo General*:** Describir el impacto en la estructura y funcionamiento organizacional, en bancos que tienen su casa central operando en la ciudad de Rosario, por la aplicación de la NGSSI.

***Unidades de Análisis**:* Banco Regional: Nuevo Banco de Santa Fé S.A., Banco que cotiza en Bolsa: Bisel Grupo Macro, Banco Local: Banco Municipal de Rosario.

***Evidencia Empírica**.* Nos encontramos ante la presencia de tres EF con distintos orígenes y distintas experiencias de vida institucional, política y organizacional que deben cumplir con la misma NGSSI que el B.C.R.A. como órgano regulador de la actividad financiera se los impone.

Aportes de ésta tesis: A través del desarrollo de ésta tesis de maestría se pudo vislumbrar que:

- Los Bancos debieron emprender distintas acciones relacionadas con: la gestión de recursos humanos, la estructura y funcionamiento organizacional, la planificación y control de la seguridad de los sistemas y las tecnologías de la información, la política de outsourcing, etc., para poder implementar la NGSSI teniendo en cuenta sus diferentes situaciones al tratarse de EF muy disímiles en su constitución, origen, funcionamiento y marco jurídico.
- El B.C.R.A. a través de la NGSSI logró que todas las EF tengan una misma estructura organizacional y control interno mínimos sin distinción de tamaño, capital, conformación jurídica, cantidad de sucursales. Para lo cual al confeccionar la NGSSI consideró diversos instrumentos de control interno sobre la materia, tales como:
    a) Las sanas o mejores prácticas emitidas por el Comité de BASILEA para la administración del riesgo operacional y la tecnología informática
    b) La norma IRAM-ISO 17799 código de práctica para la administración de la seguridad informática
    c) Ley de Sarbanes-Oxley
    d) La norma ISO 27001 de Gestión de la Seguridad Informática
    e) La norma ISO 15408 criterios de evaluación de controles internos en TI y SI
    f) COBIT Objetivos de Control para la Tecnología Informática

más la experiencia propia en el control del entorno financiero argentino, mediante la aplicación de las normativas que la antecedieron tales como: Comunicación "A" 2659 y Comunicación "A" 3198.

- En cuanto al entorno de seguridad informática, a través de la puesta en vigencia de la NGSSI, el interés del B.C.R.A. fue alcanzado, al establecer un marco adecuado de criterios de control sobre los entornos de tecnología informática y sistemas de información que permita proteger los activos y recursos informáticos de las EF, acorde con el volumen y complejidad de sus respectivas estructuras.
- Según las conversaciones y reuniones mantenidas con los auditores internos de sistemas, responsables de seguridad informática, gerente de administración, gerente de planificación y control de gestión, gerente de tecnología informática de las EF analizadas, los cambios más importante y de mayor repercusión fueron los siguientes:

    a) La responsabilidad primaria de la aplicación y cumplimiento de la NGSSI recae sobre el directorio,

    b) se crea un Comité de Tecnología Informática y un área específica de protección de activos de información,

    c) se logró que las EF alinearan los Proyectos de Tecnología Informática y Sistemas al Plan Estratégico de la EF,

    d) cambiar la visión que se tenía de la informática como una mera herramienta y pasar a considerarla como una herramienta muy importante que posibilita la concreción de los objetivos organizacionales.

- El B.C.R.A. con la puesta en vigencia de la NGSSI aporta un elemento más al cumplimiento de una de sus funciones que es la de crear a través de un pertinente marco normativo, el contexto necesario para desarrollar y fortalecer la estabilidad financiera.

De todo lo dicho anteriormente se desprende que la banca argentina (con las limitaciones expuestas en el análisis de tres bancos) mediante la implementación de la NGSSI alcanza un nivel de seguridad y control interno informático comparable a los de la banca internacional, adoptando los estándares internacionales de Seguridad Informática.

Bibliografía

Piattini M. G. & Del Peso E. (2001). *Auditoría Informática .Un enfoque práctico* (2ª Ed.). España: Alfaomega Ra-Ma,

Comunicación A 4609 BCRA (2006, diciembre). *Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnologías Informática, Sistemas de Información y Recursos Asociados para las EF, Auditoría Externa de Sistemas y Gerencia de Análisis y Auditoría del BCRA, Buenos Aires.*