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

Metodología para la gestión de riesgos de tecnología de información en una institución financiera

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTORES

César Alberto CONDORI ARI

Oriel GONZALES AQUINO

ASESOR

Gloria Helena CASTRO LEÓN

Lima, Perú

2008

Referencia bibliográfica

Condori C. & Gonzales O. (2008). *Metodología para la gestión de riesgos de tecnología de información en una institución financiera*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Este trabajo esta dedicado a toda nuestra familia en especial a nuestros padres.

AGRADECIMIENTOS

A la profesora Gloria Castro León, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

Al profesor José Piedra Isusqui y Armando Fermín Pérez por sus orientaciones, consejos y revisiones del presente trabajo.

A mis colegas y amigos por sus observaciones y porque en todo momento me incentivaron para que culmine este trabajo.

A todas aquellas personas que indirectamente me ayudaron para culminar este trabajo y que muchas veces constituyen un invalorable apoyo.

Y por encima de todo doy gracias a Dios.

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TECNOLOGIA DE INFORMACION EN UNA INSTITUCION FINANCIERA

RESUMEN

El Banco es una institución que brinda servicios financieros al sector público y clientes en general. Sus actividades principales pasan por el rol social que cumple al satisfacer las necesidades de interconexión financiera en más provincias y distritos del país, así como cumplir con los pagos al personal público y privado del país.

El Banco, como integrante del sistema financiero nacional y tiene la obligación de garantizar la adecuada administración de la información y la tecnología en que ésta se sustenta, las buenas prácticas aplicadas al sector tecnología de información a nivel nacional e internacional, las recomendaciones de empresas especializadas en consultoría de riesgos y adecuarse a las exigencias de la Resolución Nº 37-2008 de la Superintendencia de Banca y Seguros, motivo por la cual es necesario tomar las medidas para administrar apropiadamente los riesgos de tecnología de información.

La administración de Riesgos de tecnología de información es parte fundamental del tratamiento de Riesgos de Operación, tratamiento relativamente nuevo en nuestro país, por lo cual si bien es cierto no existe un estándar de adecuación en el sistema financiero nacional, se han puesto bases sólidas que garantizan la seguridad de los procesos, la información y la continuidad del negocio.

A ello, es necesario agregar que las disposiciones reguladoras en el país exigen la cuantificación de los riesgos para implementar herramientas que hagan posible cumplir con las provisiones operativas que se agregaran a las provisiones crediticias y financieras.

El modelo de administración de los Riesgos de Tecnología de Información y los resultados aquí presentados se ejecutará aplicando las siguientes etapas de desarrollo de procesos:

Etapa 1.- Estructura Organizacional y procedimiento de tratamiento de riesgos
Etapa 2.- Gestión de Riesgos [1] de Tecnología de Información.
Etapa 3.- Tratamiento de Procesos críticos de Negocio

Esta metodología nos permitirá alcanzar los siguientes resultados: Administrar los riesgos estructurales y coyunturales a los que está expuesto la institución, cumplir de la regulación vigente (Superintendencia de banca y Seguros), implementar medidas de mitigación de los riesgos de tecnología de información, clasificar los procesos críticos de negocio y alcanzar resultados económicos, sociales y operativos positivos.

[1] Entiéndase por Gestión de Riesgos al proceso de ponderación de las distintas opciones normativas a la luz de los resultados de la evaluación de riesgos y, si fuera necesario, de la selección y aplicación de las posibles medidas de control apropiadas, incluidas las medidas reglamentarias

METHODOLOGY FOR THE ADMINISTRATION OF RISKS OF TECHNOLOGY OF INFORMATION IN A FINANCIAL INSTITUTION

ABSTRACT

The Bank is the institution that offers to financial services to the public sector and clients in general. Their main activities happen through the social roll that fulfills when satisfying the necessities with financial interconnection in more provinces and districts of the country, as well as to fulfill the payments to the public and private personnel of the country.

The Bank, like member of the national financial system and, being necessary to guarantee the suitable information management and the technology in that this one is sustained, the good practices applied to the sector technology of information at national and international level, the recommendations of companies specialized in consultancy of risks and adapting to the exigencies of Resolution Nº 0037-2008 of the Supervision of Bank and Insurances has considered necessary to take the measures appropriately to administer the risks of information technology.

The administration of Risks of information technology is fundamental part of the treatment of Risks of Operation, relatively new treatment in our country, thus although it is certain does not exist a standard of adjustment in the national financial system, bases have been put solid that guarantee the security of the processes, the information and the continuity of the business.

To it, it is necessary to add that the regulating dispositions in the country demand the quantification of the irrigations to implement tools that do possible to fulfill the operative provisions that were added to the credit and financial provisions.

The model of administration of the Risks of Technology of Information and the results presented/displayed here will be executed applying the following stages of development of processes:

Stage 1. - Organizacional Structure and procedure of treatment of risks
Stage 2. - Management of Risks of Technology of Information.
Stage 3. - Treatment of critical Processes of Business

This development will allow us to reach the following results: To allow the administration of the structural and conjunctural risks to which the institution is exposed, fulfillment of the effective regulation (Supervision of bank and Insurances); To implement measures of mitigación of the risks of information technology; to classify the critical processes of business and of reaching economic, social and operative results.

ÍNDICE

1. INTRODUCCIÓN 14

1.1.- ANTECEDENTES 14
1.2.- DEFINICIÓN DEL PROBLEMA 16
1.3.- OBJETIVOS 18
1.3.1.- OBJETIVOS GENERALES 18
1.3.2.- OBJETIVOS ESPECÍFICOS 18
1.4.- JUSTIFICACIÓN 20
1.5.- PROPUESTA 22
1.6.- ORGANIZACIÓN DE LA TESINA 23

2. MARCO TEORICO 26

2.1 CONCEPTOS INMERSOS EN LOS RIESGOS DE TECNOLOGIA 26
2.1.1.- METODOLOGÍA 26
2.1.2.- RIESGO 26
2.1.3.- CALIFICACION Y CUANTIFICACION DE UN RIESGO 27
2.1.4.- CONCEPTO DE RIESGO DE TECNOLOGIA DE INFORMACION 28
2.1.5.- GESTION INTEGRAL DE RIESGOS 29
2.1.6.- SEGURIDAD DE INFORMACION 30
2.1.7.- PLAN DE CONTINUIDAD DE NEGOCIOS 31
2.1.8.- ORÍGENES DE LA ADMINISTRACION DE LOS RIESGOS DE TECNOLOGIA 32
2.1.9.- NUEVO ACUERDO DE CAPITAL (NAC) - BASILEA II 32
2.1.10.- INFORMACIÓN Y SISTEMA INFORMÁTICO 34
2.1.11.- CONFIDENCIALIDAD 36
2.1.12.- INTEGRIDAD 36
2.1.13.- DISPONIBILIDAD 37
2.1.14.- AMENAZAS A LA INFORMACIÓN 38
2.1.15.- ATAQUES PASIVOS 38
2.1.16.- ATAQUES ACTIVOS 38
2.1.17.- OTROS ASPECTOS RELACIONADOS 39

3. ESTADO DEL ARTE 42

3. 1 METODOLOGÍAS 42
3.1.1 METODOLOGÍA MAGERIT 42
3.1.2. METODOLOGÍA OCTAVE 44
3.1.3. METODOLOGÍA CRAMM 46

3.1.4. METODOLOGÍA COSO 47

3.2 EVALUACIÓN DE METODOLOGÍAS 68

4. RESOLUCIÓN DEL PROBLEMA APLICANDO LA METODOLOGÍA PLANTEADA 74

4.1 ESTRUCTURA ORGANIZACIONAL Y PROCEDIMIENTO DE TRATAMIENTO DE RIESGOS 74

4.2 GESTION DE RIESGOS DE TECNOLOGIA DE INFORMACION 76
4.2.1. DIAGNÓSTICO INICIAL DE PROCESOS CRÍTICOS 77
4.2.2 EVALUACIÓN DE VULNERABILIDADES Y RIESGOS, DISEÑO E IMPLEMENTACIÓN DE MEDIDAS DE MITIGACIÓN Y CONTROL DE RIESGOS 78

5. CONCLUSIONES Y FUTUROS TRABAJOS 94

6. REFERENCIAS BIBLIOGRAFICAS 97

7. ANEXOS 102

7.1. ANEXO 1: RESOLUCIÓN SBB N°006.2002 103
7.2. ANEXO 2: CIRCULAR Nº G-105-2002, ... 111
7.3. ANEXO 3: RESOLUCIÓN SBB N°37-2008 121
7.4. ANEXO 4: EVALUACIÓN DE RIESGOS ASOCIADOS A TECNOLOGÍA DE INFORMACIÓN 138

ÍNDICE DE FIGURAS

FIGURA 1: NECESIDAD DE ADMINISTRAR LOS RIESGOS DE TECNOLOGÍA DE INFORMACIÓN……..15

FIGURA 2: PASOS REALIZADOS POR MAGERIT……...……..……39

FIGURA 3: OCTAVE ESTÁ IMPULSADO POR EL RIESGO OPERATIVO Y PRÁCTICAS DE SEGURIDAD…….……41

FIGURA 4: ENCUESTA SOBRE LA CULTURA DE RIESGOS……..……45

FIGURA 5: FORMACIÓN DEL RIESGO ACEPTADO……..……..…..50

FIGURA 6: ESTRATEGIA ORGANIZACIONAL…….……...74

FIGURA 7: ESQUEMA DE LA METODOLOGÍA……...…..…...75

FIGURA 8: MATRIZ DE EVALUACIÓN DE RIESGOS……....80

FIGURA 9: CUADRO DE EFECTIVIDAD DE LA MATRIZ DE RIESGOS RESIDUALES……...84

ÍNDICE DE TABLAS

TABLA 1: NIVELES DE IMPACTO DE LA MATRIZ DE RIESGOS. ……..…...81

TABLA 2: NIVELES DE AMENAZA U OPORTUNIDAD DE RIESGOS……..……..81

TABLA 3: RIESGO ASOCIADO……..……...82

TABLA 4: MATRIZ DE IDENTIFICACIÓN DE CONTROLES EXISTENTES……...83

TABLA 5: MATRIZ DE RIESGOS RESIDUALES……..84

TABLA 6: RIESGOS ASOCIADOS A TI: (PROCESO: DESARROLLO DE SISTEMAS)…….134

TABLA 7: RIESGOS ASOCIADOS A TI: (SERVICIOS PRESTADOS POR TERCEROS)…..135

TABLA 8: RIESGOS ASOCIADOS A TI: (SEGURIDAD DE OPERACIONES Y COMUNICACIONES)……136

TABLA 9: RIESGOS ASOCIADOS A TI: (SEGURIDAD LÓGICA)…..……...137

TABLA 10: RIESGOS ASOCIADOS A TI: (SEGURIDAD FÍSICA)……..138

TABLA 11: RIESGOS ASOCIADOS A TI: (SEGURIDAD DE PERSONAL)…….…139

TABLA 12: RIESGOS ASOCIADOS A TI: (PROCESOS DE RESPALDO)…….140

TABLA 13: RIESGOS ASOCIADOS A TI: (FLUJO DE INFORMACIÓN)……..……..141

TABLA 14: RIESGOS ASOCIADOS A TI: (CLASIFICACIÓN DE INFORMACIÓN)……..142

TABLA 15: MEDIDAS DE MITIGACIÓN A IMPLEMENTAR……..146

CAPITULO 1

INTRODUCCIÓN

1. INTRODUCCIÓN

El presente trabajo, tiene como objetivo establecer los lineamientos generales para el adecuado tratamiento de los riesgos de tecnología de información en una Institución Financiera. Estos lineamientos deben permitir establecer todos los mecanismos y acciones para cuantificar y calificar los niveles de riesgo a los cuales está expuesta la institución, esto permitirá garantizar la gestión de actividades para mitigar las posibles pérdidas que podría ocasionar la materialización de eventos clasificados como riesgo. Otro de los objetivos fundamentales es el referido al cumplimiento de los requerimientos reguladores.

1.1.- ANTECEDENTES

La Superintendencia de Banca y Seguros (SBS), ha implementado un proceso de estandarización de procesos de control que las entidades del sistema financiero deben cumplir para adecuarse a los estándares internacionales y a las mejores prácticas con relación a la administración de estos riesgos.

La Superintendencia, emitió el año 2002, la Circular Nº G-105-2002 – Ver Anexo 1- [9] la misma que estipula los puntos de partida que se debe considerar para la adecuada administración de los riesgos de tecnología de información y la elaboración de los respectivos documentos de apoyo, el plan de seguridad de información y el plan de continuidad de negocio, a esto se suma la reciente Circular Nº 37-2008 – Ver Anexo 2 – el cual establece la adecuación al nuevo enfoque de Administración Integral de Riesgos.

Finalmente, en junio de 2004, se aprobó un Nuevo Acuerdo de Capital, la cual establece una serie de principios y recomendaciones sobre Supervisión Bancaria, cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria. Cabe señalar que uno de los puntos que se desprende de los principios propuestos por el Comité de Basilea II (Nuevo Acuerdo de Capital - NAC), [11] es que las entidades financieras deberán de

establecer y asignar el capital necesario a posible materialización de los eventos de riesgos que pudieran generar una crisis bancaria.

En ese sentido, el Banco al igual que el resto de las instituciones financieras, están iniciando los proyectos relativos a la administración de riesgos de tecnología de información, ello conllevará a lograr un ambiente seguro en el negocio financiero.

La adecuada administración de riesgos, se origina en las actividades de evaluación de procesos, requerimientos legales, contractuales y reguladores, los principios propios de la actividad inherente al negocio de la empresa, los diversos incidentes ocurridos en la seguridad de activos tanto a nivel del entorno como a los activos de información y los sistemas y la percepción de fallas por parte de los involucrados en el proceso del negocio. Con una planificación integral, anticipada, efectiva, es posible responder rápida y apropiadamente cualquier tipo de riesgo que atente en contra de los sistemas de información dada las cambiantes condiciones y nuevas plataformas de computación disponibles.

La actual Administración en una Institución financiera afirma la necesidad de dar alta prioridad a la seguridad de las operaciones sociales y de los respectivos activos que soportan estas operaciones. De esta manera, un adecuado tratamiento de los riesgos operativos, surgen como una herramienta para concientizar a los miembros de una organización sobre la importancia y sensibilidad de los procesos, las personas, las actividades externas y la información y servicios críticos que permiten a la Institución desarrollarse y mantenerse en su sector de negocios. Este proceso debe mantener el compromiso de todo el personal para con la organización.

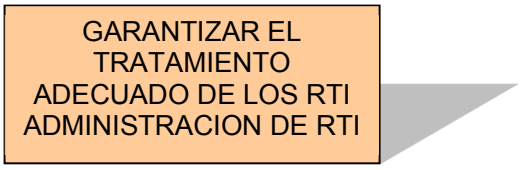
Es necesario indicar sin embargo, la existencia de factores que dificultan que la institución tenga una cultura de riesgos definida y asumida por todo el personal, factores como la resistencia al cambio por parte de empleados con un enfoque

tradicional de trabajo, con más de veinte años de servicio, hacen de este proceso un reto aun mayor que el asumido por el resto de empresas.

1.2.- DEFINICIÓN DEL PROBLEMA

La administración y tratamiento de los riesgos de operación y por ende los riesgos de tecnología de información es un requerimiento oficial relativamente nuevo en nuestro país, si bien es cierto, en los sistemas informáticos y centros de cómputo de las diferentes empresas se han tomado medidas para prevenir la ocurrencia de eventos que puedan significar pérdidas de equipos, información o sistemas, estos procedimientos de control y resguardo, en la mayoría de casos se realizaban de manera convencional pues era natural resguardar los equipos y la información que éstos contenían. Cuando empiezan a aparecer las normas y procedimientos de mejores prácticas, las regulaciones y los estándares relacionados a riesgos de operación, es que el proceso de administración de riesgos adopta realmente la dimensión que tiene ahora.

En el siguiente esquema (*Figura Nº 1*) se puede visualizar las razones por las cuales es necesario realizar una adecuada administración de los riesgos de operación y de tecnología de información y el porqué se ha convertido en una práctica necesaria, obligatoria y competitiva para las empresas financieras del país.



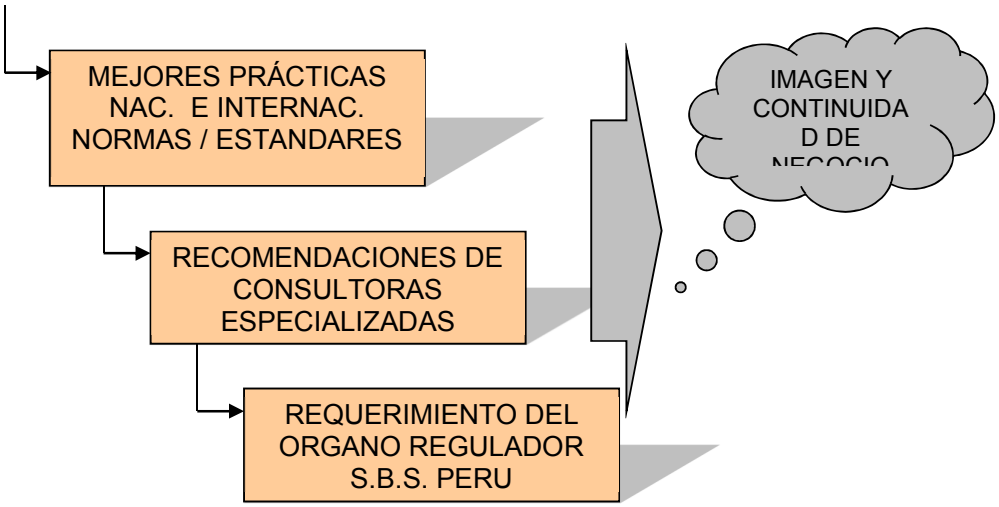


Figura Nº 1: Necesidad de Administrar los Riesgos de Tecnología de Información [4]

Si bien es cierto, las instituciones financieras han mantenido niveles de mitigación de riesgo, no existía un enfoque general y estándar para el tratamiento de los mismos, por ello y a pesar de los esfuerzos del órgano regulador, las empresas han adoptado diversos mecanismos para el tratamiento de los riesgos de tecnología de información y en general para cualquier tipo de riesgo, sin embargo, existe documentación exigida por la superintendencia que posibilita en cierta medida hablar de un tratamiento uniforme de riesgos.

El Banco, como integrante del sistema financiero nacional y eje fundamental de la economía social en el país [7], ha de considerar implementar en su estructura orgánica y en su plan operativo, la administración de los riesgos de tecnología de información considerando la importancia y la necesidad de garantizar una adecuada administración de los activos de información que permiten la continuidad operativa del negocio.

Asimismo, considerando la necesidad de cumplir con las exigencias de la Circular relacionada a la adecuada implementación de políticas y procedimientos para administrar los riesgos de tecnología de información, el Banco debe someterse a los requerimientos regulatorios con el claro objetivo de salvaguardar

la información que administra sobre todo destinada a satisfacer la demanda social del país.

1.3.- OBJETIVOS

1.3.1.- OBJETIVOS GENERALES

- Desarrollar una metodología de evaluación de riesgos de Tecnología de Información inmersos en una entidad financiera de nuestro país que permita asistir en el cumplimiento de lo normado por la Superintendencia de Banca, Seguro y AFP (SBS) [17].

- Establecer los lineamientos necesarios, para la administración de los riesgos estructurales y coyunturales a los que está expuesto la institución y establecer medidas de mitigación.

1.3.2.- OBJETIVOS ESPECÍFICOS

- Diseñar mecanismos de respuesta y control para minimizar el impacto de la ocurrencia de eventos de riesgo. Asimismo, llevar un adecuado control de las falencias asociadas a los procesos y servicios bancarios soportados por recursos de información y de tecnología.

- Determinar la posibilidad de ocurrencia y el impacto de los riesgos asociados a tecnología de información.

- Determinar y formalizar los mecanismos actuales de control y mitigación de RTI y determinar el riesgo residual actual.

- Monitorear continuamente las vulnerabilidades y las medidas de control aplicadas para mitigar los riesgos.

- Mejora de la imagen institucional al mantener un adecuado control de la información soportada en sus aplicaciones tecnológicas.

- Poseer mejores y más controlados sistemas internos.

- Concientizar internamente al personal del Banco para que sea parte de la cultura de riesgos de la institución.

1.4.- JUSTIFICACIÓN

Desde el punto de vista teórico, el presente trabajo de investigación va a permitir enriquecer la concepción teórica sobre metodologías para una adecuada Gestión de Riesgos de Tecnología de Información en una entidad financiera. Así también dar a conocer sobre los resultados obtenidos; los cuales servirán como fuente de información y antecedentes para la realización de otras investigaciones relacionadas al tema de estudio, como por ejemplo auditoria basada en riesgos.

Al desarrollar e implementar una metodología de Evaluación de Riesgos de Tecnología de Información, se conseguirá obtener efectos favorables e importantes para la organización, algunos de los cuales se detallan a continuación:

- Cumplimiento con las disposiciones dictadas por la SBS [2], en la CIRCULAR Nº G-37-2008 - Administración de Riesgos de Tecnología de Información, aprobada el 10 de enero del 2008. (Anexo Nº 2) [4]

- Participación en los retos que supondría la implementación de Basilea II en nuestro país. Si bien es cierto que, en un inicio, Basilea II esta planteado para los países mas industrializados del mundo (G-10 [3]), no se debe olvidar que al tratarse de estándares de medición y gestión de riesgos modernos, estos rápidamente se convertirán en los estándares exigidos a nivel internacional en todos los países que quieran ser competitivos a nivel mundial.

- La evolución espontánea de los Bancos (principalmente los más grandes a nivel internacional) demuestra que requieren técnicas más sofisticadas para el manejo adecuado de sus riesgos.

---

[2] SBS : Superintendencia de Banca, Seguro y AFP

[3] G -10: Grupo de los diez países mas industrializados en el mundo.

- Proporcionaría un mayor control en los riesgos de Tecnologías de Información de los riesgos considerados como críticos para la entidad.

- Mediante una gestión adecuada (identificar, evaluar y cuantificar los riesgos de TI [4]), se entenderá la forma de poder minimizar la materialización de los riesgos de TI dentro de la entidad financiera.

- Fortalecería el proceso de toma de decisiones de la alta Gerencia, correspondiente al tema de priorizar la implementación de controles para minimizar y/o eliminar los riesgos de TI considerados como críticos.

- Se dotará a la entidad financiera de un sistema de análisis adecuado, que le permitirá monitorear el estado de los eventos para la asignación de los recursos económicos que permitan implementar los controles adecuados para su mitigación, en función de sus reales necesidades y objetivos fijados.

- Fortalecería la imagen de la entidad financiera ante sus clientes, ya que estos tendrían la certeza de seguridad y continuidad de funcionamiento, de los diversos procesos críticos en los cuales se encuentran participando directa o indirectamente.

- Acreedores o potenciales socios de las entidades financieras, podrían mejorar la percepción de estas, si es que dichas entidades se encuentra regidos por los estándares y pautas generales sugeridas por el Comité de Basilea II y los lineamientos establecidos por la SBS.

Asimismo, se pretende conseguir la disminución y /o eliminación de los costos asociados a eventos de riesgo de tecnologías de Información en aspectos económicos, operativos, financieros y sociales.

---

[4] TI : Tecnología de Información.

a) COSTO ECONÓMICO

- Disminuiría el costo por pérdida y recuperación de activos de información.
- Disminución de los costos de adquisición de equipos tecnológicos, tales como los servidores principales, los servidores corporativos, servidores de banca electrónica, servidores de aplicativos en cajeros automáticos, etc.
- Disminución del costo por servicios de recuperación de dispositivos físicos

b) COSTO OPERATIVO Y FINANCIERO:

- Pérdida de información o detención de actividades operativas
- Detención de procesos de recaudación (pérdidas de ingresos de comisiones).
- Problemas con las operaciones del Banco en cajeros, ventanillas, etc.
- Salida del negocio

c) COSTO SOCIAL

- Problemas con los pagos a los clientes
- Vandalismo, huelgas, atentados
- Pérdida de reputación
- Suspensión de servicio al cliente

Esta problemática además considera los siguientes factores:

- Sanciones regulatorias
- Responsabilidades legales
- Riesgos y exposición a las amenazas internas y externas
- Preocupación de los usuarios considerando el mercado del Banco.
- Difusión de las comunicaciones

1.5.- PROPUESTA

Nuestra propuesta tiene como finalidad plantear al Banco el uso de mecanismos eficientes para la identificación, gestión, control y supervisión del riesgo tecnológico de acuerdo con los requerimientos mínimos planteados según las exigencias de la Superintendencia de Banca y Seguros [6] a las que hemos agregado algunos puntos que consideramos relevantes. La propuesta se compone de los siguientes puntos:

Identificar aquellos acontecimientos que puedan impactar en la organización impidiéndole alcanzar sus objetivos.

Realizar una valoración de los riesgos de la compañía y gestionar su tratamiento en función del riesgo aceptado en la misma.

Integrar la gestión de riesgos en los procesos de planificación estratégica de la compañía, en el control interno y en la operativa diaria de la misma [5].

1.6.- ORGANIZACIÓN DE LA TESINA

Capitulo 1: Introducción

Mencionaremos el propósito de nuestra investigación, así como la importancia e impacto que tiene en la realidad nacional; los objetivos propuestos y beneficios que se pretenden conseguir.

Capitulo 2: Marco Teórico

El propósito de este capitulo es de dar a la investigación un sistema coordinado y coherente de conceptos y proposiciones que permitan abordar el problema, describiendo detalladamente cual es el significado de los conceptos que se mencionaran durante todo el trabajo.

---

[5] Bishop, W. “The Crisis of Large Corporation Bankruptcy”, (2003).

Capitulo 3: Estado del Arte

Se realiza una comparación con algunas metodologías y estándares ya existentes relacionada con gestión de riesgos, con la finalidad de realizar una buena evaluación, gestión y administración de riesgos de Tecnología de Información.

Capitulo 4: Resolución del problema aplicando la técnica seleccionada

Se detalla la metodología planteada indicando las bases científicas en que se basa y los resultados que se obtiene, con la finalidad de realizar una buena evaluación, gestión y administración de riesgos en activos de Tecnología de Información. Asimismo, se aplica la presente metodología en la estructura organizacional del Banco de la Nación, con la finalidad entender e interpretar todo lo sustentado.

Capitulo 5: Conclusiones y futuros trabajos.

Se detalla en forma resumida, la metodología planteada, incidiendo en los diversos beneficios que traería consigo su implementación en una entidad financiera peruana. Así mismo se indica algunas buenas prácticas que sería provechoso que la entidad financiera ejecutara, al momento de implementar la Evaluación de Riesgos de Tecnología de Información. Finalmente se plantea algunos temas de interés que se pueden desarrollar en base a este trabajo.

Capitulo 6: Referencias Bibliográficas

Se detalla las diversas fuentes bibliográficas (libros, paginas de Internet, revistas, tesis, etc.), revisadas durante la realización del presente trabajo.

CAPITULO 2

MARCO TEORICO

2. MARCO TEORICO

2.1 CONCEPTOS INMERSOS EN LOS RIESGOS DE TECNOLOGIA

2.1.1.- METODOLOGÍA

Metodología es el procedimiento o conjunto de procedimientos que se utilizan para obtener conocimientos [5]. También se le puede entender como los pasos que se han seguido en:

- Una indagación determinada
- La designación de los modelos concretos de trabajo que se aplican en una determinada disciplina o especialidad.
- La referencia de procedimientos y recomendaciones que se desea a transmitir.

La metodología dependerá de los postulados que el investigador considere como válidos; de aquello que considere objeto de la ciencia y conocimiento científico; pues será a través de la acción metodológica, como recolecte, ordene y analice la realidad estudiada.

2.1.2.- RIESGO

Existe una gran variedad de definiciones o conceptos asociados a lo que es un riesgo, este se puede definir como:

- La proximidad o posibilidad de que ocurra un daño o peligro.
- Cada uno de los imprevistos y/o hechos desafortunados que puede cubrirse con un seguro.

Asimismo, al hablar de riesgos comúnmente relacionamos este concepto con las siguientes palabras: amenaza, emergencia, urgencia, apuro, etc.

Sin embargo, es necesario que podamos tratar de obtener, utilizando las anteriores ideas, un concepto formal y tal vez uno de los más usados y que

involucra tanto los hechos como las pérdidas que éstos podrían originar se adecua al siguiente: Un Riesgo es aquel evento que genera incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen. [6]

2.1.3.- CALIFICACION Y CUANTIFICACION DE UN RIESGO

Son también variadas las formas y métodos para medir un riesgo, se presume que según el tipo de riesgo en análisis, existen distintas maneras de medir el nivel de riesgo al que está expuesto el proceso o servicio en evaluación.

Al hablar de calificación, se puede considerar los objetivos del negocio, por ejemplo para los clientes de una entidad financiera, la calificación de riesgo para acceder a un crédito se mide en términos de clasificar al cliente a quien se otorga un préstamo (por ejemplo, normal, deficiente, potencial pérdida, etc.).

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran, estas escalas pueden ser ajustables para adaptarlas a las circunstancias que el análisis establezca. El análisis cualitativo se utiliza:

- Como una actividad inicial de matiz, para identificar los riesgos que requieren de un análisis más detallado.
- Cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo y
- Cuando los datos numéricos son inadecuados para un análisis cuantitativo.

---

[6] Basso, O. “Taller de Riesgos de Operación”, 2003.

Al hablar de cuantificación, el objetivo es medir numéricamente la probabilidad de que un evento de riesgo se concrete, asimismo se mide el impacto que

generaría en términos monetarios, de imagen institucional, social hacia la organización, etc. Es necesario asimismo tener en cuenta las medidas que la organización adopte para mitigar en cualquier forma la ocurrencia de algún evento de riesgo.

En este contexto, es factible relacionar los niveles de calificación con la cuantificación de un riesgo a ello se denomina análisis semi cuantitativo, por ejemplo un riesgo que tiene una probabilidad de ocurrencia de 40 en 100 casos y que genera una pérdida de 200 nuevos soles cada vez que ocurre podría considerarse como un Riesgo Alto [11]. Considerando el mismo ejemplo y conociendo que la organización ha implementado un mecanismo de control que reduce las pérdidas de 200 a 15 nuevos soles, y una ocurrencia de 12 en 100 casos, el riesgo puede adoptar un nivel de Riesgo Medio. Este ejemplo muestra una de las maneras de tratar un riesgo y ese es uno de los retos de la Administración de Riesgos.

2.1.4.- CONCEPTO DE RIESGO DE TECNOLOGIA DE INFORMACION

La definición de los riesgos de tecnología de información, está sustentado en dos pilares fundamentales, el primero de ellos enlazado a los riesgos de operación y el segundo a las definiciones internacionales de riesgo en SI.

En el primer pilar, los riesgos de tecnología de información son componentes de los riesgos de operación, entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Esta primera definición, está sustentada en la declaración de Basilea II, la misma que propone diez principios para una adecuada administración de los riesgos de operación, estos principios incluyen la adecuada estructura organizacional, la participación de la alta gerencia, la sujeción a revisión de auditoría, la generación de políticas de mitigación de riesgos y un proceso de gestión de los riesgos.

En el segundo pilar, los riesgos de tecnología de información se definen además como aquellos asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a estos sistemas, los mismos que afectan el desarrollo de las actividades del negocio contra los principios de integridad, confidencialidad y disponibilidad de la información.

Como todo componente de riesgo, los asociados a tecnología de información están inmersos dentro de aquellos eventos que generan incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.5.- GESTION INTEGRAL DE RIESGOS

Según el avance en las buenas prácticas para la administración de riesgos, este se ha ido incrementando en el alcance de su evaluación. En primer lugar, el riesgo tradicional que evaluaban las empresas financieras, se basó en el riesgo de créditos. El 15 de Julio de 1988 el Comité de Basilea publica el ACB ó Basilea I [5], el cual establecía el acuerdo de convergencia que uniforma medir la adecuación del capital en los bancos para asegurar su solvencia. Este ACB sólo tenía en cuenta el riesgo de crédito y no hacía ninguna referencia al riesgo de mercado.

En Enero de 1996 se efectuó la enmienda al ACB88 [5] que incorpora el Riesgo de Mercado con lo cual la gestión de riesgos adopta un esquema financiero, de créditos y de mercado. [7]

---

[7] Ver “Operational Risk: The Next Frontier”, RMA, (2000).
Posteriormente, a finales de la década de los noventa, Basilea II introduce novedades en el Riesgo Crediticio y además por primera vez tiene en cuenta el Riesgo de Operación que incluye los Riesgos de tecnología de información, aspecto que cada día tiene más importancia en la operatoria de los Instituciones

Financieras. A partir de esa fecha, se inicia el tratamiento integral de Riesgos y su administración da origen a la Gestión Integral de Riesgos.

La Gestión Integral de Riesgos, ha dado origen al tratamiento de los riesgos estratégicos, los riesgos legales y morales que las empresas deben considerar.

2.1.6.- SEGURIDAD DE INFORMACION

No existe una definición estricta de lo que se entiende por seguridad de información, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los procesos, su entorno y los sistemas de información. Consideraciones que van desde la protección física de las aplicaciones como componentes hardware, de su entorno, hasta la protección de la información que estos sistemas contienen o de las redes que lo comunican con el exterior.

Son muy diversos los tipos de amenazas contra los que debemos protegernos. Desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, el fraude interno, destrucción o modificación de la información.

No obstante, existen tres aspectos fundamentales que definen la seguridad de información: la confidencialidad, la integridad y la disponibilidad.

Sobre esta base, podemos definir a la seguridad de información como la adecuada interrelación de normas, procedimientos, cultura organizacional, mecanismos y recursos informáticos para garantizar los principios de confidencialidad, disponibilidad e integridad.

La seguridad de información, incluye en su análisis, un gran número de factores, por ejemplo, la British Estándar BS7799 [8] establece 10 puntos clave en el control de la seguridad de información:

- Documento de Política de Seguridad de Información.
- Asignación de Responsabilidades de Seguridad.

- Capacitación y Difusión en Seguridad de Información.
- Reporte de Incidentes de Seguridad.
- Controles Antivirus.
- Proceso de Planeación de Continuidad del Negocio.
- Control de copias Propietarias.
- Salvaguarda de los registros de la Empresa.
- Cumplimiento de la Legislación para la Protección de Datos.
- Cumplimiento de la Política de Seguridad.

2.1.7.- PLAN DE CONTINUIDAD DE NEGOCIOS

Un plan que direcciona la continuidad y el mantenimiento de todos los procesos del negocio requeridos para mantener un nivel aceptable de operación en el momento de ocurrencia de un evento de interrupción de los mismos y/o de los recursos que lo soportan.

Un plan de continuidad de negocios incluye los siguientes documentos como requerimiento mínimo de adecuación:

- Plan de Emergencias: Un mecanismo de respuesta centralizada que asegura la ejecución de las instrucciones y el control durante una interrupción operacional (Ej. Instrucciones y actividades manuales). Este plan incluye: identificación de incidentes, evaluación, escalamiento, declaración, plan de activación y desactivación inmediato y procedimientos iniciales de restauración.

---

[8] BS 7799 : http://www.peopsoft.com/Servicio_Security.htm.

- Plan de Contingencia: Un plan de ejecución y revisión constante que direcciona las acciones, personas, servicios y recursos informáticos o de comunicación disponibles para la atención de un evento de interrupción de los servicios con base en la evaluación de riesgos, disponibilidad de recursos y capacidad de respuesta.

- Plan de Recuperación: Un plan que direcciona la restauración de las aplicaciones de sistemas, software, datos e infraestructura de las mismas y procesos operativos del negocio (por ejemplo, hardware, comunicaciones, redes, servicios bancarios, etc.) después que la contingencia o desastre ha ocurrido.

2.1.8.- ORÍGENES DE LA ADMINISTRACION DE LOS RIESGOS DE TECNOLOGIA

- Requerimientos legales, regulatorios, contractuales
- Acelerados avances tecnológicos
- Incidentes de seguridad (comunicaciones divulgadas)
- Preocupación de los usuarios
- Pérdidas económicas
- Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

2.1.9.- NUEVO ACUERDO DE CAPITAL (NAC) - BASILEA II

A mediados de los años 90 y finalmente, en junio de 2004, se aprobó un Nuevo Acuerdo de Capital (Basilea II), cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria. El Comité de Basilea forma parte del Banco Internacional de Pagos (BIS) y fue creado por acuerdo de los representantes de los Bancos Centrales de los 10 países más industrializados con el propósito de formular una serie principios y estándares de supervisión bancaria, los que han sido acogidos no solo por los países miembros, sino por la mayoría de países en el mundo. Se indica que los países pertenecientes al G10, deberán de comenzar a implementar a partir del 2007 todo lo definido en Basilea II en sus versiones más simples y a partir de 2008 en sus versiones mas avanzadas.

Más allá de proponer metodologías más sensibles al riesgo para el cálculo del capital regulatorio, Basilea II plantea reglas prudenciales específicas para las instituciones de crédito, apuntando a incentivar la estabilidad del sistema financiero dando mayor importancia a los sistemas de control interno, a la administración de los bancos y a la disciplina de mercado. Es así que Basilea II se puede definir como un marco global de supervisión bancaria, basado en tres pilares: [9]

- Los Requerimientos Mínimos de Capital
- El Proceso de Examen del Supervisor
- La Disciplina de Mercado.

Cabe señalar que uno de los puntos que se desprende de los principios propuestos por el Comité de Basilea II (Nuevo Acuerdo de Capital - NAC), es que las entidades financieras deberán de establecer y asignar el capital necesario a la protección de los activos de Tecnología que pudieran generar una crisis bancaria.

En abril de 2003, la SBS decidió asumir el reto de la implementación y adecuación de lo propuesto por el comité de Basilea y estableció el Comité Especial Basilea II (CEB) [5], en el cual se encuentran representadas las diversas áreas de la Superintendencia involucradas en este proyecto.

Entre las principales labores que viene realizando este Comité se encuentran las siguientes:

---

[9] Jameson, R. “Operational Risk and Financial Institutions”, (1998).

- Diseño de la supervisión según los principios de Basilea II.
- Adecuación estructura orgánica.
- Acceso a información nivel de operación: Nueva Central de Riesgos.

- El establecimiento de procedimientos de supervisión y mecanismos de alerta.
- Evaluación cuantitativa del impacto de la implementación del NAC en el sistema financiero peruano.
- Identificación de los principales cambios en la regulación y estudio de nuevas normas.
- Diseño del marco de transparencia ajustado a Basilea II.

Como se podrá apreciar los objetivos de la emisión de los documentos (normas, resoluciones, circulares, buenas prácticas, etc.) son:

- Las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos de tecnología de información que estas enfrentan.
- Incidir en la identificación de riesgos de tecnología, de los Procesos Críticos de la entidad financiera.
- Tener un control adecuado de los Activos de TI.
- Asignar el capital necesario, para la protección de los activos, ante el posible desenlace de un riesgo.

Finalmente indicamos que en el presente trabajo, se buscará plantear una metodología adecuada, la cual deberá de englobar los diversos documentos descritos en este capitulo.

2.1.10.- INFORMACIÓN Y SISTEMA INFORMÁTICO

Entendemos por información el conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.

En cuanto a su implantación, se puede hablar de:

• Subsistema formalizado: Normas, procedimientos e información de negocio.
• Subsistema no formalizado: Flujos de información que no pasan por el sistema de información formalizado (rumores, charlas informales, llamadas telefónicas, etc.).

El sistema informático es un subconjunto del subsistema formalizado, con distinto grado de cobertura. Por otra parte, se puede ver el sistema informático como el conjunto de los recursos técnicos (máquinas y utensilios), financieros (ingresos, gastos y patrimonio) y humanos (plantilla de informáticos y personal auxiliar), cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de la empresa.

Los aspectos clave en la seguridad de información, están asociados a dos niveles:

- Aspectos de Negocio (Procesos de negocio y Organización)
- Aspectos tecnológicos (soluciones e Infraestructura)

Adicionado a esto, los riesgos fundamentales asociados con la incorrecta protección de la información como la revelación a personas no autorizadas, la inexactitud de los datos. La dificultad en el acceso a la información cuando se necesita, el fraude interno y externo, el costo financiero y social como los más importantes. Estos aspectos se relacionan con las tres características que debe cubrir un sistema de información seguro: *confidencialidad, integridad y disponibilidad*.

2.1.11.- CONFIDENCIALIDAD

Se entiende por confidencialidad el servicio o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

• El uso de técnicas de control de acceso a los sistemas [10].
• El cifrado de la información confidencial o de las comunicaciones.

2.1.12.- INTEGRIDAD

Se entiende por integridad el servicio que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Esta modificación debe ser permisible a revisiones o controles de auditoria que permitan identificar a los responsables de su modificación.

Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad:
• *Precisión accuracy,*
• *Integridad integrity,*
• *Autenticidad auntenticity.*

---

[10] Técnica : Lluvia de Ideas

El concepto de integridad asimismo, significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los Bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos.

2.1.13.- DISPONIBILIDAD

Se entiende por disponibilidad el grado en que la información está en el lugar, momento y forma en que es requerido por el usuario autorizado. Asimismo en términos de Sistema de Información cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lógicamente, la información debe estar en los formatos adecuados para los usuarios al momento de encontrarse disponible para su uso.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). [7] Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

2.1.14.- AMENAZAS A LA INFORMACIÓN

Una amenaza es cualquier elemento que afecta a los sistemas de información y a todo lo que involucra dicha información (procesos, eventos, etc.), el efecto de una amenaza es un daño, el mismo que no sólo incluye el efecto en si de la amenaza, sino también el hecho de no tomar acciones correctivas necesarias.

Una amenaza es también una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produzca una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). El análisis de riesgos identificará las amenazas que han de ser contrarrestadas. [8]

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- interrupción: Se produce cuando un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.
- Interceptación: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora.
- Modificación: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.
- Fabricación: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

2.1.15.- ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o controla, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico.

2.1.16.- ATAQUES ACTIVOS

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido, o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

1.- Suplantación de Identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.
2.- Repetición Indeterminada: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
3.- Modificación de Mensajes: Una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
4.- Degradación fraudulenta del servicio: Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

2.1.17.- OTROS ASPECTOS RELACIONADOS

Existen otros aspectos considerados en el tratamiento de los riesgos de tecnología de información y que son especialmente importantes en el entorno bancario y en el uso del comercio digital, aunque pueden asimilarse a uno de los tres aspectos fundamentales, es necesario considerarlos con especial énfasis debido a su importancia en el negocio, entre ellos tenemos: [11]

a) AUTENTICIDAD: Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

---

[11] Alguno de los principios pueden sonar muy básicos en un principio, pero probablemente se convertirán en elementos vitales al momento de la implementación.

b) IMPOSIBILIDAD DE RECHAZO (no-repudio): Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

c) CONSISTENCIA: Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.

d) AISLAMIENTO: Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él.

e) AUDITORÍA: Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo.

f) RECUPERACIÓN: En caso de emergencia o pérdida de información, deben existir los mecanismos necesarios para recuperar la información.

g) CUSTODIA Y PROPIEDAD: Es necesario tener identificado a quien custodia la información y establecer solidamente las características de propiedad y depositario de la información.

CAPITULO 3

ESTADO DEL ARTE

3. ESTADO DEL ARTE

3. 1 METODOLOGÍAS

3.1.1 METODOLOGÍA MAGERIT

La Metodología de Análisis y Gestión de Riesgos de Sistemas de Información MAGERIT, fue desarrollada por el Consejo Superior de Administración Electrónica de España, con la finalidad de administrar los sistemas de información de las entidades públicas; esta metodología fue emitida el año de 1997 y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. MAGERIT desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales.

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Objetivos de MAGERIT:

Directos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

Cabe mencionar, que el análisis de riesgos propuesto por Magerit es una aproximación metódica que permite determinar el riesgo siguiendo unos pasos (Ver Figura Nº 2)

- Determinar los activos relevantes para la Organización
- Determinar a que amenazas están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Valorar dichos activos en función del coste que supondría para la Organización recuperarse ante un problema de disponibilidad, integridad, confidencialidad o autenticidad
- Valorar las amenazas potenciales.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

Figura Nº 2: Pasos realizados por Magerit [6]

3.1.2. METODOLOGÍA OCTAVE

La Metodología OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) fue encargado por el CERT [12] al SEI o Instituto de Ingeniería de Software de la Universidad estadounidense de Carnegie Mellon. Se liberó en el segundo trimestre de 2002 y desde entonces se han producido varias revisiones. Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.

Es un método operativo, orientado a resultados: después de la primera iteración (2-3 meses) se obtiene un plan a corto plazo y un plan estratégico a largo plazo para mitigar los riesgos detectados.

Objetivos de OCTAVE:

- Especificar los elementos del riesgo organizacional y los riegos tecnológicos relativos a la estrategia y a la práctica.

- Fomentar el trabajo en equipo desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT), trabajaran juntos direccionados a las necesidades de seguridad, balanceando los tres aspectos: RIESGOS OPERATIVOS, PRACTICAS DE SEGURIDAD Y TECNOLOGIA. (*Figura Nro 3*)

---

[12] CERT (Computer Emergency Response Team): considerado como autoridad mundial para la seguridad de Internet. Fue creado por DARPA (Defense Advanced Research Projects Agency) en 1988, en respuesta a las necesidades

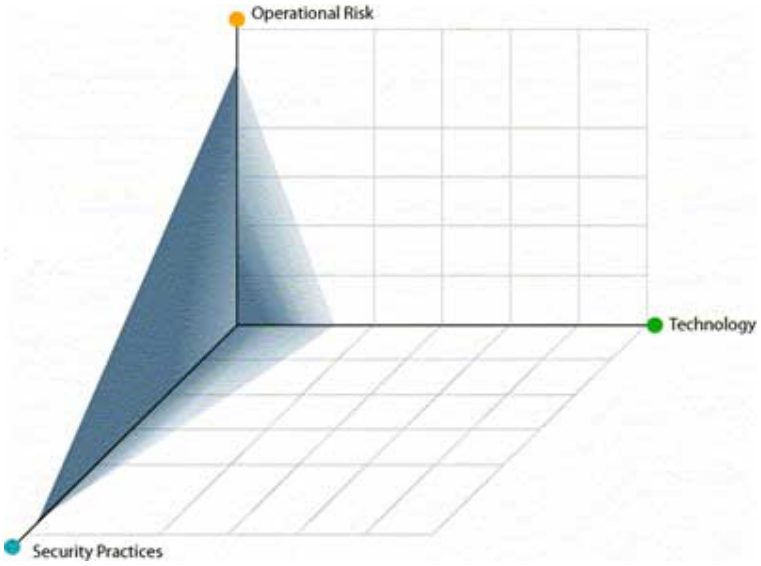


Figura Nº 3: OCTAVE está impulsado por el riesgo operativo y prácticas de seguridad [6]

- Se dirige de los servicios a los sistemas y no al revés, proponiendo un equipo de trabajo mixto entre personal encargado de la gestión de los servicios y personal técnico informático de sistemas. Está así pensado porque son las técnicas y gestoras de los servicios y proyectos las que conocen los riesgos de las entidades y de su tratamiento de la información.

- Propone una metodología muy bien detallada, con unos pasos muy claros y definidos, proporcionando el suficiente material de soporte (plantillas, ejemplos, etc.), y asumiendo todas las buenas prácticas de las normas y estándares actuales.

La aproximación de OCTAVE apunta a dos aspectos diferentes: riesgos operativos y prácticas de seguridad. La tecnología es examinada en relación a las prácticas de seguridad, permitiendo a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

3.1.3. METODOLOGÍA CRAMM

La Metodología CRAMM (CCTA Risk Analysis Management Methodology), fue desarrollada en 1985 por la Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido, que utiliza técnicas cualitativas para el análisis y gestión de riesgos, se desarrolla en tres etapas distintas, a las que se asocian una serie de cuestionarios, objetivos y guías.

- Identificación de Riesgos.
- Análisis de Riesgos.
- Evaluación de Riesgos.

Objetivos de CRAMM:

- Proveer un marco conceptual genérico para el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo.

- Especificar los elementos del proceso de administración de riesgos, sin forzar a la uniformidad en el sistema de administración del riesgo. Cabe señalar que este sistema de administración es influenciada necesariamente por las necesidades de la organización, sus objetivos particulares, sus productos y servicios, y los procesos y prácticas específicas empleadas.

3.1.4. METODOLOGÍA COSO

Esta Metodología proporciona técnicas empleadas en diversos niveles de una entidad para aplicar los principios de gestión de riesgos corporativos. Dicha metodología presenta además las técnicas empleadas para llevar a cabo la evaluación del sistema de control interno de una entidad, incluyendo un conjunto de herramientas generales, herramientas desarrolladas para una entidad de gran dimensión y un manual de referencia.

La gestión de riesgos corporativos incluye las siguientes consideraciones:

3.1.4.1 AMBIENTE INTERNO

Se describe brevemente el impacto que pueden tener los elementos del ambiente interno en el éxito o fracaso de una organización y expone algunas afirmaciones de la filosofía de gestión de riesgos, técnicas para evaluar el grado en que se halla integrada dicha filosofía en la cultura de la entidad y herramientas para fomentar una cultura de integridad y valores éticos.

El ambiente interno de una organización tiene un impacto significativo en el modo como se implanta la gestión de riesgos corporativos y en su funcionamiento continuado, constituyendo el contexto en que se aplican otros componentes de la gestión de riesgos corporativos, con un importante efecto positivo o negativo sobre ellos.

La filosofía de la gestión de riesgos de una organización es el conjunto de creencias y actitudes compartidas que caracterizan el modo en que la entidad contempla el riesgo en todas sus actuaciones, desde el desarrollo e implantación de la estrategia hasta sus actividades cotidianas, dicha filosofía queda reflejada prácticamente en todo el quehacer de la dirección al gestionar la entidad y se plasma en las declaraciones sobre políticas, las comunicaciones verbales y escritas y la toma de decisiones. Tanto si la dirección pone su énfasis en las políticas escritas, normas de conducta, indicadores de rendimiento e informes de excepción, como si prefiere operar más informalmente mediante contactos

personales con los directivos claves, lo críticamente importante es que desde ella se potencie la filosofía, no sólo con palabras, sino con acciones diarias.

Con el fin de obtener un mayor conocimiento sobre el grado de integración de la filosofía de gestión de riesgos en la cultura de la entidad, algunas empresas llevan a cabo una encuesta sobre la cultura de riesgos, midiendo la presencia y fortaleza de los atributos relacionados con ellos.

Algunas empresas encuestan periódicamente, por ejemplo cada año, a toda su plantilla y con mayor frecuencia a una muestra suya representativa. Algunas empresas distribuyen los resultados de estas encuestas trimestralmente, para proporcionar un mayor conocimiento del pulso y tendencias continuas de la entidad, lo que resulta especialmente útil en tiempos de cambio. Los resultados de dichas encuestas proporcionan indicadores de las áreas de fortalezas y debilidades en la cultura de una organización.

Nº	Pregunta	Atributo	Calificación media		Dsv. Est.	Cant.	MD	D	N	A	MA
1	Los líderes de mi unidad dan un ejemplo positivo de conducta ética	Liderazgo y estrategia	1,42	Fuerte	0,71	186	1	3	9	77	96
2	Comprendo la misión y estrategia general de la entidad.	Liderazgo y estrategia	1,05	Buena	0,69	186	0	7	18	119	42
3	Se emprenden acciones disciplinarias contra aquellos que muestran una conducta profesional impropia	Responsabilidad y motivación	0,21	Acción necesaria	1,20	175	11	55	18	68	23
4	La rotación del personal no ha afectado significativamente a nuestra capacidad de alcanzar los objetivos.	Personas y comunicación	0,81	Precaución	0,88	145	4	3	39	69	30
5	Los líderes de mi unidad de negocio son receptivos a todas las comunicaciones acerca del riesgo, incluyendo las malas noticias.	Gestión de riesgos e infraestructura	0,99	Buena	0,85	183	2	13	16	106	46

En este ejemplo, cada pregunta se califica usando una escala que va de -2 a +2:
-2 Muy en Desacuerdo (MD)
-1 Desacuerdo (D)
0 Neutral (N)
+1 De acuerdo (A)
+2 Muy de acuerdo (MA)
La evaluación, presentada en un código de colores, está basada en la media de las calificaciones. La desviación estándar proporciona información adicional, al ser una medida del grado de consenso de las respuestas en torno a la cuestión planteada. Así, cuanto menor sea la desviación estándar, mayor será el grado de acuerdo entre las respuestas a cada tema.

Figura Nº 4: Encuesta sobre la cultura de riesgos [3]

La *Figura Nº 4* muestra parte de una ilustración que indica cómo se presentan e interpretan los resultados de una encuesta sobre la cultura de riesgos. Estos resultados ayudan a la entidad a identificar atributos que deben reforzarse de entrada y a asegurar que el ámbito interno sea eficaz.

La eficacia de la gestión de riesgos corporativos no debe sobreponerse a la integridad y los valores éticos de las personas que crean, administran y controlan las actividades de la organización.

La integridad y el compromiso con los valores éticos son propios del individuo. Los juicios de valor, la actitud y el estilo se basan en experiencias personales. No hay ningún puesto más importante para influir sobre la integridad y valores éticos que el de consejero delegado y la alta dirección, ya que establecen el talante al nivel superior y afectan a la conducta del resto del personal de la organización. Un talante adecuado al nivel más alto contribuye a que:

- Los miembros de la entidad hagan lo correcto, tanto desde el punto de vista legal como moral.

- Se cree una cultura de apoyo al cumplimiento, comprometida con la gestión de riesgos corporativos.

- No se navegue por zonas “grises” en las que no existen normas o pautas específicas de cumplimiento.

- Se fomente una voluntad de buscar ayuda e informar de los problemas antes de que éstos no tengan solución.

Las organizaciones apoyan una cultura de valores éticos e integridad mediante la comunicación de documentos tales como una declaración de valores fundamentales que establezca los principios y prioridades de la entidad y un código de conducta. Este código proporciona una conexión entre la misión/visión y las políticas y procedimientos operativos. Sin ser una guía exhaustiva de conducta, ni un documento legal que perfile en gran detalle los protocolos clave de la organización, un código de conducta es una declaración proactiva de las posiciones de la entidad frente a las cuestiones éticas y de cumplimiento. Estos códigos también pueden ser útiles como guías de fácil utilización acerca de las políticas relativas a la conducta de los empleados y de la propia organización.

Para realizar el seguimiento del grado de cumplimiento de las normas establecidas por parte de los empleados, algunas empresas utilizan periódicamente grupos de debate dentro de la plantilla. Esta información, procesada a menudo con la ayuda de tecnología, se emplea para “validar” los valores fundamentales. También puede emplearse la tecnología para habilitar el

intercambio y actualización de información, así como para realizar el seguimiento del cumplimiento por parte de los empleados del código de conducta y de las políticas, estándares y procedimientos relacionados.

Se presentan algunos ejemplos de cómo las organizaciones emplean la tecnología para fomentar la cultura deseada.

- Existencia de un enlace directo desde la página de inicio en Internet (o en la Intranet) de la organización a la declaración de valores y el código de conducta, facilitando su uso y enviando un mensaje acerca de su importancia.

- Códigos e información relacionada con ellos disponibles electrónicamente, proporcionando así un fácil acceso y eliminando la necesidad de copias impresas.

- Confirmación de que la plantilla ha recibido la información.

- Celebración de cursos presenciales y formación “on line”.

- Referencia automática al código o pautas empleadas durante la realización de tareas.

- Recordatorios automáticos a la plantilla acerca de las acciones requeridas.

- Notificación al supervisor inmediato del empleado e incluso a niveles superiores en el caso de que no se adopten las acciones requeridas de manera oportuna.

- Método para obtener el certificado de cumplimiento de las normas.

- Existencia de rastros de las actividades.

3.1.4.2 ESTABLECIMIENTO DE OBJETIVOS

Permite ilustrar el vínculo entre la misión de una entidad y los objetivos estratégicos, así como con otros objetivos relacionados, y la alineación de estos dos tipos de objetivos con el nivel de riesgo aceptado y las tolerancias al riesgo.

Al considerar las posibles formas alternativas de alcanzar los objetivos estratégicos, la dirección identifica los riesgos asociados a una gama amplia de elecciones estratégicas y considera sus implicaciones. Se pueden aplicar diferentes técnicas de identificación y evaluación de los riesgos, que se expondrán en capítulos posteriores, durante el proceso de establecimiento de la estrategia.

El riesgo aceptado puede expresarse en términos cualitativos o cuantitativos.

Algunas organizaciones expresan el riesgo aceptado en términos de un "mapa de riesgo", como se ilustra en la *Figura Nº 5*. En esta figura, cualquier riesgo residual significativo en la zona amarilla excede del riesgo aceptado por la empresa, lo que requiere de la dirección la puesta en marcha de acciones para reducir su probabilidad y/o impacto y situarlo dentro del riesgo aceptado por la entidad.

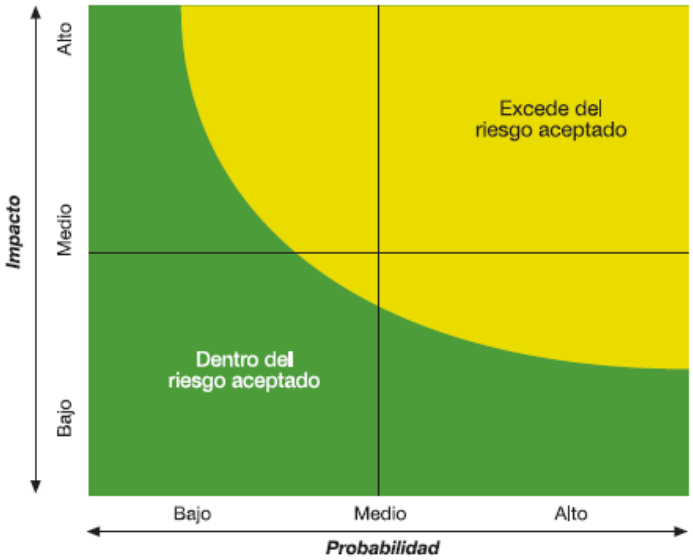


Figura Nº 5: Formación del riesgo aceptado [3]

Las tolerancias al riesgo son los niveles aceptables de desviación relativa a la consecución de objetivos, operar dentro de las tolerancias al riesgo proporciona

a la dirección una mayor confianza en que la entidad permanece dentro de su riesgo aceptado, que, a su vez, proporciona una seguridad más elevada de que la entidad alcanzará sus objetivos.

La tolerancia al riesgo se establece en ocasiones al nivel de entidad y se asigna a lo largo de las unidades de negocio.

3.1.4.3 IDENTIFICACIÓN DE EVENTOS

La dirección identifica los eventos potenciales que, de ocurrir, afectarán a la entidad y determina si representan oportunidades o si pueden afectar negativamente a la capacidad de la empresa para implantar la estrategia y lograr los objetivos con éxito. Los eventos con impacto negativo representan riesgos, que exigen la evaluación y respuesta de la dirección. Los eventos con impacto positivo representan oportunidades, que la dirección reconduce hacia la estrategia y el proceso de fijación de objetivos. Cuando identifica los eventos, la dirección contempla una serie de factores internos y externos que pueden dar lugar a riesgos y oportunidades, en el contexto del ámbito global de la organización [15].

En algunas circunstancias, la identificación de eventos relacionados con un objetivo específico es razonablemente sencilla, En otras circunstancias, la identificación de riesgos no resulta inmediatamente evidente, por lo que se emplean diversas técnicas, como se comenta en los siguientes párrafos.

La metodología de identificación de eventos en una entidad puede comprender una combinación de técnicas y herramientas de apoyo. Las técnicas de identificación de eventos se basan tanto en el pasado como en el futuro.

La dirección utiliza diversas técnicas para identificar posibles acontecimientos que afecten al logro de los objetivos. Estas técnicas se emplean en la identificación de riesgos y oportunidades. Por ejemplo, al implantar un nuevo proceso de negocio, rediseñarlo o evaluarlo. Pueden emplearse en conexión con la planificación estratégica o de unidad de negocio o al considerar nuevas iniciativas o un cambio en la organización.

Las direcciones utilizan listados de eventos posibles comunes a un sector o área funcional específica. Estos listados se elaboran por el personal de la entidad o bien son listas externas genéricas y se utilizan, por ejemplo, con relación a un proyecto, proceso o actividad determinada, pudiendo resultar útiles a la hora de asegurar una visión coherente con otras actividades similares de la organización. Cuando se trata de listados generados externamente, el inventario se revisa y somete a mejoras, adaptando su contenido a las circunstancias de la entidad, para presentar una mejor relación con los riesgos de la organización y ser consecuentes con el lenguaje común de gestión de riesgos corporativos de la entidad.

Los talleres o grupos de trabajo dirigidos para identificar eventos reúnen habitualmente a personal de muy diversas funciones o niveles, con el propósito de aprovechar el conocimiento colectivo del grupo y desarrollar una lista de acontecimientos relacionados, por ejemplo, con los objetivos estratégicos de una unidad de negocio o de procesos de la empresa. Los resultados de estos talleres dependen habitualmente de la profundidad y amplitud de la información que aportan los participantes.

Algunas organizaciones, en conexión con el establecimiento de objetivos, ponen en marcha un taller en que participa la alta dirección, a fin de identificar eventos que podrían afectar al logro de objetivos corporativos estratégicos.

Las entrevistas se desarrollan habitualmente entre entrevistador y entrevistado o, en ocasiones, con dos entrevistadores para cada persona entrevistada, en cuyo caso el entrevistador está acompañado por un compañero que toma notas. Su propósito es averiguar los puntos de vista y conocimientos sinceros del entrevistado en relación con los acontecimientos pasados y los posibles acontecimientos futuros.

A continuación se ilustra el orden del día de una entrevista centrada en los objetivos de una unidad de negocio. [9]

Los cuestionarios abordan una amplia gama de cuestiones que los participantes deben considerar, centrando su reflexión en los factores internos y externos que han dado, o pueden dar lugar, a eventos. Las preguntas pueden ser abiertas o cerradas, según sea el objetivo de la encuesta. Pueden dirigirse a un individuo o a varios o bien pueden emplearse en conexión con una encuesta de base más amplia, ya sea dentro de una organización o esté dirigida a clientes, proveedores u otros terceros.

El análisis del flujo de procesos implica normalmente la representación esquemática de un proceso, con el objetivo de comprender las interrelaciones entre las entradas, tareas, salidas y responsabilidades de sus componentes. Una vez realizado este esquema, los acontecimientos pueden ser identificados y considerados frente a los objetivos del proceso. Al igual que con otras técnicas de identificación de eventos, el análisis del flujo de procesos puede utilizarse en una visión de la organización a nivel global o a un nivel de detalle.

Los principales indicadores de eventos, a menudo denominados principales indicadores de riesgo, son mediciones cualitativas o cuantitativas que proporcionan un mayor conocimiento de los riesgos potenciales, tales como el precio del combustible, la rotación de las cuentas de valores de los inversores y el tráfico de un sitio de Internet. Para resultar útiles, los principales indicadores de riesgo deben estar disponibles para la dirección de manera oportuna, lo que, dependiendo de la información, puede implicar una frecuencia diaria, semanal, mensual o en tiempo real.

Los indicadores de alarma se centran habitualmente en operaciones diarias y se emiten, sobre la base de excepciones, cuando se sobrepasa un umbral preestablecido. Las empresas poseen a menudo indicadores de alarma establecidos en unidades de negocio o departamentos. Estos indicadores, para ser eficaces, deben establecer el momento en que deberá informarse a los directivos partiendo del tiempo necesario para poner en marcha una acción.

El seguimiento de la información relevante puede ayudar a una organización a identificar acontecimientos pasados con un impacto negativo y a cuantificar las

pérdidas asociadas, a fin de predecir futuros sucesos. La información de eventos se emplea habitualmente en la evaluación de riesgos –basándose en la propia experiencia acerca de su probabilidad e impacto pero también puede ser útil para identificar eventos mediante la creación de una base de discusión basada en hechos, la institucionalización del conocimiento (que resulta particularmente útil en situaciones de alta rotación del personal) y servir como fuente para comprender las interdependencias entre eventos con pérdidas asociadas y desarrollar modelos predictivos y causales.

Existen bases de datos externas, desarrolladas y mantenidas por proveedores de servicios y disponibles mediante suscripción, que hacen referencia a eventos con pérdidas asociadas. En algunos sectores, como el de banca, se han formado consorcios para compartir información interna.

Las bases de datos de eventos con pérdidas asociadas contienen información sobre aquellos acontecimientos reales que cumplen criterios específicos. La información de bases de datos externas puede resultar útil para complementar la información generada internamente para estimar la probabilidad e impacto de eventos futuros, en particular para acontecimientos posibles con una baja probabilidad (que es altamente improbable que la empresa haya experimentado en el pasado), pero con un alto impacto. Por ejemplo, una de estas bases de datos contiene información de eventos con pérdidas asociadas para varios sectores, donde se declararon perdidas operativas superiores a un millón de dólares.

Algunas empresas realizan el seguimiento de una gama de datos externos. Por ejemplo, las grandes empresas realizan el seguimiento de varios de los principales indicadores económicos, con el fin de identificar movimientos que apunten a un cambio en la demanda de sus productos y servicios. De manera similar, las instituciones financieras realizan el seguimiento de cambios en las políticas mundiales para identificar principales indicadores que apunten a una modificación en las estrategias futuras de inversión, así como acontecimientos que exijan una modificación inmediata de las carteras de inversión.

Las técnicas anteriormente presentadas se aplican, normalmente, en circunstancias particulares que se presentan con una frecuencia variable a lo largo del tiempo. También se identifican eventos posibles de manera continua en conexión con las actividades diarias propias del negocio.

Bajo determinadas circunstancias, son muchos los eventos que pueden tener impacto sobre el logro de un objetivo. Para conseguir una mejor visión y comprensión acerca de sus interrelaciones, algunas empresas utilizan diagramas de eventos en árbol, también conocidos como diagramas de espina de pescado. Un diagrama de este tipo proporciona un medio para identificar y representar de manera gráfica la incertidumbre, centrándose por lo general en un objetivo y en el modo en que múltiples eventos afectan a su logro.

Mediante la agrupación de posibles eventos de características similares, la dirección puede determinar con más precisión las oportunidades y los riesgos.

Algunas entidades clasifican los eventos posibles, para ayudar a asegurar que los esfuerzos para su identificación sean completos. Esto también puede ayudar a desarrollar posteriormente una perspectiva de cartera.

3.1.4.4 EVALUACIÓN DE RIESGOS

La evaluación de riesgos permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva probabilidad e impacto y normalmente usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.

El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente. Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aprobación de transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

La metodología de evaluación de riesgos de una entidad consiste en una combinación de técnicas cualitativas y cuantitativas. La dirección aplica a menudo técnicas cualitativas cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficaz por su coste. Las técnicas cuantitativas típicamente aportan más precisión y se usan en actividades más complejas y sofisticadas, para complementar las técnicas cualitativas.

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se debe aplicar alguna forma de medición.

Técnicas cualitativas

Si bien algunas evaluaciones cualitativas de riesgos se establecen en términos subjetivos y otras en términos objetivos, la calidad de estas evaluaciones depende principalmente del conocimiento y juicio de las personas implicadas, su comprensión de los acontecimientos posibles y del contexto y dinámica que los rodea.

Técnicas cuantitativas

Las técnicas cuantitativas pueden utilizarse cuando existe la suficiente información para estimar la probabilidad o el impacto del riesgo empleando mediciones de intervalo o de razón. Los métodos cuantitativos incluyen técnicas probabilísticas, no probabilísticas y de benchmarking..

Algunas organizaciones, en particular las instituciones financieras, estiman el capital económico. Algunas empresas utilizan este término para referirse a la cantidad de capital requerida para protegerse contra riesgos financieros. Otras la utilizan de manera diferente, como una medida del capital necesario para hacer funcionar el negocio de la manera planificada. La dirección lo puede utilizar para establecer estrategias, asignar recursos y medir el rendimiento.

Las organizaciones utilizan diversos métodos para presentar las evaluaciones de riesgos. La presentación de una manera clara y concisa resulta especialmente importante en el caso de la evaluación cualitativa, dado que en este caso los riesgos no se resumen en una cifra o intervalo numérico, como sucede en las técnicas cuantitativas. Algunas técnicas incluyen mapas de riesgo y representaciones numéricas.

Un mapa de riesgo es una representación gráfica de la probabilidad e impacto de uno o más riesgos. Puede adoptar la forma de mapas de calor o diagramas de proceso que trazan estimaciones cuantitativas y cualitativas de la probabilidad e impacto del riesgo. Los riesgos se representan de manera que los más significativos (mayor probabilidad y/o impacto) resalten, diferenciándolos de los menos significativos (menor probabilidad y/o impacto). Dependiendo del nivel de detalle y de la profundidad del análisis, los mapas de riesgo pueden presentar la

probabilidad y/o el impacto general esperado o bien incorporar un elemento de variabilidad de dicha probabilidad e impacto. Los siguientes ejemplos de mapas de riesgo representan la evaluación de riesgos relativos al objetivo de conservar a empleados de alto rendimiento.

Estos mismos riesgos pueden representarse en un mapa de riesgo matricial, donde la probabilidad se sitúa en el eje horizontal y el impacto en el vertical.

3.1.4.5 RESPUESTA A LOS RIESGOS

Una vez evaluados los riesgos relevantes, la dirección determina cómo responder a ellos. Las respuestas pueden ser las de evitar, reducir, compartir y aceptar el riesgo. Al considerar su respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costes y beneficios, y selecciona aquella que sitúe el riesgo residual dentro de las tolerancias al riesgo establecidas. La dirección identifica cualquier oportunidad que pueda existir y asume una perspectiva del riesgo globalmente para la entidad o bien una perspectiva de la cartera de riesgos, determinando si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

Para los riesgos significativos, una entidad considera típicamente las respuestas posibles dentro de una gama de opciones de respuesta.

A continuación se presentan ejemplos de respuesta al riesgo en las categorías correspondientes: Evitar, distribuir, mitigar y aceptar dicho riesgo.

Evitar

- Prescindir de una unidad de negocio, línea de producto o segmento geográfico.
- Decidir no emprender nuevas iniciativas/actividades

Compartir

- Adoptar seguros contra pérdidas inesperadas significativas.
- Entrar en una sociedad de capita riesgo/sociedad compartida.
- Establecer acuerdos con otras empresas.
- Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo.
- Externalizar procesos de negocio.
- Distribuir el riesgo mediante acuerdos contractuales con clientes, proveedores u otros socios del negocio.

Reducir

- Diversificar las ofertas de productos.
- Establecer límites operativos.
- Establecer procesos de negocio eficaces.
- Aumentar la implicación de la dirección en la toma de decisiones y el seguimiento.
- Reequilibrar la cartera de activos para reducir el índice de riesgo con respecto a determinados tipos de pérdidas.
- Reasignar el capital entre las unidades operativas.

Aceptar

- Provisionar las posibles pérdidas.
- Confiar en las compensaciones naturales existentes dentro de una cartera.
- Aceptar el riesgo si se adapta a las tolerancias al riesgo existentes.

Una vez completadas las acciones de respuesta al riesgo, la dirección posee una visión de los riesgos y respuestas individuales, así como de su alineación con las tolerancias asociadas.

Al igual que en la evaluación del riesgo inherente, el riesgo residual puede ser valorado de manera cualitativa o cuantitativa. En términos generales, se utilizan las mismas mediciones en las evaluaciones del riesgo inherente y el riesgo residual. Para determinados riesgos, la dirección puede confiar en múltiples

técnicas para reducir el riesgo residual general hasta situarlo dentro de las tolerancias al riesgo.

Prácticamente todas las respuestas al riesgo implican algún tipo de coste directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el coste inicial del diseño e implantación de una respuesta (procesos, personal y tecnología), así como el coste de mantener la respuesta de manera continua. Los costes y beneficios asociados pueden medirse cuantitativa o cualitativamente, empleando normalmente una unidad de medida coherente con la empleada para establecer el objetivo y las tolerancias al riesgo relacionadas.

3.1.4.6 ACTIVIDADES DE CONTROL

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos. Las actividades de control tienen lugar a través de la organización, a todos los niveles y en todas las funciones. Incluyen una gama de actividades –tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.

Después de haber seleccionado las respuestas al riesgo, la dirección identifica las actividades de control necesarias para ayudar a asegurar que las respuestas a los riesgos se lleven a cabo adecuada y oportunamente.

Si bien las actividades de control se establecen, por norma general, para asegurar que se llevan a cabo de manera adecuada la respuesta a los riesgos, en el caso de ciertos objetivos las propias actividades de control constituyen la respuesta al riesgo.

Esto sucede con frecuencia en situaciones de riesgos relativos a objetivos de control de gestión.

3.1.4.7 INFORMACIÓN Y COMUNICACIÓN

La información pertinente se identifica, capta y comunica de una forma y en un marco de tiempo que permiten a las personas llevar a cabo sus responsabilidades Los sistemas de información usan datos generados internamente y otras entradas de fuentes externas y sus salidas informativas facilitan la gestión de riesgos y la toma de decisiones informadas relativas a los objetivos. También existe una comunicación eficaz fluyendo en todas direcciones dentro de la organización. Todo el personal recibe un mensaje claro desde la alta dirección de que deben considerar seriamente las responsabilidades de gestión de los riesgos corporativos. Las personas entienden su papel en dicha gestión y cómo las actividades individuales se relacionan con el trabajo de los demás. Asimismo, deben tener unos medios para comunicar hacia arriba la información significativa. También debe haber una comunicación eficaz con terceros, tales como los clientes, proveedores, reguladores y accionistas.
La información se necesita a todos los niveles de la organización para identificar, evaluar y responder a los riesgos y por otra parte dirigir la entidad y conseguir sus objetivos.

La información, tanto si procede de fuentes externas como internas, se recopila y analiza para establecer la estrategia y los objetivos, identificar eventos, analizar riesgos, determinar respuestas a ellos y, en general, llevar a cabo la gestión de riesgos corporativos y otras actividades de gestión.

El diseño de una arquitectura de sistemas de información y la adquisición de la tecnología son aspectos importantes de la estrategia de una entidad y las decisiones respecto a la tecnología pueden resultar críticas para lograr los objetivos. La tecnología juega un papel crítico al permitir el flujo de información en una organización, incluyendo la información directamente relevante para la gestión de riesgos corporativos.

La selección de tecnologías específicas para apoyar esta gestión es habitualmente reflejo de:

- La manera de abordar la gestión de riesgos corporativos por parte de la empresa y su grado de sofisticación.

- Los tipos de acontecimientos que afectan a la organización.

- La arquitectura informática general de la entidad.

- El grado de centralización de la tecnología de apoyo.

En determinadas organizaciones, la información es gestionada de manera independiente por cada unidad o función, mientras que otras poseen sistemas integrados.

Muchas organizaciones poseen infraestructuras informáticas de elevada complejidad, desarrolladas a lo largo del tiempo para apoyar a los objetivos operativos, de control de gestión y cumplimiento. En muchos casos, la información generada por estos sistemas en el curso normal del negocio está integrada en el proceso de gestión de riesgos corporativos

Los avances en la recogida, procesamiento y almacenamiento de datos han dado como resultado un crecimiento exponencial del volumen de datos. Con más datos disponibles a menudo en tiempo real para más gente en una organización, el reto es evitar la “sobrecarga de información”, asegurando el flujo de la información adecuada, en la forma adecuada, al nivel de detalle adecuado, a las personas adecuadas y en el momento adecuado.

Muchas organizaciones han establecido un enfoque estructurado de la gestión de la información, lo que permite a la dirección identificar el valor de ésta, clasificarla en categorías por su importancia y desarrollar procesos eficaces y adecuadas herramientas y métodos para la recogida, almacenamiento y distribución de los datos.

Disponer de la información adecuada en el momento y lugar adecuados resulta esencial para llevar a cabo la gestión de riesgos corporativos.

Los informes del tipo “cuadro de mando” son utilizados por las organizaciones para presentar información necesaria para la gestión de riesgos corporativos. Estos informes permiten a la dirección determinar con rapidez en qué medida se encuentra alineado el perfil de riesgo de la entidad con las tolerancias al riesgo. Si no están en línea, lo que sugiere que las respuestas al riesgo o los controles existentes no funcionan de la manera esperada, la dirección puede emprender acciones correctoras.

La dirección proporciona comunicaciones específicas y orientadas que se dirigen a las expectativas de comportamiento y las responsabilidades del personal. Esto incluye una exposición clara de la filosofía y enfoque de la gestión de riesgos corporativos de la entidad y una delegación clara de autoridad. La comunicación sobre procesos y procedimientos debería alinearse con la cultura deseada y reforzarla. La comunicación resulta clave para crear el entorno “adecuado” y para apoyar al resto de componentes de la gestión de riesgos corporativos. Por ejemplo, las comunicaciones descendentes sobre la filosofía de la empresa y lo que se espera del personal de la organización, junto con el necesario flujo de información ascendente, ayudan a introducir la filosofía de gestión de riesgos en la cultura de una entidad. De manera similar, la dirección refuerza o modifica la cultura de una organización con sus palabras y sus acciones diarias.

3.1.4.8 SUPERVISIÓN

La gestión de riesgos corporativos se supervisa - revisando la presencia y funcionamiento de sus componentes a lo largo del tiempo, lo que se lleva a cabo mediante actividades permanentes de supervisión, evaluaciones independientes o una combinación de ambas técnicas. Durante el transcurso normal de las actividades de gestión, tiene lugar una supervisión permanente. El alcance y frecuencia de las evaluaciones independientes dependerá fundamentalmente de la evaluación de riesgos y la eficacia de los procedimientos de supervisión permanente. Las deficiencias en la gestión de riesgos corporativos se comunican de forma ascendente, trasladando los temas más importantes a la alta dirección y al consejo de administración.

Diferentes actividades llevadas a cabo en el curso normal de la gestión de un negocio pueden servir para realizar la supervisión de la eficacia de los componentes de la gestión de riesgos corporativos. Estas actividades incluyen la revisión diaria de información de las gestiones normales del negocio, tales como:

- La dirección revisa informes de indicadores claves de actividad del negocio, tales como datos resumidos de nuevas ventas o sobre la posición de liquidez e información sobre la cartera de pedidos atrasados, márgenes brutos y otras estadísticas claves financieras y operativas.
- La dirección operativa compara la producción, inventario, medidas de calidad, ventas y otra información obtenida en el curso de las actividades diarias con información generada en el sistema, así como con el presupuesto y la planificación.
- La dirección revisa el rendimiento, comparándolo con los límites establecidos para los índices de riesgo, como es el caso de tasas de error aceptables, artículos en tránsito, partidas de conciliación, balances de riesgo en divisa extranjera o índice de riesgo equivalente.
- La dirección revisa transacciones comunicadas a través de indicadores de alerta.
- La dirección revisa indicadores clave de rendimiento, tales como tendencias en la dirección y magnitud de los riesgos, estado de las iniciativas estratégicas y tácticas, tendencias de las variaciones en los resultados reales con respecto al presupuesto o a periodos anteriores e indicadores de acontecimientos, como se describe en el capítulo de Identificación de eventos.

Aunque los procedimientos de seguimiento permanente normalmente proporcionan una retroalimentación importante sobre la eficacia de otros componentes de la gestión de riesgos corporativos, puede resultar provechoso echar un nuevo vistazo de vez en cuando, centrándose directamente sobre la eficacia de dicha gestión. Habitualmente, las evaluaciones independientes de la gestión de riesgos corporativos se llevan a cabo periódicamente. En algunos

casos, son originadas por un cambio en la estrategia, procesos clave o estructura de la entidad. Las evaluaciones independientes son llevadas a cabo por la dirección, el departamento de Auditoría Interna, especialistas externos o por una alguna combinación de estas funciones. Las evaluaciones independientes tienen a veces un alcance amplio, incluyendo toda la entidad y todos los componentes de gestión de riesgos corporativos. En otros casos, la evaluación se limita a una unidad de negocio, proceso o departamento específico, abordando otras áreas del negocio más adelante.

El Departamento de Auditoría interna proporciona una evaluación de los riesgos y actividades de control de una unidad de negocio, proceso o departamento. Estas evaluaciones proveen de una perspectiva objetiva sobre cualquiera de los componentes de la gestión de riesgos corporativos o sobre todos ellos, desde el ámbito interno de la empresa hasta la supervisión. En algunos casos, se presta especial atención a la identificación de riesgos, el análisis de probabilidad e impacto, la respuesta al riesgo, las actividades de control y la información y comunicación. La Auditoría interna, basada en el conocimiento del negocio, puede estar en posición de considerar el modo en que las nuevas iniciativas y circunstancias de la empresa podrían afectar a la aplicación de la gestión de riesgos corporativos, lo que podría tener en cuenta en su revisión y comprobación de la información relevante. Hay más información disponible en los consejos para la práctica profesional de la auditoría interna publicados por el Institute of Internal Auditors, que establecen pautas para la evaluación y generación de informes sobre la eficacia de la gestión de riesgos.

La evaluación de la gestión de riesgos corporativos constituye un proceso en sí misma. Aunque los enfoques o técnicas varían, hay que aportar al proceso una disciplina, con ciertos fundamentos inherentes a ella. Un proceso metódico proporciona una base sólida para una evaluación. Se utilizan los más diversos enfoques y técnicas, en general dependiendo de las circunstancias de la empresa y la naturaleza y alcance de la evaluación a realizar.

El nivel de documentación de la gestión de riesgos corporativos de una entidad varía según su dimensión, complejidad y factores similares. El nivel deseado de

documentación de la gestión de riesgos corporativos varía por empresa, a menudo en función del tamaño, complejidad y estilo de gestión. Además de la amplitud y profundidad de la documentación, las consideraciones al respecto incluyen si estará en soporte papel o electrónico, si estará centralizada o distribuida y cuáles son los medios de acceso para actualización y revisión.

Al evaluar la gestión de riesgos corporativos, se revisa la documentación existente de los procesos y otras actividades e, incluso, puede crearse dicha documentación, para permitir al equipo de evaluación comprender fácilmente los riesgos de la unidad, proceso o departamento y las respuestas a ellos.

Dicha documentación puede constituir la base para el desarrollo de procesos de revisión que incluyan pruebas para determinar si los procesos, junto con las políticas y procedimientos relacionados que se hayan establecido, son adecuados para enfrentarse a los riesgos de la entidad y si son respetados.

Todas las deficiencias identificadas de gestión de riesgos corporativos que afectan a la capacidad de la entidad para desarrollar e implantar su estrategia y establecer y alcanzar sus objetivos deberían comunicarse a quienes se encuentran en posición de tomar las medidas necesarias.

3.2 EVALUACIÓN DE METODOLOGÍAS

Para la presente mostramos un cuadro comparativo de los diversos temas que abarca cada metodología:

	METODOLOGIA MAGERIT	METODOLOGIA OCTAVE	METODOLOGIA CRAMM	METODOLOGIA COSO
Objetivos	Proporciona realizar una evaluación de riesgos de TI, en toda la organización que esta siendo evaluada.	Proporciona realizar una evaluación basada en Procesos o en Áreas Funcionales / Operativas de la Entidad Financiera. Cabe señalar que uno de los puntos de esta metodología, es la identificación del nivel de criticidad de los procesos de la entidad financiera evaluada.	Es un conglomerado de buenas prácticas que se debería de seguir para la gestión adecuada de los riesgos.	Proporcionar una evaluación de riesgos, a nivel corporativo haciendo participe a todas las áreas involucradas.
Estructura	La clasificación de eventos de riesgo a propuesta, es la siguiente: Servicios, Datos / información, Aplicaciones (Software), Equipos informáticos (Software), Redes de Comunicación, Soporte de Información, Equipamiento	Se encuentra basada en la NTP ISO 17799 y otras categorías que se creyó necesario ingresar (Documentos, Edificios y Equipamiento, Equipamiento Informático, Insumos, Recursos Humanos, Servicios, Software e	Se encuentra orientado exclusivamente a la gestión de riesgos que comprende la identificación, análisis, evaluación, tratamiento y monitoreo continuo del riesgo.	Con orientación a la gestión de riesgos en todas las etapas de evaluación hasta el informe a los entes reguladores.

	Auxiliar, Instalaciones y Personal.	Imagen y Reputación).		
Manejo del Riesgo	Indica que se debe de realizar las diversas evaluaciones para la identificación de los riesgos, tomando en cuenta la dependencia entre áreas.	Se encuentra orientada a la evaluación de Riesgos de TI, utilizando la identificación de los posibles riesgos inmersos en cada uno de los activos.	Propone realizar una evaluación de riesgos, en toda la organización que esta siendo evaluada.	Se encuentra orientada a la evaluación de Riesgos de TI, utilizando la identificación por procesos en cada una del a áreas evaluadas.
Metodología adoptada	No existe una técnica o metodología definida para la identificación de riesgos, MAGERIT en este punto nos proporciona una lista de buenas prácticas, las cuales se encuentran basadas en Preguntas.	Se utiliza la Metodología de la Elipses (identificación de riesgos en base a procesos).	Esta metodología ya tiene definido, un estándar de los formatos que se utilizarán, a lo largo de las fases de la evaluación de riesgos.	Permite integrar el método de evaluación del riesgo adoptado con el contenido del marco establecido para el control interno.
Calificación del Impacto	La calificación del impacto de los riesgos, es en base a la asignación de un valor entero tomado de la escala estándar [0 - 10].	La calificación del valor del impacto de los riesgos, se realiza en base a la combinación de los valores característicos de seguridad (confidencialidad, integridad y disponibilidad).	La calificación del valor del impacto de los riesgos, se realiza durante la evaluación de riesgos, solo toman en cuenta los riesgos mayores aceptables (de	La calificación del valor del impacto de los riesgos, se realiza en base a medidas cualitativas y cuantitativas que representa para la institución la

			mayor impacto), excluyendo a los riesgos menores (de menor impacto).	materialización de los mismos.
Identificación de Variables.	En esta metodología MAGERIT, participa activamente la variable "Amenaza", para la cual se utilizan dimensiones de valoración basados en la disponibilidad, integridad, entre otros.	La asignación de la variable Frecuencia, es obtenida en base a la valorización de la amenaza.	La asignación de la variable Frecuencia, es obtenida en base a la valorización de los riesgos inmersos para cada evento identificado.	Interviene directamente las variables frecuencia e impacto, para el registro del riesgo potencial. El control establecido se pondera para conseguir los riesgos residuales.
Base de Datos de Riesgos.	No cuenta con Bases de Datos de Riesgos, Amenazas Vulnerabilidad y Controles	Cuenta con Bases de Datos de Riesgos, Amenazas Vulnerabilidad y Controles, las cuales fueron obtenidas según lo establecido por la herramienta COBIT y la Norma ISO 17799, así mismo estas bases de datos son alimentadas en base a la información proporcionada por los analistas (experiencia).	No cuenta con Bases de Datos de Riesgos, Amenazas Vulnerabilidad y Controles.	Permite elaborar la construcción de Base de Datos histórico de eventos de Riesgo, necesarios para la conciliación del Nuevo acuerdo de Capital.

Tipos de Análisis	Los tipos de análisis propuestos por este estándar son: cualitativo, semi cuantitativo, cuantitativo y análisis de sensibilidad.	Esta metodología realiza un análisis cuantitativo (Valor monetario, valores asignados en base parámetros, diversas operaciones matemáticas, entre otros).	Los tipos de análisis propuestos por este estándar son: cualitativo únicamente.	Los tipos de análisis propuestos son: cualitativo y cuantitativo, pudiendo integrar ambas durante la evaluación de eventos.

La tabla a continuación nos ayudará a elegir la metodología que mas se adapta para realizar nuestro proyecto:

Factor	Ponderación	METODOLOGIA MAGERIT	METODOLOGIA OCTAVE	METODOLOGIA CRAMM	METODOLOGIA COSO
Objetivos	25	20	15	15	20
Estructura	20	15	8	12	8
Manejo del Riesgo	20	10	10	18	18
Metodología adoptada	15	15	10	15	12
Calificación del Impacto	15	12	10	7	15
Base de Datos de Riesgos.	5	4	4	2	5
Total	100	76	57	69	78

De acuerdo a los factores evaluados y la calificación asignada a las metodologías planetadas, la metodología coso presenta mayores beneficios que nos permiten establecer los lineamientos necesarios para alcanzar los objetivos inicialmente establecidos, asimismo propicia un entorno que prepararnos a las exigencias que implica el nuevo acuerdo de capital.

CAPITULO 4

RESOLUCIÓN DEL PROBLEMA

4. RESOLUCIÓN DEL PROBLEMA APLICANDO LA METODOLOGÍA PLANTEADA

El modelo de administración de los Riesgos de Tecnología de Información según el Marco Integrado se ejecutará aplicando las siguientes etapas:

4.1 ESTRUCTURA ORGANIZACIONAL Y PROCEDIMIENTO DE TRATAMIENTO DE RIESGOS

En esta etapa, se ha definido de manera clara los lineamientos de la organización con respecto al tratamiento de los riesgos, así como conseguir el compromiso de participación de la Alta Gerencia y mostrar la importancia y la necesidad de una adecuada administración de los riesgos a nivel general.

a) DEFINICIÓN DE LA ESTRUCTURA ORGANIZACIONAL

Teniendo en cuenta lo estipulado en la normativa, donde se indica la necesidad por parte de las empresas de establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, la Gerencia de Riesgos del Banco delega esta responsabilidad a la División de Riesgos de tecnología de Información.

b) DEFINICIÓN DE LA VISIÓN Y ESTRATEGIA ORGANIZACIONAL VISIÓN

La administración de riesgos de tecnología de información, será reconocida como ente gestor de un ambiente seguro en el manejo de la tecnología y la información asociada a ella dentro del Banco, alcanzando adecuados niveles que garanticen la seguridad de información, la continuidad de negocio y la participación de toda la organización, contribuyendo con el desarrollo de mecanismos y servicios financieros seguros e innovadores que permitan mejorar la competitividad empresarial y la calidad en el servicio.

ESTRATEGIA ORGANIZACIONAL

La estrategia organizacional para la gestión y difusión de una cultura de riesgo, se sustenta en un proceso continuo de concientización que se inicia con la verificación de todos los sistemas, aplicaciones y procesos actuales. La elaboración y despliegue de las políticas, los procesos y arquitectura de seguridad con la participación de las diversas áreas involucradas en las operaciones y servicios que requieren de tecnología y finalmente, la estrategia general de riesgos que considera los sub planes de adecuación bajo un enfoque de gestión de riesgos orientado a la estrategia del Banco.

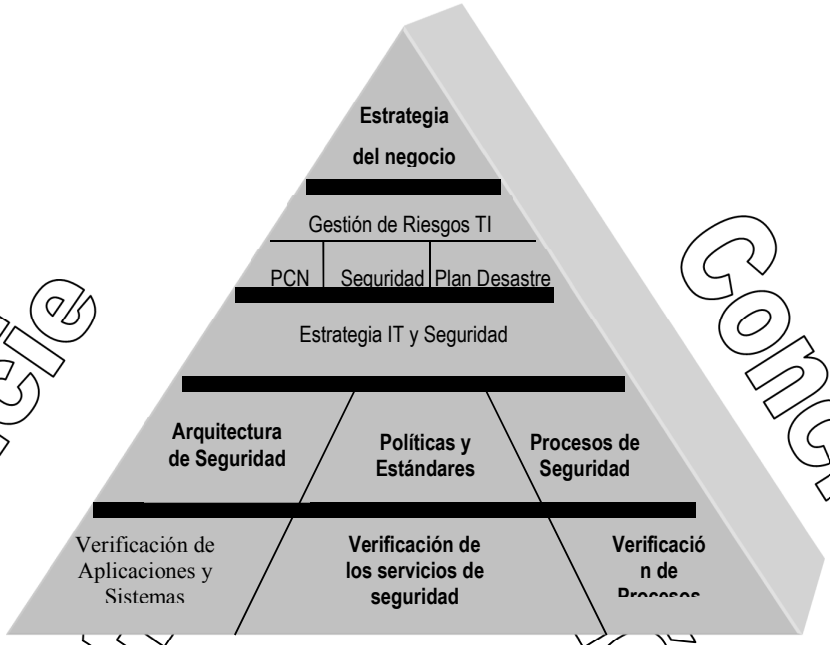


Figura N° 6: Estrategia Organizacional [5]

c) CONCIENTIZACIÓN EN LA ALTA DIRECCIÓN

Debido a la importancia de la Administración de riesgos, y a las implicancias que tiene en la institución, como es la emisión de políticas, normas y procedimientos, entre otros; se hace necesario el respaldo de la Alta Dirección. Al respecto, la Gerencia General ha mostrado el total apoyo a la Gerencia de Riesgos y está participando activamente en la difusión de los planes a las demás gerencias. Hay que resaltar la ubicación del Departamento de Riesgos como órgano de línea de la Gerencia General.

4.2 GESTION DE RIESGOS DE TECNOLOGIA DE INFORMACION

La metodología a ser usada por la División de Riesgos de Tecnologías de Información, estará basada esencialmente en lo establecido por el Marco Integrado, así como la recopilación de metodologías aplicadas por empresas financieras y la recolección de información de los estándares internacionales relacionados.

Nuestra metodología incluye las siguientes fases:

1.- Diagnóstico Inicial de procesos críticos.

2.- Un proceso continúo de evaluación de vulnerabilidades y riesgos, diseño e implementación de medidas de mitigación y el control de los riesgos.

3.- Un proceso de capacitación y concientización como soporte a los dos anteriores.

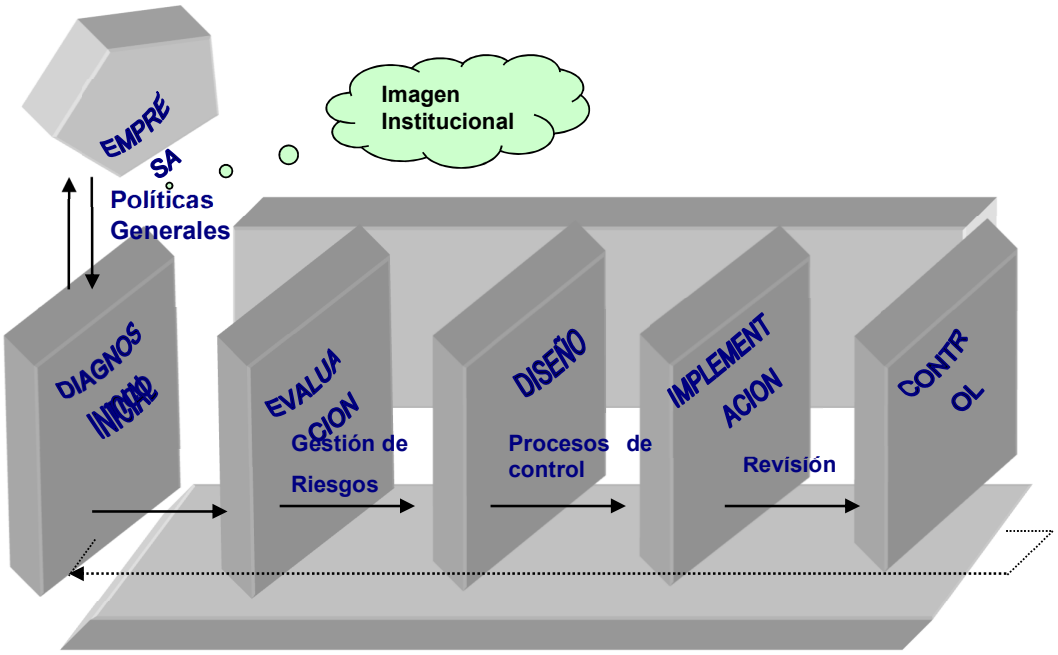


Figura 7: Esquema de la Metodología RMC [3]

4.2.1. DIAGNÓSTICO INICIAL DE PROCESOS CRÍTICOS

En está fase, se realiza un levantamiento total de información sobre los procesos del negocio, con énfasis especial en las áreas de TI y sobre la base del flujo de las políticas generales del Banco. Para ello, se utiliza una plantilla de Relevamiento de información para cada uno de los puntos críticos asociados con riesgos de tecnología de información y se consolida en un documento inicial de evaluación de la situación en la que el Banco se encuentre con relación a la Administración de los riesgos de tecnología de información. Los puntos críticos fueron:

- Servicios prestados por terceros
- Seguridad lógica
- Seguridad de personal
- Seguridad física
- Clasificación de seguridad
- Desarrollo de Sistemas
- Flujo de información interna y externa
- Procesos de respaldo
- Seguridad en operaciones y comunicaciones
- Eventos externos asociados a la operatividad y gestión del Banco.

El desarrollo de esta etapa permite detectar cuales son los factores críticos hacia los cuales la Gerencia orientará un plan de tratamiento y control de riesgos. Para la recopilación de información, se han realizado entrevistas con personal de las diferentes dependencias.

Posteriormente, se envía a las áreas involucradas una encuesta de autoevaluación conteniendo los mismos tópicos incluidos en el levantamiento de información con el objetivo de validar nuestra percepción y minimizar la sensibilidad a los resultados de la evaluación de información.

Los resultados del diagnóstico muestran de manera detallada y en resumen los puntos críticos considerados en relación con el nivel de control de los Riesgos de Tecnología a los que se encuentran expuestos. Este diagnóstico permite determinar lo siguiente:

- Nivel de Control de los Riesgos de Tecnología de Información.
- Estado de los mecanismos de control (formalizados, actualizados y/o en desuso).
- Existencia de documentos y normas asociados, desactualizados o no se conocen.
- Factores con mayor nivel de control.
- Factores con menor nivel de control y que requieren de medidas de mitigación inmediatas.

4.2.2 EVALUACIÓN DE VULNERABILIDADES Y RIESGOS, DISEÑO E IMPLEMENTACIÓN DE MEDIDAS DE MITIGACIÓN Y CONTROL DE RIESGOS

Este proceso está inmerso en un programa retroalimentado denominado VERIFICACION CONTINUA el mismo que enlaza los procesos anteriores utilizando herramientas de gestión de riesgo, procesos de emisión de reportes a la Alta Dirección y control a través de hojas de verificación y control.

Como herramientas de gestión de riesgo, se utiliza:

- La matriz de evaluación de riesgos.
- La matriz de clasificación de nivel de control de riesgo.
- La matriz de riesgos residuales.
- Plantilla de Evaluación de Riesgos.

Estas herramientas permitirán apreciar tanto cualitativa como cuantitativamente el impacto del riesgo asociado a los procesos críticos de negocio, con lo cual se recomendarán las medidas correctivas y preventivas necesarias.

En esta fase se realiza el análisis de los activos de información del Banco y el análisis de cada uno de los factores críticos.

A) CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

El objetivo de esta fase es la recopilación y continua actualización de los activos de información, tanto a nivel del centro de cómputo, central de almacenamiento de dispositivos de respaldo y otras ubicaciones físicas y remotas.

Asimismo, se implementa niveles de clasificación, impacto y criticidad para los activos inventariados, lo que permite documentar formalmente lo relativo a activos de información.

Para el proceso, se ha considerado el valor de medición de nivel de Impacto asociado a un valor que puede tener en la empresa la ocurrencia de un incidente que afecte al activo en evaluación. Dicho valor ha sido ponderado en una escala del 1 al 5; donde 1 se refiere al de menor impacto y 5 al máximo. Asimismo, para la Igualmente para la Clasificación de la información documentaria asociada a cada uno de los activos, se ha considerado los valores de USO INTERNO, CONFIDENCIAL, RESTRINGIDA, SIN RESTRICCIONES. Finalmente, para la clasificación de criticidad, se ha utilizado IMPRESCINDIBLE, ALTA, REEMPLAZABLE, NO CRÍTICO Y PRESCINDIBLE como niveles de medición.

Esta clasificación se realiza utilizando el inventario de activos existente en el Banco, la valorización de los activos considerando los factores de impacto, clasificación y criticidad fue realizada utilizando técnicas basado en la experiencia del personal que administra directamente el riesgo, en este caso, el trabajo es directamente ejecutado con el personal experto del Departamento de Informática y la División de Seguridad del Banco, esta primera clasificación permitirá generar una base de datos de clasificación histórica que permitirá más adelante aplicar técnicas estadísticas para medir con menor sensibilidad a fallas la criticidad de activos de información.

B) IDENTIFICACIÓN Y EVALUACIÓN DE VULNERABILIDADES, RIESGOS Y MEDIDAS DE MITIGACIÓN

El procedimiento para la identificación y evaluación de riesgos y vulnerabilidades se ha realizado sobre la base de los puntos críticos asociados con tecnología y se ha desarrollado un proceso sistemático estructurado buscando abarcar la praxis de los usuarios finales y los responsables de los procesos críticos, los conceptos basados en la experiencia, un análisis de escenarios y un inventario inicial de riesgos asociados a la naturaleza implícita del proceso.

El análisis ha involucrado las fuentes de riesgo, sus consecuencias y un completo proceso que involucra la posibilidad de la ocurrencia del evento de riesgo asociada con el impacto hacia la institución y además considera los procedimientos actuales de control con orientación a incluir aquellas medidas de mitigación que puedan ser resultado de la evaluación de los riesgos.

Las medidas de control o mitigación de los riesgos evalúan todas aquellas actividades que permitan reducir el riesgo asociado a los factores de negocio, tales como controles preventivos, planes de contingencia, transferencia de impactos a seguros, y guardan correlación con la primera etapa de la metodología donde se recogieron las medidas de mitigación naturales al Banco.

Considerando que en el Banco, no existía a la fecha ninguna aplicación de registro de eventos de riesgo, se ha implementado un servicio de registro e identificación de eventos de riesgo, mediante el cual, las diversas áreas del Banco pueden ir incrementando la base de datos de riesgos de operación y de tecnología de información que se ha desarrollado considerando las bases de datos pre establecidas por la BBA Operacional Risk Database Association[13], el sistema de objetivos de control de COBIT y las normas ISO 17799. Los nuevos eventos de riesgo a registrar, están sustentados en la naturaleza del negocio particular y la experiencia de los responsables de los procesos y servicios en el

[13] British Bankers Association: Management and Supervision of Operational Risk http://www.bba.org.uk

Banco con quienes se tuvo reuniones de coordinación en las cuales se recopiló los demás eventos de riesgo componentes del registro de riesgos.

A continuación, se muestra las herramientas aplicadas y en la matriz de "Evaluación de riesgos asociados tecnologías de información" se aprecia los resultados del proceso para cada uno de los puntos críticos evaluados

MATRIZ DE EVALUACIÓN DE RIESGOS:

Es una matriz que refleja el nivel del riesgo asociado a un proceso de negocio, está basada en el impacto que generaría en el negocio la ocurrencia de amenazas u oportunidades y la probabilidad de ocurrencia de éstas. [6]

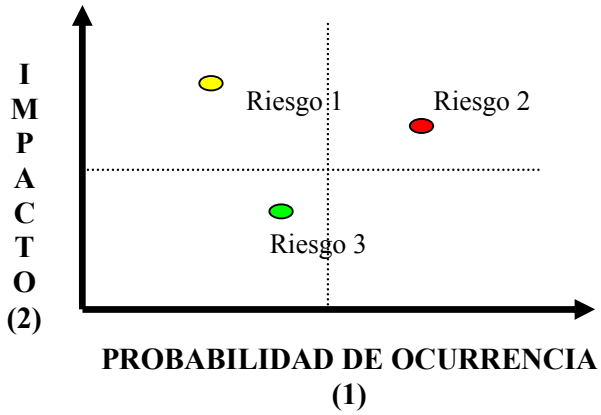


Figura Nº 8: Matriz de evaluación de riesgos [3]

El impacto será medido como la consecuencia de las amenazas y las oportunidades en los aspectos económicos, políticos, sociales y en los objetivos de la empresa [6]. El impacto ha sido calificado en 5 niveles:

NIVEL DE IMPACTO	CALIFICACION	DESCRIPCION
BAJO	0	Impacto irrelevante, a nivel económico y operativo es poco significativo, a nivel social no se percibe.
MEDIO BAJO	1	El impacto es percibido a nivel interno, existen pérdidas operativas y económicas aceptables.
MEDIO	2	Impacto moderado en los niveles económico, operativo y de servicios
MEDIO ALTO	3	El impacto a nivel operativo es significativo, a nivel económico puede ocasionar pérdidas sustanciales, existencia de detención de procesos.
ALTO	4	El impacto en el negocio es totalmente negativo, la empresa puede finalizar sus operaciones, las acciones correctivas son irrelevantes, peligro total en la reputación y situación en el mercado.

Tabla Nº 1: Niveles de Impacto de la Matriz de Riesgos.

La probabilidad es la medida de la posibilidad de ocurrencia de la amenaza u oportunidad. Esta ha sido calificada en 5 niveles:

PROBABILIDAD	CALIFICACION	DESCRIPCION Y CARACTERISTICAS
BAJO	0	Ocurrencia muy improbable, no se conocen casos asociados al negocio, periodos de tiempo largos de ocurrencia
MEDIO BAJO	1	Ocurrencia poco probable, se conocen casos aislados, los periodos de ocurrencia son en periodos largos.
MEDIO	2	Probabilidad de ocurrencia a nivel significativo, existe varios casos asociados, la ocurrencia se da en periodos cíclicos conocidos.
MEDIO ALTO	3	Los acontecimientos ocurren con frecuencia, conocimiento de casos
ALTO	4	La ocurrencia en este nivel es continua, existencia importante de factores externos asociados, existencia muy significativa de casos similares.

Tabla Nº 2: Niveles de amenaza u oportunidad de Riesgos

Por lo cual, el nivel de riesgo asociado se reflejará en aplicación de los dos componentes antes mencionados en la relación de importancia del 60% para el impacto y 40% para la probabilidad de ocurrencia, esto sustentado en la naturaleza social del Banco:

PROBABILIDAD

IMPACTO	BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO	ALTO
BAJ0	BAJO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO
MEDIO BAJO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO	MEDIO
MEDIO	MEDIO BAJO	MEDIO	MEDIO	MEDIO	MEDIO ALTO
MEDIO ALTO	MEDIO	MEDIO	MEDIO ALTO	MEDIO ALTO	MEDIO ALTO
ALTO	MEDIO	MEDIO	MEDIO ALTO	ALTO	ALTO

Riesgo Asociado = P*0.4 + I*0.6

Tabla Nº 3: Riesgo Asociado

MATRIZ DE IDENTIFICACIÓN DE CONTROLES EXISTENTES:

Las medidas de control o mitigación de los riesgos evalúan todas aquellas actividades que permitan reducir el riesgo asociado a los factores de negocio, tales como controles preventivos, planes de contingencia, transferencia de impactos a seguros, etc.

NIVEL DE CONTROL	CARACTERISTICAS PRINCIPALES	OBSERVACIONES DOCUMENTARIAS	ESQUEMA GRÁFICO
0: No Controlado	No existe mecanismos formales o informales de control, no existen medidas de ningún tipo para el control de riesgos. No se reconocen los factores de riesgo asociados a los procesos. Es muy probable la materialización del riesgo	No existen documentos	rojo
1: Nivel de Control bajo.	Existen indicios informales de control de riesgos, generalmente se llevan a cabo por costumbre, no cubre la totalidad de los grupos involucrados, está en proceso de formación. El riesgo se puede materializar.	Existen documentos asociados no relativos directamente al punto crítico	naranja
2: Nivel de Control parcial	Existen mecanismos de control, éstos no están formalizados o están en desuso, asimismo éstos no son de conocimiento de los involucrados. Se están formando equipos de control. Existen posibilidades de la ocurrencia de las amenazas	Existen documentos y normas asociados, éstos están desactualizados o no se conocen	amarillo
3.- Nivel de Control razonable	Existencia regular de mecanismos formales de control de riesgos, éstos se difunden a casi todos los usuarios involucrados, existen equipos encargados del control de riesgos.	Existen documentos publicados actualizados y formalizados, definición de roles y responsabilidades.	verde
4.- Nivel de control óptimo	Se tiene participación total de los involucrados, distribución eficiente de documentos de sustento y mecanismos formales de control, monitoreo y seguimiento del nivel de control de riesgos. Muy poca posibilidad de materialización del riesgo.	Existen documentos formales, estándares, de seguimiento dual, con definición de roles, responsabilidades y certificados	azul

Tabla Nº 4: Matriz de identificación de controles existentes.

MATRIZ DE RIESGO RESIDUAL

Es la medida del nivel de riesgo, que se realiza posteriormente a la ejecución de las actividades de mitigación de riesgos.

CONTROL DE RIESGOS

NIVEL RIESGO

	OPTIMO	RAZON.	PARCIAL	BAJO	SIN CON.
BAJO	BAJO	BAJO	BAJO	BAJO	BAJO
MEDIO BAJO	BAJO	BAJO	BAJO	MEDIO BAJO	MEDIO BAJO
MEDIO	BAJO	BAJO	MEDIO BAJO	MEDIO	MEDIO
MEDIO ALTO	BAJO	MEDIO BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO
ALTO	BAJO	MEDIO BAJO	MEDIO	MEDIO ALTO	ALTO

Tabla Nº 5: Matriz de Riesgos Residuales

Efectividad: Es el resultado de la evaluación de los riesgos del negocio teniendo en consideración las medidas de control y mitigación, ello permitirá las medidas a tomar por parte de las dependencias del Banco. [7]

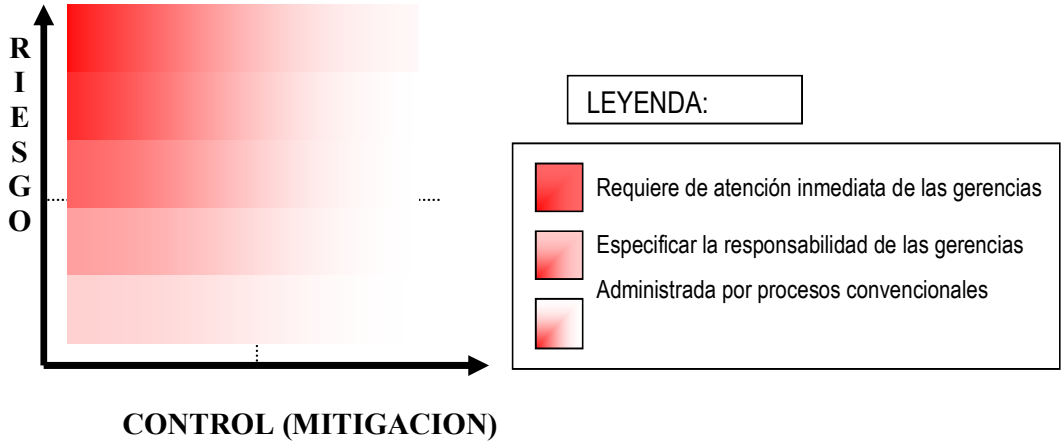


Figura Nº 9: Cuadro de Efectividad de la Matriz de Riesgos Residuales [3]

IMPLEMENTACION DE MEDIDAS DE MITIGACION

Como se ha indicado, la implementación de las medidas de mitigación, son recomendaciones a aplicar en el Banco posterior a la validación de la efectividad de los procedimientos de control existentes. Para este proceso, se ha simplificado en dos tipos de evaluación de riesgo:

1.- Para aquellos eventos de riesgo que tienen medidas de mitigación implementada s o en ejecución.- En este caso, las medidas de mitigación adicionales se han recomendado considerando la efectividad del mecanismo de mitigación actual y cuando el riesgo residual mantenga un nivel superior al nivel MEDIO. Este proceso, se ha realizado de la siguiente manera: Si la medida de mitigación actual no es efectiva, es decir, no reduce efectivamente el nivel de riesgo del evento en análisis, se evaluará la posibilidad de modificarlo o repotenciarlo.

2.- Para aquellos eventos de riesgo que actualmente no tienen ninguna medida de mitigación implementada o en ejecución.- En este caso, las medidas de mitigación se han recomendado cuando el riesgo residual mantenga un nivel superior al nivel MEDIO.

Para ambas opciones, se evalúa el costo beneficio de la implementación o modificación de las medidas de mitigación. El resultado se muestra en el Detalle de Evaluación de medidas de mitigación.

PROCESO DE CAPACITACIÓN Y CONCIENTIZACIÓN

Un proceso de capacitación y concientización como soporte a las dos anteriores etapas, el mismo que incluye al personal general del Banco y a la Gerencia General la misma que permitirá la expansión de la cultura de riesgo, la misma que incrementará nuestra imagen institucional.

Esta fase se orientará a cubrir la necesidad de concientizar acerca de la importancia de una cultura de riesgos, así como también a capacitar para el

correcto despliegue y manejo descentralizado de los riesgos en cada una de las sucursales y agencias en todo el país.

TRATAMIENTO DE PROCESOS CRITICOS DE NEGOCIO

Una de las principales consideraciones dentro de la Administración de riesgos de Tecnología de información es el tratamiento de los procesos críticos del negocio, para la consecución de este objetivo, se ha logrado Identificar los factores externos e internos de interrupción del negocio y los parámetros para la clasificación y priorización de procesos críticos relacionados a la actividad y naturaleza del Banco.

Esta identificación es el punto de partida para la identificación tanto de los procesos críticos del negocio, como también la tecnología que está ligada a cada uno de los mismos.

IDENTIFICACION DE LOS FACTORES DE INTERRUPCION

Para el proceso de identificación de los factores que de materializarse podrían interrumpir la Continuidad del Negocio se ha creído conveniente hacer una distinción entre los factores internos, es decir, los que se generan por eventos propios del Banco; y los factores externos, cuya causa son eventos que se encuentran fuera del control del Banco.

FACTORES INTERNOS

Como su nombre lo indica, son factores producidos por eventos que se generan dentro del Banco, en el proceso operativo constante. Por ser de origen interno, se puede realizar un control adecuado a cada unos de estos factores, es decir, está dentro de la capacidad del Banco poder aplicar medidas de control interno para preveerlos de manera adecuada.

Dentro de esta clasificación hemos identificado los siguientes:

- Robo Físico: Robo de infraestructura de vital importancia para el normal desarrollo de las operaciones del banco, incluye equipos informáticos, información, entre otros. Esta también considerado como factor externo, cuando la sustracción es perpetrada por personas ajenas al Banco.
- Paralización de labores: Relacionado con huelgas y demás tipos de protesta que pudieran paralizar la actividad dentro de la institución.
- Falla en los dispositivos de conectividad: Se refiere a cualquier eventualidad que se pudiese producir con los equipos críticos de interconexión como router, switch, firewall, entre otros.
- Falla en los enlaces de comunicación: Hace referencia a fallas que podrían ocasionarse durante la transmisión de la información, en especial se consideran, las fallas de comunicación con el servidor central.
- Sabotaje: Relacionado con la destrucción o deterioro de equipos, maquinaria e instalaciones del Banco por parte de los empleados, se incluye en este rubro el ataque informático interno
- Inadecuada manipulación de dispositivos críticos: Factor de interrupción producido por un error, falla o manejo inadecuado de los equipos y dispositivos críticos por parte de los responsables de éstos.

FACTORES EXTERNOS

Son factores generados por eventos que se encuentran fuera del alcance y del control del Banco. Estos factores son los que se muestran a continuación:

- Factor Regulatorio: Cambios de la regulación en la industria/país.
- Factor Político: Guerra, política económica, bloqueo de negocios.
- Factor Legal: Interpretación, emisión o modificación de leyes.
- Desastres: Relacionado con desastres naturales a los cuales por la ubicación geográfica estamos propensos, siendo los más perjudiciales terremoto, inundación, entre otros.
- Vandalismo: Guarda relación con ataques originados por terceras personas, que no tienen vinculación alguna con el banco, sobre la

infraestructura del mismo, se incluyen aquí las protestas y marchas violentas ajenas a la institución.

- Delitos informáticos: Considera los ataques informáticos perpetrados por los conocidos hackers, crackers, y/o cualquier otro tipo de pirata informático que violase las barreras de seguridad establecidas por el Banco.
- Ataques de ex empleados: Considera cualquier tipo de ataque, en su mayoría informáticos, perpetrado por ex empleados del Banco. Su conocimiento de los niveles de seguridad, así como de claves y vías de acceso, facilitan la violación de las barreras de seguridad del Banco. Este factor es una variante de los delitos informáticos.
- Acciones Terroristas: Ocasionado por ataques terroristas, en toda su variedad.
- Contingencias de energía: Relacionado con caídas del fluido eléctrico, apagones, pulsos de tensión, entre otros.
- Contingencias de comunicación: Relacionado con la dependencia de comunicación con otras empresas.

PARAMETROS PARA CLASIFICACION DE PROCESOS

Para priorizar de manera correcta los procesos sensibles a la ocurrencia de los factores tanto internos como externos, se hace necesario hacer uso de ciertos parámetros que permitan medir de manera adecuada la criticidad de estos procesos.

Los parámetros ha ser usados, de acuerdo a su nivel de importancia, son los siguientes:

Impacto Económico (IE)

Relacionado con el impacto económico total que generaría la ocurrencia de un factor de interrupción. Este parámetro está conformado por el gasto de recuperación, la pérdida por interrupción, el número de operaciones y el volumen marginal de operaciones.

- **Gasto por Recuperación (GR):** Gasto económico necesario para la recuperación de la continuidad del proceso.
- **Pérdida por Interrupción (PI):** Pérdida económica ocasionada durante el periodo en el que un proceso se encuentre no operativo.
- **Número de Operaciones (NO):** Número total de operaciones que se realiza a través de un proceso en una unidad de tiempo de interrupción.
- **Monto de Operaciones (MO):** Monto de las operaciones que se realiza a través de un proceso en una unidad de tiempo de interrupción.

Por tanto, el impacto económico se expresa de la siguiente manera:

IE = (GR + PI + NO + MO) / 4

Tiempo Mínimo de Recuperación (TMR)

Relacionado con el período de tiempo que un proceso se encuentra no operativo. Para este parámetro se debe considerar el tiempo mínimo requerido para que el proceso se reestablezca, asimismo debe de realizase el calculo de tiempo mínimo del peor caso que se pudiese presentar en la ocurrencia de un factor de interrupción.

Impacto Social (IS)

Todos aquellos factores que por la naturaleza y misión del banco podrían significar dejar de cumplir con el soporte, servicio y beneficios a los empleados activos y pasivos del sector público y la necesidad de asegurar la prestación de servicios como única oferta bancaria.

Afección a la Imagen Institucional (II)

Relacionado con los efectos que podría tener, la ocurrencia de un factor de interrupción, sobre los clientes, proveedores y demás entes que tengan relación, directa o indirecta, con el Banco.

Ubicación Geográfica (UG)

Relacionado con el ámbito geográfico en el cual está incluido el proceso afectado por un factor de interrupción.

Otros (OT)

Relacionado con cualquier otro parámetro adicional o propio para cada proceso que tenga relevancia en cuanto a la ocurrencia de un factor de interrupción del negocio.

CALCULO DE PUNTUACION DE PROCESOS

El cálculo de la puntuación de un proceso, será obtenido en función de la ponderación de los parámetros identificados anteriormente; es así que esta puntuación se obtiene considerando ponderadamente cada uno factor.

El modelo matemático del cálculo de la puntuación de un proceso crítico se expresa de la siguiente manera:

Puntuación del Proceso (X) =	100* **IE(x)** + 40***TMR(x)** + 100***IS(x)** + 50***II(x)** + 30***UG(x)** + 10* **0T(x)**

Donde:

Puntuación del Proceso(X): Puntuación total del nivel de criticidad que posee el proceso "X" dado que está siendo afectado por un factor de interrupción. Esta puntuación permitirá ubicar de manera jerarquizada cada uno de los procesos desde los más críticos para la continuidad del negocio, hasta los menos críticos, de tal manera que se orienten los planes de recuperación a los más importantes según el resultado ordenado de la evaluación, Siempre que haya ocurrido un factor de interrupción.

IE(x): Impacto económico que causaría la interrupción del proceso "X", frente a la ocurrencia del factor de interrupción".

TMR(x): Tiempo mínimo de recuperación que necesitaría el proceso "X", de ser interrumpido por la ocurrencia del factor de interrupción".

IS(x): Impacto social que por la naturaleza del banco generaría la interrupción del proceso “X”, a causa de la ocurrencia del factor de interrupción.

II(x/y): Medición del nivel en que afecta a la imagen institucional la interrupción del proceso “”X”, a causa de la ocurrencia del factor de interrupción.

UG(x): Medición del nivel en que afecta por la ubicación geográfica la interrupción del proceso “X”, a causa de la ocurrencia del factor de interrupción.

OT(x): Cualquier otro parámetro propio del proceso “”x”, frente a la ocurrencia del factor de interrupción.

Rango de Calificación: El rango de calificación para cada uno de los factores de cuantificación se realizará en escala numérica de 1 a 9 considerando para ello que el nivel de impacto o pérdida aumenta con la escala. [6]

RANGO DE CALIFICACION →								
INCREMENTO DE NIVEL DE IMPACTO O PERDIDA								
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
← DISMINUCION DE NIVEL DE IMPACTO O PERDIDA								

Se muestra el resultado de la evaluación aplicando la puntuación de procesos a los Servicios externos del Banco. Esta evaluación se realizó en trabajo conjunto con el Departamento de Operaciones quienes brindaron la información de número de operaciones, monto de operaciones por servicio en evaluación y lo referente a los tiempos de recuperación y pérdidas estimadas aplicando un primer nivel de gastos según volumen de operaciones y aplicando técnicas basado en la experiencia del personal a cargo de los procesos críticos de negocio. El impacto social ha sido evaluado en trabajo conjunto con el Departamento de Servicios Bancarios, mientras que el factor geográfico ha tenido un primer desarrollo a nivel de la Red de Agencias.

CAPITULO 5

CONCLUSIONES Y FUTUROS TRABAJOS

5. CONCLUSIONES Y FUTUROS TRABAJOS

La administración integral de riesgos ha cobrado importante valor dentro de las actividades de una empresa, considerando además que las empresas financieras son un nicho de negocio sustantivamente crítico por la información, los servicios y los activos a proteger relacionados con su naturaleza, en este sentido y considerando el soporte a las operaciones y servicios que brinda la tecnología, es fundamental garantizar la adecuada administración de los riesgos inherentes al nivel de servicio y continuidad del negocio que ésta presta. Por ello, administrar los riesgos de tecnología de información, permitirá cubrir aquellos aspectos que conlleven a lograr minimizar cualquier efecto de vulnerabilidad o evento externo que signifique riesgos y que traigan consigo pérdidas de algún tipo a la empresa.

Se conseguirá mantener un adecuado esquema continuo de evaluación de los riesgos a los que está expuesta la tecnología de información, los recursos asociados a ella, los activos de información y los procesos con soporte en equipos tecnológicos. El Banco, aplicará un control permanente a aquellos factores estructurales y en aquellos casos coyunturales donde sea necesario un análisis de proceso en especial, se aplicará la misma metodología considerando el riesgo coyuntural como un tipo especial de riesgo al cual se le hará el seguimiento respectivo.

Se logrará disponer de un registro permanentemente y actualizado de los principales eventos de riesgos que afecten la operativa de los procesos. Esto nos permitirá una adecuada sinergia con los procedimientos de continuidad del negocio.

Los alcances a nivel organizacional, implican resultados en el corto y mediano plazo a nivel de Resultados de infraestructura tecnológica y seguridad de información soportada en esta infraestructura, servicios y operaciones con soporte en tecnología, los requerimientos de la superintendencia.

El Banco dispondrá de información clasificada, pudiendo orientar la atención de las Gerencias respectivas hacia los eventos de riesgos que pudieran significar mayores pérdidas para el negocio. Se podrá disponer de información relevante que nos permitan construir herramientas para evaluar y monitorear permanentemente el hallazgo de nuevos eventos de riesgo y a los cuales se les dará el tratamiento respectivo.

Para lograr estos resultados, se tiene en cuenta factores estratégicos como el apoyo de la Alta Dirección, la necesidad de disponer de amplios espacios de difusión, la fácil implementación de los mecanismos de administración de riesgos, la necesidad de orientar a la institución hacia la formalización de procesos y actividades, una permanente verificación y pruebas de control que garanticen la disponibilidad, integridad y confidencialidad de información y finalmente un adecuado plan de despliegue de la cultura de riesgos que garantice la participación general de los empleados.

Este trabajo permitirá establecer el enfoque basado en riesgos, como el requerido por la Auditoría moderna y el exigido por las organizaciones actuales. Este trabajo, permite al auditor partir de la problemática de la administración del riesgo y promover el mejoramiento continuo del control interno, mediante la evaluación y asesoría sobre el proceso de identificación, evaluación, control y monitoreo de los riesgos críticos de la organización.

El auditor actual, sin importar su área de especialidad, debe ampliar su enfoque y planeamiento del trabajo, para cubrir “todos” los riesgos del negocio, partiendo de su contexto estratégico, y particularmente el riesgo operativo por su impacto en todos los procesos de las organizaciones. De esta forma, el auditor no solo logrará resultados alineados con las expectativas de la alta gerencia, sino que le permitirá administrar razonablemente el riesgo de Auditoría y brindar un mayor valor agregado a su trabajo.

CAPITULO 6

REFERENCIAS BIBLIOGRAFICAS

6. REFERENCIAS BIBLIOGRAFICAS

LIBROS

[1] FRANCESE ROSES – Risk Management, Una nueva forma de asegurar el éxito empresarial. ACV Ediciones Barcelona 2002.

[2] COBIT – Objetivos de Control para la Información y tecnologías afines - Control Objectives – 4Ta. Edición. COBIT, Junio 2006.

[3] ISO/IEC 17799 International Standard, Información Technology – Code of practice for information security management, first edition, ISO/IEC 2000.

[4] ALBERTO CANCELADO G. - Sistema De Administración De Riesgos En Tecnología Informática, Noviembre 2003.

[5] HEIDI RICHARDS - Federal Reserve Board, Information Technology Risks, Marzo 2001

[6] ESTANDAR AUSTRALIANO – Administración de Riesgos AS/NZS 4360:1999.

TESIS

[7] BORGHELLO CRISTIAN F. – TESIS: Seguridad Informática: Sus Implicancias e Implementación- Universidad Tecnológica Nacional de Argentina, Licenciatura en Sistemas, 2001.

[8] ALLAN R. PALIOTTA - A Total-Process View of information Security Risk Management, Agosto 2001

[9] GUISSELLA MOSCOSO S. – TESIS: Metodología Para La Evaluación de Riesgos de Activos de TI en Entidades Financieras - Universidad Nacional Mayor de San Marcos, 2006.

REVISTAS INDEXADAS:

[10] CHARLES CRESSON WOOD, Cisa, Cissp – Information Security Policies Made Easy V. 6 Baseline Software, Inc., USA 1997.

[11] EDPACS - The Edp Audit, Control, And Security- A view of international IT Security Standards, Especially ISO/IEC17799, Diciembre 2001.

[12] PROTECTING VALUE – Study 2003 Managing Business Risks

[13] ERNST & YOUNG - Global Information Security Survey 2002 -Technology And Security Risk Services

[14] ANDRES CORREAL – Plan de Contingencias, Fundación Universitaria de Boyacá, Nov. 2002

[15] M. FARIAS – ELINOS - Auditoría de los Sistemas de Información - LIDETEA, Universidad de la Salle México,

[16] RODOLFO OCONITRILLO BRENES - Gestión De Riesgos, Una propuesta práctica para Cooperativas de Ahorro y Crédito

[17] GABRIEL CASAS SAAVEDRA – Evaluación de Riesgos, IV Reunión de Auditores Internos de Banca Central – CEMLA Cartagena de Indias, Colombia julio de 1998.

[18] BETTY INFANTE – Evade ITESM México – Banca por Internet, una nueva forma de hacer negocios, 2003.

[19] RU SECURE – Information Security Policies V. 2.0 – Securing Information In The Digital Age, Abril 2003.

[20] GALLO, PORTUGAL, PARRONDO, SANCHEZ - La Protección de Datos Personales, Soluciones en Entornos Microsoft ®, Microsoft Ibérica S.R.L. 2003.

SITIOS DE REFERENCIA EN INTERNET:

[21] ISACA: The Information Systems Audit and Control Association & Foundation (Accesado Enero 2008)
http://www.isaca.org/

[22] Elaboración de mapas de riesgo (Accesado Febrero 2008)
http://www.securitymanagement.com/library/001147.html

[23] Riesgos del Software – tutorial (Accesado Marzo 2008)
http://www.cs.virginia.edu/~knabe/riesgos.html

[24] Guía para la evaluación de riesgos (Accesado Enero 2008)
http://www.istas.net/sl/bajar/rspsc2.pdf

[25] Minimizar los riesgos en el uso de la tecnología
(Accesado Enero 2008)
http://www.aceproject.org/main/espanol/et/ete.htm

[26] Análisis de Riesgos y plan de respuesta a contingencias
(Accesado Abril 2008)
http://www.transredes.com/pdfs/MedioAmb/eeia/eeiaColpaMineros/08_AnalRiesgosPlanContin.PDF

[27] Links De Seguridad De Información (Accesado Febrero 2008)
http://www.security.kirion.net/seguridad/

[28] Seguridad De Información (Accesado Febrero 2008)
http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm

[29] La Importancia de la Seguridad Informática: Las políticas y la Legislación (Accesado Abril 2008)
http://seguridad.internet2.ulsa.mx/

CAPITULO 7

ANEXOS

7. ANEXOS

ANEXO 1: RESOLUCIÓN N°006.2002

ANEXO 2: CIRCULAR Nº G-105-2002

ANEXO 3: RESOLUCIÓN N°37.2008

ANEXO 4: MATRIZ DE EVALUACIÓN DE RIESGOS ASOCIADOS A TECNOLOGÍA DE INFORMACIÓN

- Desarrollo de Sistemas
- Servicios Prestados por Terceros
- Seguridad de Operaciones y Comunicaciones
- Seguridad Lógica
- Seguridad Física
- Seguridad de Personal
- Procesos de Respaldo
- Flujo de Información
- Clasificación de Información
- Medidas de Mitigación a Implementar - Evaluación de Riesgos De TI

7.1. ANEXO 1: RESOLUCIÓN SBB N°006.2002

Lima, 4 de enero de 2002

Resolución S.B.S.
Nº 006-2002

6.1.- EL SUPERINTENDENTE DE BANCA Y SEGUROS

CONSIDERANDO:

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público de acuerdo a lo señalado en el artículo 347º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley Nº 26702, y sus modificatorias, en adelante Ley General;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentran los riesgos de operación, los cuales pueden generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, resulta necesario establecer criterios mínimos prudenciales para que las empresas supervisadas realicen de manera adecuada la gestión de dichos riesgos;

Estando a lo opinado por las Superintendencias Adjuntas de Banca, Seguros y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349º de la Ley General y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Administración de los Riesgos de Operación, que forma parte integrante de la presente Resolución.

Artículo Segundo. - La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial ¨ El Peruano".

Regístrese, comuníquese y publíquese,

SOCORRO HEYSEN ZEGARRA

Superintendente de Banca y Seguros (e)

CAPITULO I

DISPOSICIONES GENERALES

6.1.1.- ALCANCE

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º.- Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Administración de riesgos: Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
d. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles.
e. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada. [14]
f. Reglamento del Sistema de Control Interno: Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.
g. Servicios críticos provistos por terceros: Servicios relacionados a procesos críticos provistos por terceros, cuya realización podría ser razonablemente desarrollada por la empresa supervisada. 1
h. Superintendencia: Superintendencia de Banca y Seguros.
i. Tecnología de información: Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.
j. Riesgo legal: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros [15]

---

[14] Literales e. y g. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005
[15] Literal incorporado mediante Resolución SBS N° 240-2005 del 08/02/2005

Riesgos de operación

Artículo 3º.- Las empresas deben administrar adecuadamente los riesgos de operación que enfrentan. Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación. [16]

Responsabilidad del Directorio y la Gerencia

Artículo 4º.- El Directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Asimismo, será también su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos y de las disposiciones contenidas en el presente Reglamento. Corresponderá a la Gerencia General la implementación de las políticas y procedimientos generales establecidos por el Directorio.

Unidad de riesgos

Artículo 5º.- De conformidad con lo dispuesto en el Reglamento del Sistema de Control Interno, la Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. Preparación y evaluación de políticas para la administración de los riesgos de operación.
b. Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.
c. Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
d. Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.
e. Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.
f. Otras necesarias para el desarrollo de su función.

---

[16] Literales e. y g. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005

Manual de organización y funciones

Artículo 6º.- De conformidad con las disposiciones contenidas en la presente norma y en el Reglamento del Sistema de Control Interno, la empresa deberá disponer de una estructura organizacional y administrativa que le permita una adecuada administración de los riesgos de operación. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones de la empresa.

Manuales de políticas y procedimientos

Artículo 7º.- Las políticas y procedimientos establecidos para la administración de los riesgos de operación deberán estar claramente definidos en los manuales de políticas y procedimientos; asimismo, deberán ser consistentes con el tamaño y naturaleza de la empresa y con la complejidad de sus operaciones y servicios.

Manual de control de riesgos

Artículo 8º.- El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la administración de los riesgos de operación.
b. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.
c. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.

d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.

e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

CAPITULO II
ADMINISTRACION DE LOS ASPECTOS QUE ORIGINAN LOS RIESGOS DE OPERACION

Procesos internos

Artículo 9º.- Las empresas deberán administrar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Tecnología de información

Artículo 10º.- Las empresas deberán administrar apropiadamente los riesgos asociados a la tecnología de información, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las empresas podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

Personas

Artículo 11º.- Las empresas deben administrar apropiadamente los riesgos asociados a las personas de la empresa, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Eventos externos

Artículo 12º.- Las empresas deberán considerar en la administración de los riesgos de operación la posibilidad de pérdidas derivada de la ocurrencia de eventos ajenos al control de la empresa que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen a los riesgos de operación referidos en los artículos 9º, 10º y 11º del presente Reglamento. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

CAPITULO III
REQUERIMIENTOS DE INFORMACION

Informe anual a la Superintendencia

Artículo 13º.- Las empresas deberán presentar a la Superintendencia, dentro de los noventa (90) días calendario siguientes al cierre de cada ejercicio anual, un informe referido a la evaluación de los riesgos de operación que enfrenta la empresa por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

a. Metodología empleada para la administración de los riesgos de operación.
b. Identificación de los riesgos de operación por proceso o unidad de negocio y apoyo.
c. Evaluación de los riesgos de operación identificados.
d. Medidas adoptadas para administrar los riesgos de operación materiales identificados y plazos para su aplicación. Dichas medidas podrán ser, entre otras:
    - Evitar el riesgo
    - Reducir su probabilidad de ocurrencia
    - Reducir las consecuencias
    - Transferir el riesgo
    - Retener el riesgo
e. Funcionarios responsables de las actividades de control de riesgo identificadas.
f. Plan de actividades de la Unidad de Riesgos en lo referente a la administración de los riesgos de operación.

Mediante Oficio Múltiple, la Superintendencia podrá definir posteriormente la estructura mínima del informe anual, informes periódicos de situación, asi como su presentación por medios electrónicos. [17]

---

[17] Literales e. y g. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005

Información adicional

Artículo 14º.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de los riesgos de operación de la empresa.

Asimismo, la empresa deberá tener a disposición de esta Superintendencia todos los documentos a que hace mención el presente Reglamento, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de las empresas cuya matriz no se encuentre en el país.

CAPITULO IV
COLABORADORES EXTERNOS

Auditoría Interna

Artículo 15º.- La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación, así como de lo dispuesto en el presente Reglamento. Asimismo, la Unidad de Auditoría Interna deberá incluir la referida evaluación en las actividades permanentes del Plan Anual y deberá realizar los informes y recomendaciones que se deriven de la misma.

Auditoría Externa

Artículo 16º.- Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de operación, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Empresas Clasificadoras de Riesgo

Artículo 17º.- Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la administración de los riesgos de operación en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Servicios provistos por terceros

Primera.- Las empresas son responsables de asegurar el cumplimiento de la normatividad emitida por la Superintendencia, aun en aquellos casos en que ciertas funciones sean realizadas por terceros. En este sentido, además del cumplimiento de lo dispuesto en la presente Resolución, las empresas deberán asegurarse de que los contratos suscritos con proveedores de servicios críticos a la empresa, incluyan cláusulas que faciliten una adecuada revisión de la

respectiva prestación, por parte de las empresas, la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

Medidas adicionales

Segunda.- La Superintendencia podrá disponer la adopción de medidas adicionales a las previstas en el presente Reglamento con el propósito de atenuar la exposición a los riesgos de operación que enfrentan las empresas.

Sanciones

Tercera.- En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plazo y Plan de Adecuación

Cuarta.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vencerá el 30 de junio de 2003. A dicha fecha las empresas deberán tener a disposición de este organismo de control los Manuales de Políticas y Procedimientos, el Manual de Organización y Funciones, el Manual de Control de Riesgos y los contratos de servicios críticos provistos por terceros a que se refiere la primera disposición final y transitoria del presente reglamento, adecuados a las disposiciones comprendidas en el mismo.

Para el ejercicio 2002 las empresas no se encuentran obligadas a presentar el informe anual a que se refiere el artículo 13º del presente reglamento. Sin embargo, en un plazo que no excederá del 30 de junio de 2002 deberán remitir a este organismo de control un plan de adecuación a las disposiciones contenidas en la presente norma. Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Reglamento de Auditoría Interna

Quinta.- Toda referencia realizada al término riesgo informático en el Reglamento de Auditoría Interna, aprobado mediante la Resolución SBS Nº 1041-99, deberá ser entendida como referida a los riesgos de operación, de acuerdo con lo dispuesto en la presente norma.

7.2. ANEXO 2: CIRCULAR Nº G-105-2002,

Lima, 22 de febrero de 2002

CIRCULAR Nº G-105-2002

Ref.: Riesgos de tecnología de información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias, en adelante Ley General, y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001, con la finalidad de establecer criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información, a que se refiere el artículo 10º del Reglamento para la Administración de los Riesgos de Operación, aprobado mediante la Resolución SBS Nº 006-2002 del 4 de enero de 2002, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º .- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

b. Ley General: Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

c. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada. [18]

d. Reglamento: Reglamento para la Administración de los Riesgos de Operación aprobado por Resolución SBS N° 006-2002 del 4 de enero de 2002.

e. Riesgo de operación: Entiéndase por riesgo de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación. 1

f. Riesgos de tecnología de información: Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.

g. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

h. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

---

[18] Literales e. y g. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005

Responsabilidad de la empresa

Artículo 3°.- Las empresas deben establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de

información, incidiendo en los procesos críticos asociados a dicho riesgo, considerando las disposiciones contenidas en la presente norma, en el Reglamento, y en el Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.
La administración de dicho riesgo debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

I. Eficacia. La información debe ser relevante y pertinente para los objetivos de negocio y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la empresa.
II. Eficiencia. La información debe ser producida y entregada de forma productiva y económica.
III. Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
IV. Integridad. La información debe ser completa, exacta y válida.
V. Disponibilidad. La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.
VI. Cumplimiento normativo. La información debe cumplir con los criterios y estándares internos de la empresa, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

6.1.2.- ESTRUCTURA ORGANIZACIONAL Y PROCEDIMIENTOS

Artículo 4°.- Las empresas deben definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan.

6.1.3.- ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN

Artículo 5º.- Las empresas deberán establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante "Plan de Seguridad de la información - (PSI [19])".

---

[19] PSI: Plan de Seguridad de la Información.

El PSI debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.

Las actividades mínimas que deben desarrollarse para implementar el PSI, son las siguientes:

a. Definición de una política de seguridad.
b. Evaluación de riesgos de seguridad a los que está expuesta la información
c. Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
d. Plan de implementación de los controles y procedimientos de revisión periódicos.
e. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Las empresas bancarias y las empresas de operaciones múltiples que accedan al módulo 3 de operaciones a que se refiere el artículo 290º de la Ley General deberán contar con una función de seguridad a dedicación exclusiva.

Subcontratación (outsourcing)

Artículo 6º.- La empresa es responsable y debe verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en la Primera Disposición Final y Transitoria del Reglamento. Asimismo, la empresa debe asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Las empresas que a la fecha de vigencia de la presente norma se encontrasen en la situación antes señalada, deberán solicitar la autorización correspondiente. Para la evaluación de estas autorizaciones, las empresas deberán presentar documentación que sustente lo siguiente:

a) La forma en que la empresa asegurará el cumplimiento de la presente circular y la Primera Disposición Final y Transitoria del Reglamento.
b) La empresa, así como los representantes de quienes brindarán el servicio de procesamiento en el exterior, deberán asegurar adecuado acceso a la información con fines de supervisión, en tiempos razonables y a solo requerimiento.

Aspectos de la seguridad de información

Artículo 7°.- Para la administración de la seguridad de la información, las empresas deberán tomar en consideración los siguientes aspectos:

7.1 Seguridad lógica

Las empresas deben definir una política para el control de accesos, que incluya los criterios para la concesión y administración de los accesos a los sistemas de información, redes y sistemas operativos, así como los derechos y atributos que se confieren.
Entre otros aspectos, debe contemplarse lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios. Revisiones periódicas deben efectuarse sobre los derechos concedidos a los usuarios.
b) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
c) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
d) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.
e) Usuarios remotos y computación móvil.

7.2 Seguridad de personal

Las empresas deben definir procedimientos para reducir los riesgos asociados al error humano , robo, fraude o mal uso de activos, vinculados al riesgo de tecnología de información. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la definición de roles y responsabilidades establecidos sobre la seguridad de información, verificación de antecedentes, políticas de rotación y vacaciones, y entrenamiento.

7.3 Seguridad física y ambiental

Las empresas deben definir controles físicos al acceso, daño o interceptación de información. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.
Se definirán medidas adicionales para las áreas de trabajo con necesidades especiales de seguridad, como los centros de procesamiento, entre otras zonas en que se maneje información que requiera de alto nivel de protección.

7.4 Clasificación de seguridad

Las empresas deben realizar un inventario periódico de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en

caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

Administración de las operaciones y comunicaciones

Artículo 8º.- Las empresas deben establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

- Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
- Control sobre los cambios del ambiente de desarrollo al de producción.
- Separación de funciones para reducir el riesgo de error o fraude.
- Separación del ambiente de producción y el de desarrollo.
- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
- Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
- Seguridad sobre correo electrónico.
- Seguridad sobre banca electrónica.

Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad

Artículo 9º.- Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente .
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

Procedimientos de respaldo

Artículo 10º.- Las empresas deben establecer procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con lo requerido en el Plan de Continuidad.

La empresa debe conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

Planeamiento para la continuidad de negocios

Artículo 11º.- Las empresas, bajo responsabilidad de la Gerencia y el Directorio, deben desarrollar y mantener un "Plan de Continuidad de Negocios" (PCN), que tendrá como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

6.1.4.- CRITERIOS PARA EL DISEÑO E IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIOS

Artículo 12º.- Para el desarrollo del PCN se debe realizar previamente una evaluación de riesgos asociados a la seguridad de la información. Culminada la evaluación, se desarrollarán sub-planes específicos para mantener o recuperar los procesos críticos de negocios ante fallas en sus activos, causadas por eventos internos (virus, errores no esperados en la implementación, otros), o externos (falla en las comunicaciones o energía, incendio, terremoto, proveedores, otros).

Prueba del Plan de Continuidad de Negocios

Artículo 13º.- La prueba del PCN es una herramienta de la dirección para controlar los riesgos sobre la continuidad de operación y sobre la disponibilidad de la información, por lo que la secuencia, frecuencia y profundidad de la prueba del PCN, deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada empresa.

En todos los casos, mediante una única prueba o una secuencia de ellas, según lo considere adecuado cada empresa de acuerdo a su evaluación de riesgos, los principales aspectos del PCN deberán ser probados cuando menos cada dos años.

Anualmente, dentro del primer mes del ejercicio, se enviará a la Superintendencia el programa de pruebas correspondiente, en que se indicará las actividades a realizar durante el ciclo de 2 años y una descripción de los objetivos a alcanzar en el año que se inicia.

Cumplimiento normativo

Artículo 14º.- La empresa deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

Privacidad de la información

Artículo 15º .- Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme la normatividad vigente sobre la materia.

Auditoría Interna y Externa

Artículo 16º.- La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la presente norma.

Asimismo, las Sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información, considerando asimismo, el cumplimiento de lo dispuesto en la presente norma.

6.1.5.- AUDITORÍA DE SISTEMAS

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria del Reglamento.

Las empresas autorizadas para operar en otros módulos, para la verificación del cumplimiento antes señalado, deberán asegurar una combinación apropiada de auditoría interna y/o externa, compatible con el nivel de complejidad y perfil de riesgo de la empresa. La Superintendencia dispondrá un tratamiento similar a las empresas pertenecientes al módulo 3, cuando a su criterio la complejidad de sus sistemas informáticos y su perfil de riesgo así lo amerite.

Información a la Superintendencia

Artículo 18°.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13° del Reglamento, deberá incluir los riesgos de operación asociados a la tecnología de información, como parte integral de dicha evaluación, para lo cual se sujetará a lo dispuesto en dicho Reglamento y a lo establecido en la presente norma.

Sanciones

Artículo 19°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plan de adecuación

Artículo 20°.- En el Plan de Adecuación señalado en el segundo párrafo de la Cuarta Disposición Final y Transitoria del Reglamento, las empresas deberán incluir un sub-plan para la adecuación a las disposiciones contenidas en la presente norma.

Plazo de adecuación

Artículo 21°.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vence el 30 de junio de 2003

Atentamente,

SOCORRO HEYSEN ZEGARRA

Superintendente de Banca y Seguros (e)

7.3. ANEXO 3: RESOLUCIÓN SBB N°37-2008

Lima, 10 de enero de 2008

Resolución S.B.S.

N° 37 -2008

El Superintendente de Banca, Seguros y

Administradoras Privadas de Fondos de Pensiones:

CONSIDERANDO:

Que, el numeral 2 del artículo 134° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley Nº 26702 y sus modificatorias, en adelante Ley General, dispone como un medio de protección al ahorrista, supervisar que las empresas del sistema financiero se encuentren debidamente organizadas, así como administradas por personal idóneo;

Que, la Asociación Internacional de Supervisores de Seguros – IAIS – dispone en el Principio Básico de Seguros 18 "Evaluación y administración de riesgos" que la autoridad supervisora requiere que las aseguradoras reconozcan el rango de riesgos que ellos enfrentan y que los evalúen y administren con efectividad;

Que, conforme al inciso e) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, es atribución y obligación de la Superintendencia fiscalizar a las AFP en el cumplimiento de las disposiciones legales y directivas administrativas que les rigen, razón por la cual resulta conveniente incluirlas dentro del ámbito de aplicación de la Gestión Integral de Riesgos;

Que, de conformidad con el artículo 290° de la Ley General, constituye un requisito para la ampliación de las operaciones de las empresas del sistema financiero, contar con controles internos adecuados para las nuevas operaciones;

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con una Gestión Integral de Riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios;

Que, dicha Gestión Integral de Riesgos debe estar diseñada para contar con un entorno interno apropiado, desarrollar una adecuada determinación de objetivos, implementar una oportuna identificación, evaluación, tratamiento y control de riesgos, así como elaborar los reportes pertinentes y efectuar un adecuado monitoreo;

Que, es necesario revisar los criterios previstos en el Reglamento del Sistema de Control interno a fin de hacerlo compatible con las mejores prácticas internacionales para el desarrollo de una Gestión Integral de Riesgos, tomando como referencia, entre otros documentos, al Marco Integrado para la Gestión de Riesgos Corporativos, publicado por el Committee of Sponsoring Organizations of the Treadway Commission (COSO); y hacerlo extensivo al conjunto de las empresas supervisadas bajo un único marco de referencia;

Estando a lo opinado por las Superintendencias Adjuntas de Banca y Microfinanzas, Seguros, Administradoras Privadas de Fondos de Pensiones, Riesgos, Asesoría Jurídica, así como por la Gerencia de Estudios Económicos; y,

En uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento de la Gestión Integral de Riesgos, que forma parte de la presente Resolución.

Artículo Segundo.- La presente Resolución entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de diciembre de 2008, fecha a partir de la cual quedarán sin efecto la Resolución SBS Nº 1040-99, así como todas aquellas disposiciones que se le opongan de manera total o parcial.

Artículo Tercero.- Incorpórese el procedimiento N° 110 "Autorizaciones especiales sobre la Gestión Integral de Riesgos" del Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia de Banca, Seguros y AFP aprobado mediante Resolución SBS N° 131-2002, conforme el texto que se adjunta a la presente Resolución.

Regístrese, comuníquese y publíquese,

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

REGLAMENTO DE LA

GESTIÓN INTEGRAL DE RIESGOS

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1º.- Alcance

El presente Reglamento será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Artículo 2º.- Definiciones

Para la aplicación de la presente Norma deberán considerarse las siguientes definiciones:

a) Apetito por el riesgo.- El nivel de riesgo que la empresa está dispuesta a asumir en su búsqueda de rentabilidad y valor.
b) Casa Matriz.- Se refiere a la sociedad principal o a la que ejerza el control en un conglomerado financiero o mixto.
c) Control interno.- Un proceso, realizado por el Directorio, la Gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y

eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones.

d) Directorio.- Toda referencia al Directorio, entiéndase realizada también a cualquier órgano equivalente.

e) Director Independiente.- Un director que es seleccionado por su prestigio profesional y que no se encuentra vinculado con la administración de la empresa ni con el grupo económico de la misma.

f) Evento.- Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

g) Impacto.- La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado severidad.

h) Manuales de gestión de riesgos.- Documentos que contienen las funciones, responsabilidades, políticas, metodologías y procedimientos dispuestos para la identificación, evaluación, tratamiento, control, reporte y monitoreo de los riesgos de la empresa.

i) Manuales de organización y funciones.- Documentos que detallan la estructura orgánica de la empresa, los objetivos y funciones de sus unidades, así como las obligaciones y responsabilidades de su personal.

j) Manuales de políticas y procedimientos.- Documentos que contienen funciones, responsabilidades, las políticas, metodologías y procedimientos establecidos por la empresa para la realización de las actividades de cada una de las unidades con las que cuenta, incluyendo las que corresponden a la gestión de riesgos.

k) Probabilidad.- La posibilidad de la ocurrencia de un evento que usualmente es aproximada mediante una distribución estadística. En ausencia de información suficiente, o donde no resulta posible obtenerla, se puede aproximar mediante métodos cualitativos.

l) Proceso.- Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.

m) Riesgo.- La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa.

n) Seguridad razonable.- Se refiere al nivel de seguridad que una empresa puede tener en alcanzar sus objetivos, considerando que siempre es posible que se produzcan desviaciones o impactos financieros importantes que no sean prevenidos o detectados, dada la incertidumbre inherente al futuro.

o) Subcontratación.- Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizada por la empresa contratante.

p) Superintendencia.- Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

q) Tolerancia al riesgo.- El nivel de variación que la empresa está dispuesta a asumir en caso de desviación a los objetivos empresariales trazados.

CAPÍTULO II

GESTIÓN INTEGRAL DE RIESGOS

Artículo 3º.- Gestión Integral de Riesgos

La Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos.

La Gestión Integral de Riesgos considera las siguientes categorías de objetivos:

a) Estrategia.- Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
b) Operaciones.- Son objetivos vinculados al uso eficaz y eficiente de los recursos.
c) Información.- Son objetivos vinculados a la confiabilidad de la información suministrada.
d) Cumplimiento.- Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

Las empresas deben efectuar una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

Artículo 4º.- Componentes

La Gestión Integral de Riesgos puede descomponerse en componentes, que se encuentran presentes en diverso grado, según se analice la totalidad de la empresa, una línea de negocio, un proceso o una unidad organizativa. La empresa podrá contar con una descomposición propia, que se adapte a su organización, pero ella debe considerar los principales elementos descritos a continuación:

a) Ambiente interno.- Que comprende, entre otros, los valores éticos, la idoneidad técnica y moral de sus funcionarios; la estructura organizacional; y las condiciones para la asignación de autoridad y responsabilidades.

b) Establecimiento de objetivos.- Proceso por el que se determinan los objetivos empresariales, los cuales deben encontrarse alineados a la visión y misión de la empresa, y ser compatibles con la tolerancia al riesgo y el grado de exposición al riesgo aceptado.

c) Identificación de riesgos.- Proceso por el que se identifican los riesgos internos y externos que pueden tener un impacto negativo sobre los objetivos de la empresa. Entre otros aspectos, considera la posible interdependencia entre eventos, así como los factores influyentes que los determinan.

d) **Evaluación de riesgos**.- Proceso por el que se evalúa el riesgo de una empresa, actividad, conjunto de actividades, área, portafolio, producto o servicio; mediante técnicas cualitativas, cuantitativas o una combinación de ambas.

e) **Tratamiento**.- Proceso por el que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de tolerancia al riesgo definido.

f) **Actividades de control.-** Proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están preferentemente incorporadas en los procesos de negocio y las actividades de apoyo. Incluye los controles generales así como los de aplicación a los sistemas de información, además de la tecnología de información relacionada. Buscan la eficacia y efectividad de las operaciones de la empresa, la confiabilidad de la información financiera u operativa, interna y externa, así como el cumplimiento de las disposiciones legales que le sean aplicables.

g) **Información y comunicación**.- Proceso por el que se genera y transmite información apropiada y oportuna a la dirección, la gerencia, el personal, así como a interesados externos tales como clientes, proveedores, accionistas y reguladores, entre ellos esta Superintendencia. Esta información es interna y externa, y puede incluir información de gestión, financiera y operativa.

h) **Monitoreo.-** Proceso que consiste en la evaluación del adecuado funcionamiento de la Gestión Integral de Riesgos y la implementación de las modificaciones que sean requeridas. El monitoreo debe realizarse en el curso normal de las actividades de la empresa, y complementarse por evaluaciones independientes o una combinación de ambas. Incluye el reporte de las deficiencias encontradas y su corrección.

Artículo 5°.- Tipos de riesgos

Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos. Algunos riesgos pueden encontrarse asociados a una actividad en particular, como en el proceso de inversión, que se encuentra expuesto a riesgos de crédito, de mercado, de operación, entre otros. A continuación se enumera una lista no limitativa de los diversos tipos de riesgos a que está expuesta una empresa:

a) **Riesgo de crédito**

La posibilidad de pérdidas por la imposibilidad o falta de voluntad de los deudores o contrapartes, o terceros obligados para cumplir completamente sus obligaciones contractuales registradas dentro o fuera del balance general.

b) **Riesgo estratégico**

La posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

c) Riesgo de liquidez

La posibilidad de pérdidas por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descalces de flujos de efectivo, así como por no poder cerrar rápidamente posiciones abiertas, en la cantidad suficiente y a un precio razonable.

d) Riesgo de mercado

La posibilidad de pérdidas en posiciones dentro y fuera de balance derivadas de fluctuaciones en los precios de mercado.

e) Riesgo operacional

La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación**.**

f) Riesgo de seguro

La posibilidad de pérdidas por las bases técnicas o actuariales empleadas en el cálculo de las primas y de las reservas técnicas de los seguros, insuficiencia de la cobertura de reaseguros, así como el aumento inesperado de los gastos y de la distribución en el tiempo de los siniestros. Se le conoce también como riesgo técnico.

g) Riesgo de reputación

La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.

Artículo 6º.- Prácticas cuestionables

La empresa deberá establecer los sistemas internos apropiados que faciliten la oportuna denuncia e investigación de las actividades ilícitas, fraudulentas, identificadas por cualquier trabajador de la empresa o por alguna persona que interactúa con ésta. Dichas actividades deberán ser reportadas a la unidad de auditoría interna, para lo cual la empresa implementará procedimientos que permitan mantener la confidencialidad del denunciante. En el caso de que los hechos sean significativos, la unidad de auditoría interna deberá informar al Comité de Auditoría y a la Superintendencia.

Artículo 7°.- Relación de la Gestión Integral de Riesgos y el Control Interno

La Gestión Integral de Riesgos incluye al control interno del que es parte integral. La Gestión Integral de Riesgos expande y desarrolla los conceptos de control interno en una forma más amplia y sólida, con un mayor énfasis en el riesgo.

El objetivo de confiabilidad en la información financiera del control interno se encuentra principalmente referido a la confiabilidad de los estados financieros. En la Gestión Integral de Riesgos, este objetivo es expandido para incluir todos los reportes e informes generados por las empresas, tanto internos como externos. Entre ellos los usados por la Dirección y la Gerencia, aquellos enviados a terceros, información entregada a los reguladores, así como a accionistas y otros grupos de interés. El alcance también incorpora la información no financiera.

De acuerdo a lo indicado en el artículo 3°, una nueva categoría de objetivos referidos a la estrategia, y las categorías de objetivos referidos a las operaciones, información y cumplimiento deben encontrarse alineados a la estrategia. La Gestión Integral de Riesgos es aplicada también en la selección de objetivos.

CAPÍTULO III

EL DIRECTORIO Y LA GERENCIA

Artículo 8º.- Responsabilidad del Directorio

El Directorio es responsable de establecer una gestión integral de riesgos y de propiciar un ambiente interno que facilite su desarrollo adecuado. Entre sus responsabilidades específicas están:

a) Aprobar las políticas generales que guíen las actividades de la empresa en la gestión de los diversos riesgos que enfrenta.
b) Seleccionar una plana gerencial con idoneidad técnica y moral, que actúe de forma prudente y apropiada en el desarrollo de sus negocios y operaciones, así como en el cumplimiento de sus responsabilidades.
c) Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión Integral de Riesgos, a fin de contar con la infraestructura, metodología y personal apropiado.
d) Establecer un sistema de incentivos que fomente el adecuado funcionamiento de una gestión integral de riesgos y que no favorezca la toma inapropiada de riesgos.
e) Aprobar los manuales de organización y funciones, de políticas y procedimientos y demás manuales de la empresa.
f) Aprobar políticas generales para las responsabilidades a cargo de la empresa, incluyendo:
    f.1 La administración prudente y según los acuerdos establecidos o la regulación aplicable, de los activos en depósito y en custodia, administrados o invertidos por cuenta de clientes y terceros, evitando conflictos de interés.
    f.2 Asegurar razonablemente que los consejos de inversión o similares realizados en su ámbito, son presentados con la información apropiada, al tener en cuenta la tolerancia al riesgo y expectativa de rendimiento del cliente.

g) Establecer los objetivos empresariales, evaluar y aprobar sus planes de negocios con debida consideración a los riesgos asociados.

h) Conocer los principales riesgos afrontados por la entidad estableciendo, cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.

i) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

j) Asegurar razonablemente que el patrimonio contable de la empresa sea suficiente para enfrentar los riesgos a los que está expuesto, para lo cual debe conocer las necesidades de capital y establecer políticas de gestión que apoye las necesidades de la empresa, cumpliendo con los requerimientos regulatorios de manera apropiada.

k) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de los riesgos a que está expuesta, y que los principales riesgos se encuentran bajo control dentro de los límites que han establecido.

Artículo 9°.- Declaración de cumplimiento del Directorio

El Directorio es responsable de evaluar el adecuado funcionamiento de los criterios definidos en la presente normativa. Anualmente, el Directorio suscribirá una Declaración de cumplimiento, que contendrá cuando menos lo indicado a continuación, pudiendo la Superintendencia definir criterios mínimos adicionales mediante oficio múltiple de aplicación general:

a) Que el Directorio conoce los estándares previstos en la presente norma, así como sus responsabilidades.

b) Que la empresa cuenta con una gestión apropiada de sus riesgos para la complejidad y tamaño de la empresa, así como de los criterios indicados en la presente norma, con la excepción de posibles deficiencias identificadas y comunicadas en la declaración.

c) Que el Directorio ha tomado conocimiento de la información de la Gerencia, de los informes del Comité de Auditoría, del Comité de Riesgos, de Auditoría Externa, y de otra información que el Directorio considere relevante, y que las medidas correctivas dispuestas consten en las actas correspondientes.

Esta declaración será suscrita en un plazo que no excederá de ciento veinte (120) días calendario posterior al ejercicio anual, debiendo estar a disposición de esta Superintendencia.

Artículo 10º.- Responsabilidad de la Gerencia

La gerencia general tiene la responsabilidad de implementar la Gestión Integral de Riesgos conforme a las disposiciones del Directorio, además de las responsabilidades dadas por otras normas.

La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades.

Los gerentes de las unidades organizativas de negocios o de apoyo, en su ámbito de acción, tienen la responsabilidad de administrar los riesgos relacionados al logro de los objetivos de sus unidades. Entre sus responsabilidades específicas están:

a) Asegurar la consistencia entre las operaciones y los niveles de tolerancia al riesgo definidos aplicables a su ámbito de acción.
b) Asumir, ante el gerente de nivel inmediato superior, los resultados de la gestión de riesgos correspondiente a su unidad; y así hasta llegar al gerente general que tiene esta responsabilidad ante el Directorio.

CAPÍTULO IV

LOS COMITÉS DEL DIRECTORIO

Artículo 11º.- Comités

El Directorio podrá constituir los comités que considere necesarios con la finalidad de dar cumplimiento a las disposiciones contenidas en el presente reglamento y a las responsabilidades señaladas por el artículo 8° anteriormente citado.

Para el caso de las empresas de operaciones múltiples y las empresas de seguros a las que se refiere el artículo 16° de la Ley General, así como para las AFP, será obligatoria la constitución de un comité de auditoría y un comité de riesgos. En el caso de aquellas empresas que no se encuentren obligadas a constituir los comités y que, además, decidan no hacerlo, todas las funciones atribuidas a el(los) comité(s) no constituido(s) serán asumidas por el Directorio.

Artículo 12°.- Reglamento de los Comités

Los Comités constituidos por el Directorio deberán contar con un Reglamento que contendrá las políticas y procedimientos necesarios para el cumplimiento de sus funciones. Dicho reglamento establecerá, entre otros aspectos, los criterios para evitar conflictos de intereses, incompatibilidad de funciones, la periodicidad de sus reuniones, sus actividades programadas, la información que debe ser remitida, así como la forma como reportará al Directorio. Los acuerdos adoptados en las reuniones deberán constar en un Libro de Actas.

SUB-CAPÍTULO I

COMITÉ DE RIESGOS

Artículo 13º.- Conformación del comité de riesgos

El comité de riesgos deberá estar conformado por al menos un miembro del Directorio, y se organizará como un comité integral, que deberán abarcar las decisiones que atañen a los riesgos significativos a los que esté expuesta la empresa. Los integrantes del Comité de Riesgos deben tener los conocimientos y la experiencia necesaria para cumplir adecuadamente sus funciones.

El Directorio podrá crear los comités de riesgos especializados que considere necesarios, en razón del tamaño y complejidad de las operaciones y servicios de la empresa.

Artículo 14°.- Funciones del comité de riesgos

El comité de riesgos, por delegación del Directorio y dentro de los límites que éste fije, podrá asumir las siguientes funciones:

a) Aprobar las políticas y la organización para la Gestión Integral de Riesgos, así como las modificaciones que se realicen a los mismos.
b) Definir el nivel de tolerancia y el grado de exposición al riesgo que la empresa está dispuesta a asumir en el desarrollo del negocio.
c) Decidir las acciones necesarias para la implementación de las acciones correctivas requeridas, en caso existan desviaciones con respecto a los niveles de tolerancia al riesgo y a los grados de exposición asumidos.
d) Aprobar la toma de exposiciones que involucren variaciones significativas en el perfil de riesgo de la empresa o de los patrimonios administrados bajo responsabilidad de la empresa.
e) Evaluar la suficiencia de capital de la empresa para enfrentar sus riesgos y alertar de las posibles insuficiencias.
f) Proponer mejoras en la Gestión Integral de Riesgos.

SUB-CAPÍTULO II

COMITÉ DE AUDITORÍA

Artículo 15º.- Conformación del comité de auditoría

El comité de auditoría deberá estar conformado por miembros del Directorio que no realicen actividades de gestión en la empresa. Dicho comité tendrá como mínimo tres (3) miembros, debiendo renovarse cada tres (3) años, al menos, uno de ellos. Los integrantes del comité de auditoría deben tener los conocimientos y la experiencia necesarios para cumplir adecuadamente sus funciones.

Para el caso de las empresas de operaciones múltiples y las empresas de seguros a las que se refiere el artículo 16° de la Ley General; así como para las AFP; el comité de auditoría deberá estar conformado por al menos un director independiente.

Artículo 16°.- Funciones del comité de auditoría

El comité de auditoría tiene como propósito principal vigilar que los procesos contables y de reporte financiero sean apropiados, así como evaluar las actividades realizadas por los auditores internos y externos.

Entre sus principales funciones están:

a) Vigilar el adecuado funcionamiento del sistema de control interno;
b) Informar al Directorio sobre la existencia de limitaciones en la confiabilidad de los procesos contables y financieros;
c) Vigilar y mantener informado al Directorio sobre el cumplimiento de las políticas y procedimientos internos y sobre la detección de problemas de control y administración interna, así como de las medidas correctivas implementadas en función de las evaluaciones realizadas por la unidad de auditoría interna, los auditores externos y esta Superintendencia;
d) Definir los criterios para la selección y contratación de los auditores externos, evaluar su desempeño así como determinar los informes complementarios que requieran para el mejor desempeño de sus funciones o el cumplimiento de requisitos legales, salvo en aquellos casos en los que el comité de auditoría de la casa matriz asuma las funciones de definir los criterios para la selección y contratación de los auditores externos, así como la evaluación de sus desempeño; y,
e) Definir los criterios para la selección y contratación del auditor interno y sus principales colaboradores, fijar su remuneración y evaluar su desempeño, así como su régimen de incentivos monetarios, salvo que dichas funciones sean asumidas por el comité de auditoría de la casa matriz.

CAPÍTULO V

UNIDAD DE RIESGOS

Artículo 17º.- Unidad de Riesgos

La Gestión Integral de Riesgos requiere que las empresas se organicen de acuerdo a su complejidad y líneas de negocio en que operan. En este sentido, las empresas podrán contar

con una unidad centralizada o con unidades especializadas en la gestión de riesgos específicos, de acuerdo a la naturaleza de las operaciones y la estructura de la empresa, siempre que cuando sean éstas tomadas en su conjunto, permitan la implementación de los criterios previstos en la presente norma.

La Superintendencia podrá requerir la creación de una unidad de riesgos integral en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Siempre que no sea requerido por la normativa vigente, cuando no exista una unidad de riesgos especializada, y en ausencia de delegación del Directorio, se entenderá que estas funciones han sido asignadas a la gerencia general.

Los integrantes de la Unidad de Riesgos deberán poseer la experiencia y conocimientos que les permitan el apropiado cumplimiento de sus funciones, para lo cual deberá establecerse un plan de capacitación que será presentado al directorio anualmente.

Artículo 18º.- Funciones de la Unidad de Riesgos

La Unidad de Riesgos deberá participar en el diseño y permanente adecuación de los manuales de gestión de riesgos y demás normas internas que tengan por objeto definir las responsabilidades de las unidades de negocios y sus funcionarios en el control de riesgos de la empresa.

La Unidad de Riesgos es la encargada de apoyar y asistir a las demás unidades de la empresa para la realización de una buena gestión de riesgos en sus áreas de responsabilidad, y para ello debe ser independiente de las unidades de negocios.

Las principales responsabilidades de la unidad de riesgos son las siguientes:

a) Proponer las políticas, procedimientos y metodologías apropiadas para la Gestión Integral de Riesgos en la empresa, incluyendo los roles y responsabilidades;
b) Velar por una Gestión Integral de Riesgos competente, promoviendo el alineamiento de las medidas de tratamiento de los riesgos de la empresa con los niveles de tolerancia al riesgo y el desarrollo de controles apropiados;
c) Guiar la integración entre la gestión de riesgos, los planes de negocio y las actividades de gestión empresarial;
d) Establecer un lenguaje común de gestión de riesgos basado en las definiciones de esta norma y de los demás reglamentos aplicables;
e) Estimar los requerimientos patrimoniales que permitan cubrir los riesgos que enfrenta la empresa, así como los requerimientos regulatorios, de ser el caso. Además, alertar sobre las posibles insuficiencias de patrimonio efectivo para cubrir los riesgos identificados; y,

f) Informar a la gerencia general y al comité de riesgos los aspectos relevantes de la gestión de riesgos para una oportuna toma de decisiones.

g)

Artículo 19º.- Jefe de la Unidad de Riesgos

El jefe de la Unidad de Riesgos deberá tener apropiada formación académica y experiencia relevante, quién debe coordinar permanentemente con la gerencia, el comité de riesgos, el comité de auditoría, los comités especializados, las unidades de negocio y de apoyo, así como con esta Superintendencia, en cuanto a la Gestión Integral de Riesgos realizada por la empresa.

Además, es responsable de informar al Directorio, comités respectivos y a las áreas de decisión correspondientes, sobre los riesgos, el grado de exposición al riesgo aceptado y la gestión de éstos, de acuerdo a las políticas y procedimientos establecidos por la empresa.

Los criterios mencionados son de aplicación a los jefes de las unidades de riesgos especializadas, en caso que no exista una unidad centralizada.

El jefe de la Unidad de Riesgos, en caso que la Unidad de Riesgos sea centralizada, deberá tener nivel gerencial.

Artículo 20º.- Informe Anual de Riesgos

La Unidad de Riesgos deberá elaborar al cierre de cada ejercicio, un informe anual de riesgos, que incluya el plan de actividades para el ejercicio siguiente.

Posteriormente, mediante Oficio Múltiple, la Superintendencia podrá definir la estructura mínima del informe anual de riesgos, informes parciales por riesgos, informes periódicos de situación, así como su presentación por medios electrónicos.

CAPÍTULO VI

SUBCONTRATACIÓN

Artículo 21º.- Subcontratación

Las empresas y las personas cuyas responsabilidades se hayan determinado en el presente reglamento y demás normas, asumen plena responsabilidad sobre los resultados de los procesos

subcontratados con terceros, pudiendo ser sancionados por su incumplimiento. Asimismo deben asegurarse que se mantenga reserva y confidencialidad sobre la información que pudiera serles proporcionada.

En toda subcontratación significativa, un análisis formal de los riesgos asociados deberá ser realizado y puesto en conocimiento del Directorio para su aprobación. Se entenderá por significativa aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

La subcontratación de una o más funciones de la gestión de riesgos será considerada como significativa para fines de este reglamento.

Las empresas deberán asegurarse de que en los casos de subcontratación significativa, los contratos suscritos con los proveedores correspondientes incluyan cláusulas que faciliten una adecuada revisión de la respectiva prestación por parte de las empresas, de la Unidad de Auditoría Interna, de la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

En el caso de subcontratación significativa del servicio de auditoría interna, se sujetará a lo establecido en el Reglamento de Auditoría Interna.

CAPÍTULO VII

ROL DE LA AUDITORÍA INTERNA Y EXTERNA

Artículo 22º.- Unidad de Auditoría Interna

La Auditoría Interna, desempeña un rol independiente a la gestión, que vigila la adecuación de la Gestión Integral de Riesgos, debiendo sujetarse a las disposiciones específicas que regulan su actividad en el Reglamento de Auditoría Interna.

Artículo 23º.- Auditores Externos

La Auditoría Externa es independiente a la empresa y tiene como función principal la evaluación de la confiabilidad de la información financiera, debiendo sujetarse a las disposiciones específicas que regulan su actividad en el Reglamento de Auditoría Externa.

DISPOSICIONES FINALES Y TRANSITORIAS

Primera.- Autorizaciones especiales

En caso justificado, la empresa podrá solicitar a la Superintendencia, exoneración específica de alguno de los requerimientos normativos indicados en este Reglamento, adjuntando la documentación de sustento correspondiente respecto a alguno de los siguientes requisitos en lo que sea apropiado para la debida evaluación de esta Superintendencia:

a) La empresa cuenta con un sistema de gestión que, tomado en su conjunto, cumple sustancialmente con los criterios mínimos indicados en la presente normativa.
b) Cuando la organización recibe diversos servicios de su casa matriz, de la empresa que ejerce el control directo o indirecto, o de la que tenga responsabilidad directa de la operación, siempre que tomados en su conjunto igualen o excedan los criterios previstos en el Reglamento.
c) Cuando por limitación legal, le resulta imposible cumplir con parte de la normativa.
d) Cuando se requiera por fines de estandarización y lenguaje común con su casa matriz, o con la empresa que ejerza el control directo o indirecto o la que tenga responsabilidad directa de la operación, a fin de aprovechar ventajas metodológicas, como por ejemplo conocimiento y experiencia demostrada en diseño e implementación de gestión de riesgos acorde con buenas prácticas, infraestructura, y métodos y procedimientos que demuestren un claro conocimiento y gestión de los riesgos a los que están expuestos.

Las funciones del comité de auditoría podrán ser asumidas por la Casa Matriz, sólo si las actividades del conglomerado al que pertenezca una empresa supervisada no se desarrollen principalmente en el Perú y bajo autorización expresa de esta Superintendencia. Para ello las empresas deberán solicitar autorización indicando la forma en que se cumplirán las disposiciones establecidas en el presente Reglamento, obligación que permanece mientras se encuentre vigente la autorización.

Las Resoluciones de autorización correspondientes, serán publicadas en el Diario Oficial El Peruano.

Esta Superintendencia podrá suspender en cualquier momento las autorizaciones especiales concedidas a que hace referencia esta norma, cuando en el ejercicio de su función supervisora observe que las circunstancias lo ameritan, que la empresa ha incumplido con las obligaciones

previstas, o que la autorización concedida no ha contribuido a una mejora de su práctica de gestión de riesgos, lo que comunicará a la empresa mediante oficio.

Segunda.- Transparencia

La empresa deberá revelar en su Memoria Anual, cuando menos una descripción general de las principales características de la Gestión Integral de Riesgos.

Tercera.- Plazo y Plan de Adecuación

En un plazo que no excederá de noventa (90) días calendario de haberse publicado el presente Reglamento, las empresas deberán remitir a esta Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Cuarta.- Declaración del Directorio

La primera declaración a que hace referencia el artículo 9° será exigible, por el ejercicio correspondiente al 2008, lo cual se encontrará a disposición de esta Superintendencia dentro de los 120 días calendario del 2009.

7.4. ANEXO 4: EVALUACIÓN DE RIESGOS ASOCIADOS A TECNOLOGÍA DE INFORMACIÓN

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION
Factor Crítico / Proceso en Evaluación:		Desarrollo de Sistemas

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	DS001	Ausencia de requerimientos funcionales de validación de la información de entrada para generación o modificación de sistemas	2: Medio	3: Medio Alto	MEDIO ALTO	No se está validando ni realizando pruebas de validación de información de entrada, se utiliza información continua	0: No Controlado	MEDIO ALTO
002	DS002	Ausencia de planeamiento de sistemas de información	2: Medio	4: Alto	MEDIO ALTO	Se está desarrollando el PETI	2: Parcial	MEDIO BAJO
003	DS003	Ausencia o deficiencia de metodología de desarrollo de sistemas	1: Medio Bajo	3: Medio Alto	MEDIO	La metodología de desarrollo de sistemas está en proceso de formalización y despliegue	1: Bajo	MEDIO
004	DS004	Ausencia o no utilización de estándares de desarrollo	2: Medio	2: Medio	MEDIO	Aun no se han establecido mecanismos de procesos estándares.	0: No Controlado	MEDIO
005	DS005	Ausencia de documentos de sustento en las solicitudes de nuevos sistemas	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Las solicitudes de generación o modificación tienen un proceso de "sentido Comun" con firmas del usuarios solicitante, no existen formatos	2: Parcial	MEDIO BAJO
006	DS006	Ausencia de procesos formales de control de cambios	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Existen niveles de control de cambios, pero no están estandarizados ni formalizados, dependen mucho del responsable y del jefe de división	2: Parcial	MEDIO BAJO
007	DS007	Fallas en la implementación de cambios a sistemas desarrollados	1: Medio Bajo	3: Medio Alto	MEDIO	Los cambios en los sistemas se prueban antes del pase a producción	3: Razonable	BAJO
008	DS008	Ausencia de auditorías de calidad y pruebas a nuevos sistemas	1: Medio Bajo	3: Medio Alto	MEDIO	Los cambios en los sistemas se prueban antes del pase a producción y son revisados por auditoria	3: Razonable	BAJO
009	DS009	Ausencia de tecnología de administración de proyectos	2: Medio	2: Medio	MEDIO	Se tiene un módulo de administracion de proyectos, pero no se está utilizando	1: Bajo	MEDIO
010	DS010	Información crítica no protegida en los sistemas de información	3: Medio Alto	2: Medio	MEDIO	La información crítica se mantiene aislada, sin embargo se realiza por buenas prácticas, aun no se tiene establecida una clasificación adecuada.	2: Parcial	MEDIO BAJO

Tabla 6: Riesgos Asociados a TI: (Proceso: Desarrollo de Sistemas)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Servicios Prestados por Terceros

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	ST001	Mal uso de información del banco por parte de terceras empresas	1: Medio Bajo	4: Alto	MEDIO ALTO	No existen políticas de acuerdos de confidencialidad formal, el control es muy informal	1: Bajo	MEDIO
002	ST002	Fraude	1: Medio Bajo	3: Medio Alto	MEDIO	Se hace seguimiento y control en base a sentido común de los responsables, no existen controles formales	2: Parcial	MEDIO BAJO
003	ST003	Robo y divulgación de información	2: Medio	3: Medio Alto	MEDIO ALTO	No se están ejecutando controles	0: No Controlado	MEDIO ALTO
004	ST004	Contratos sin inclusión de compromisos, responsabilidades y clausulas de penalidad	3: Medio Alto	2: Medio	MEDIO	Los contratos tienen clausulas de penalidad, pero no establecen mecanismos de confidencialidad.	1: Bajo	MEDIO
005	ST005	Ausencia de controles a la seguridad de terceros	2: Medio	3: Medio Alto	MEDIO ALTO	No existen mecanismos de control	0: No Controlado	MEDIO ALTO
006	ST006	No se realizan procesos de control de la sensibilidad de información en manos de terceros.	1: Medio Bajo	2: Medio	MEDIO	No existen mecanismos de control	0: No Controlado	MEDIO
007	ST007	Dependencia excesiva de terceros para la realización de diversos procesos	2: Medio	4: Alto	MEDIO ALTO	En los casos críticos, se ha buscado mas de dos proveedores (ATM), en los demas, se ha considerado no imprescindible	3: Razonable	MEDIO BAJO
008	ST008	No se realizan procesos de medición de desempeño o estos son deficientes y no documentados	1: Medio Bajo	1: Medio Bajo	MEDIO BAJO	Se realiza verificación de trabajos realizados y evaluación de objetivos alcanzados para el pago.	2: Parcial	BAJO
009	ST009	No existen procesos de monitores de servicios o estos son deficientes	2: Medio	3: Medio Alto	MEDIO ALTO	No se monitorea permanentemente el servicio, unicamente en el caso de reportes de falla.	1: Bajo	MEDIO
010	ST010	No se lleva un adecuado registro de contratos según sensibilidad de información expuesta a terceros	3: Medio Alto	2: Medio	MEDIO	Se tiene un inventario de contratos, pero no tiene clasificación de importancia y sensibilidad, el responsable aplica muchas veces su experiencia.	1: Bajo	MEDIO

Tabla 7: Riesgos Asociados a TI: (Servicios Prestados por Terceros)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Seguridad de Operaciones y Comunicaciones

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SO001	Ausencia de control de cambios al ambiente operativo : los sistemas de informacion, instalaciones de procesamiento y procedimientos.	2: Medio	2: Medio	MEDIO	Existen niveles de control de cambios, pero no están estandarizados ni formalizados, dependen mucho del responsable y del jefe de división	2: Parcial	MEDIO BAJO
002	SO002	No disponibilidad de los sistemas y servicios	1: Medio Bajo	3: Medio Alto	MEDIO	Se tiene implementado mecanismos Non Stop y control permanente del servidor principal	3: Razonable	BAJO
003	SO003	Tiempo de respuesta alto en sistemas en linea	1: Medio Bajo	3: Medio Alto	MEDIO	No se están ejecutando procesos de control mas alla de verificar la linea en los incidentes	1: Bajo	MEDIO
004	SO004	Planificacion ineficiente en procesos batch	0: Bajo	3: Medio Alto	MEDIO	Los procesos se encuentran planificados pero no se lleva un monitoreo de los mismos	2: Parcial	MEDIO BAJO
005	SO005	Fallas en los equipos y/o aplicaciones	1: Medio Bajo	3: Medio Alto	MEDIO	Se dispone de mecanismos de seguimiento y revisión permanente, hay deficiencias en soporte.	2: Parcial	MEDIO BAJO
006	SO006	Cambios no autorizados a la informacion en produccion	0: Bajo	3: Medio Alto	MEDIO	Todo cambio en producción debe estar acompañado de la solicitud de cambio, falta documentar y formalizar el proceso.	3: Razonable	BAJO
007	SO007	Inexistencia o deficiencias notables en ambiente de desarrollo	1: Medio Bajo	2: Medio	MEDIO	El personal es responsable del control de los procesos.	2: Parcial	MEDIO BAJO
008	SO008	Pruebas y control de calidad de los nuevos sistemas en produccion	2: Medio	2: Medio	MEDIO	Los controles no permiten pruebas en producción	3: Razonable	BAJO
009	SO009	Insuficiente capacidad de procesamiento de los equipos y medios de almacenamiento	1: Medio Bajo	4: Alto	MEDIO ALTO	Procesos Merge, Procesos continuos de reasignación y optimizacion de espacio físico.	3: Razonable	MEDIO BAJO
010	SO010	Introduccion de software malicioso o no autorizado	1: Medio Bajo	4: Alto	MEDIO ALTO	Se controla en las PC principales y administrativas, no así en las PC operativas	2: Parcial	MEDIO BAJO

Tabla 8: Riesgos Asociados a TI: (Seguridad de Operaciones y Comunicaciones)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION
Factor Crítico / Proceso en Evaluación:		*Seguridad Lógica*

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SL001	Acciones y/o actividades no autorizadas en los servicios de red	1: Medio Bajo	2: Medio	MEDIO	Se ha implementado visores de control de red, apliaciones de seguimiento por usuario.	2: Parcial	MEDIO BAJO
002	SL002	Ausencia o deficiencia en la identificación de usuarios en los sistemas	3: Medio Alto	2: Medio	MEDIO	En los sistemas administrativos se maneja por sistema operativo, en las sedes operativas no hay control	2: Parcial	MEDIO BAJO
003	SL003	Ausencia o deficiencia de validación de contraseñas de acceso a los sistemas	0: Bajo	2: Medio	MEDIO BAJO	En los sistemas administrativos se maneja por sistema operativo, en las sedes operativas no hay control	2: Parcial	BAJO
004	SL004	Ausencia o deficiencia de herramientas de auditoría	4: Alto	3: Medio Alto	MEDIO ALTO	Existen programas log en los servidores principales, no en los aplicativos desarrollados	2: Parcial	MEDIO BAJO
005	SL005	Ausencia de autenticación de usuarios en comunicaciones remotas	3: Medio Alto	1: Medio Bajo	MEDIO	Se valida por Host, no se autentica	3: Razonable	BAJO
006	SL006	Ingreso de virus, gusanos, caballos de troya, etc.	4: Alto	3: Medio Alto	MEDIO ALTO	Se tiene instalado antivirus en todas las PC	3: Razonable	MEDIO BAJO
007	SL007	Administración de derechos de perfiles no realizado por un área especializada en seguridad informática	2: Medio	3: Medio Alto	MEDIO ALTO	No existe area de seguridad informatica implementada, solo el MOF	0: No Controlado	MEDIO ALTO
008	SL008	Uso de distintas claves y perfiles distintos para cada aplicativo	4: Alto	2: Medio	MEDIO ALTO	No hay planificación para uso de Single SignOn	0: No Controlado	MEDIO ALTO
009	SL009	Ausencia de documentos de sustento de solicitudes de alta de usuarios	3: Medio Alto	2: Medio	MEDIO	La solicitud de alta de usuarios viene firmada por el jefe de departamento solicitante	3: Razonable	BAJO
010	SL010	Ausencia de documentos de clasificación de perfiles de usuario para cada aplicativo	3: Medio Alto	2: Medio	MEDIO	Se implementara una base de datos de perfiles de usuario, se administra actualmente de modo informal.	1: Bajo	MEDIO

Tabla 9: Riesgos Asociados a TI: (Seguridad Lógica)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Seguridad Física

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SF001	Ocurrencia de desastres que destruyan o deterioren de manera parcial o total ambientes físicos del banco	1: Medio Bajo	4: Alto	MEDIO ALTO	Se tiene un plan de seguridad física y de emergencia en oficinas, no se han hecho simulacros	2: Parcial	MEDIO BAJO
002	SF002	Ocurrencia de actos vandálicos que dañen los ambientes físicos del banco	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Se tiene un plan de seguridad física y de emergencia en oficinas, no se han hecho simulacros o acciones preventivas	1: Bajo	MEDIO
003	SF003	Ausencia de equipos de seguridad (alarmas, detectores de humo o agua, extintores, etc) adecuados	0: Bajo	3: Medio Alto	MEDIO	Se tiene implementado equipos de seguridad en todas las agencias	3: Razonable	BAJO
004	SF004	Inoperatividad de equipos de seguridad adecuados	2: Medio	3: Medio Alto	MEDIO ALTO	Se tiene controles preventivos y correctivos para equipos.	3: Razonable	MEDIO BAJO
005	SF005	No se realiza mantenimiento de equipos de seguridad o de ambientes físicos	1: Medio Bajo	3: Medio Alto	MEDIO	Se tiene controles preventivos y correctivos para equipos.	3: Razonable	BAJO
006	SF006	Presencia no generalizada en todo el banco de equipos de seguridad	0: Bajo	3: Medio Alto	MEDIO	Todas las agencias tienen equipos de seguridad implementados	3: Razonable	BAJO
007	SF007	Inexistencia de áreas físicas seguras en caso de desastre o no señalización de las mismas	0: Bajo	3: Medio Alto	MEDIO	Se encuentran señalizadas las zonas de seguridad, y los puntos de seguridad.	3: Razonable	BAJO
008	SF008	No existencia de control físico de acceso a los ambientes no públicos del banco	2: Medio	3: Medio Alto	MEDIO ALTO	Vigilancia privada y controles visuales con camaras de video en CCTV	2: Parcial	MEDIO BAJO
009	SF009	Inadecuada distribución y clasificicación de ambientes físicos según tipo de acceso permitido	2: Medio	2: Medio	MEDIO	No se tienen planos adecuados de distribución en algunas agencias, la mayoría de las nuevas están implementando dicho esquema de trabajo.	2: Parcial	MEDIO BAJO
010	SF010	Equipos mal ubicados en ambientes físicos	1: Medio Bajo	1: Medio Bajo	MEDIO BAJO	No se tienen planos adecuados de distribución en algunas agencias, la mayoría de las nuevas están implementando dicho esquema de trabajo.	2: Parcial	BAJO

Tabla 10: Riesgos Asociados a TI: (Seguridad Física)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Seguridad de Personal

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	SP001	Error en la manipulacion de los sistemas de informacion utilizados en personal	2: Medio	3: Medio Alto	MEDIO ALTO	No existen mecanismos de control formales	1: Bajo	MEDIO
002	SP002	Fraude Interno	2: Medio	3: Medio Alto	MEDIO ALTO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
003	SP003	Sabotaje	2: Medio	3: Medio Alto	MEDIO ALTO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
004	SP004	Robo de informacion	1: Medio Bajo	2: Medio	MEDIO	No existen mecanismos de control formales	1: Bajo	MEDIO
005	SP005	Abuso de accesos a los sistemas de informacion	1: Medio Bajo	2: Medio	MEDIO	Se controla via aplicativo host pero no hay limites de acceso.	1: Bajo	MEDIO
006	SP006	Manipulacion de la informacion	1: Medio Bajo	3: Medio Alto	MEDIO	Se realizan validaciones por totales y en informática se evalúa el archivo de personal	2: Parcial	MEDIO BAJO
007	SP007	Mal uso de la plataforma tecnologica	3: Medio Alto	3: Medio Alto	MEDIO ALTO	La experiencia de los usuarios finales limita el nivel de riesgo sin embargo no hay mecanismos de control	2: Parcial	MEDIO BAJO
008	SP008	Desconocimiento de las amenazas y problemas de seguridad de informacion	1: Medio Bajo	2: Medio	MEDIO	No hay programas de despliegue implementados actualmente	0: No Controlado	MEDIO
009	SP009	No existen definidas políticas de reemplazo de personal ausente	2: Medio	3: Medio Alto	MEDIO ALTO	Se aplican reemplazos ante la necesidad, no hay planes de reemplazo ni escalabilidad	1: Bajo	MEDIO
010	SP010	Ausencia por motivos no definidos de personal en cualquier area o agencia.	1: Medio Bajo	2: Medio	MEDIO	Se tiene establecido el reportar su ausencia a tiempo.	2: Parcial	MEDIO BAJO

Tabla 11: Riesgos Asociados a TI: (Seguridad de Personal)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	*Procesos de Respaldo*

NUM ORDEN	*COD RIESGO*	*DESCRIPCION DE EVENTOS DE RIESGO*	*NIVEL DE PROBABILIDAD*	*NIVEL DE IMPACTO*	*NIVEL DE RIESGO*	*CONTROLES ASOCIADOS*	*NIVEL DE CONTROL*	*RIESGO RESIDUAL ACTUAL*
001	*PR001*	*No se realizan procedimientos de respaldo de información crítica*	*3: Medio Alto*	*3: Medio Alto*	*MEDIO ALTO*	*Se realizan los backup, hay problemas asociados con la ubicación de estos*	*2: Parcial*	*MEDIO BAJO*
002	*PR002*	*No existe redundancia en los respaldos de información*	*4: Alto*	*4: Alto*	*ALTO*	*Se realizan dos copias de respaldo sin embargo no en todos los aplicativos*	*2: Parcial*	*MEDIO*
003	*PR003*	*No se realizan procesos de respaldo a la totalidad de sistemas críticos.*	*3: Medio Alto*	*2: Medio*	*MEDIO*	*Se realizan los backup, hay problemas asociados con la ubicación de estos*	*2: Parcial*	*MEDIO BAJO*
004	*PR004*	*No existencia de redundancia en los equipos de comunicación y líneas de comunicación*	*4: Alto*	*2: Medio*	*MEDIO ALTO*	*No existe dicho mecanismo de redundancia a la fecha.*	*0: No Controlado*	*MEDIO ALTO*
005	*PR005*	*Pérdida de información de respaldo (por robo, deterioro de dispositivos de almacenamiento)*	*2: Medio*	*3: Medio Alto*	*MEDIO ALTO*	*No hay mecanismos de control*	*0: No Controlado*	*MEDIO ALTO*
006	*PR006*	*Daños en los equipos de grabación y generación de respaldo*	*2: Medio*	*3: Medio Alto*	*MEDIO ALTO*	*No se tienen mecanismos de control, existe un control correctivo de equipos*	*1: Bajo*	*MEDIO*
007	*PR007*	*Ineficiente sistema de rotación de respaldo de información*	*3: Medio Alto*	*2: Medio*	*MEDIO*	*No hay mecanismos de rotación establecidos, se realizan de manera primaria unicamente*	*1: Bajo*	*MEDIO*
008	*PR008*	*Inadecuado inventario de dispositivos de almacenamiento*	*2: Medio*	*2: Medio*	*MEDIO*	*Los inventarios de dispositivos de almacenamiento se realizan solo para algunos servicios y servidores*	*2: Parcial*	*MEDIO BAJO*
009	*PR009*	*Inadecuado rotulado de dispositivos de almacenamiento*	*1: Medio Bajo*	*1: Medio Bajo*	*MEDIO BAJO*	*Existe un rotulado establecido*	*3: Razonable*	*BAJO*
010	*PR010*	*No existencia de procesos de recuperación y pruebas de efectividad de respaldo de información*	*3: Medio Alto*	*3: Medio Alto*	*MEDIO ALTO*	*La restauración del servidor principal es diaria, otra pruebas se realizan de manera permanente*	*2: Parcial*	*MEDIO BAJO*

Tabla 12: Riesgos Asociados a TI: (Procesos de Respaldo)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Flujo de Información

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	FI001	Existencia de medios inseguros para trasladar información	3: Medio Alto	2: Medio	MEDIO	No se tiene un control sobre los mecanismos de traslado de información	1: Bajo	MEDIO
002	FI002	Recepción/envío de correos electrónicos no deseados	3: Medio Alto	3: Medio Alto	MEDIO ALTO	Se ha implementado un analizador de contenidos y servicios antispam	3: Razonable	MEDIO BAJO
003	FI003	Deficiencias en el transporte físico a entidades externas	2: Medio	2: Medio	MEDIO	No se tiene un control sobre los mecanismos de traslado de información	1: Bajo	MEDIO
004	FI004	Inexistencia de acuerdos y responsabilidades	3: Medio Alto	2: Medio	MEDIO	Existencia de contratos con responsabilidades pero que no enfocan el factor confidencialidad.	2: Parcial	MEDIO BAJO
005	FI005	Inexistencia de documentación de nivel de sensibilidad de información	2: Medio	2: Medio	MEDIO	No existen clasificación de información	0: No Controlado	MEDIO
006	FI006	Inexistencia de registro de circulación de documentos (bitacoras físicas, actas, base de datos de documentos)	2: Medio	1: Medio Bajo	MEDIO BAJO	No existen mecanismos formales, se almacenan de modos distintos en cada area.	1: Bajo	MEDIO BAJO
007	FI007	Inexistencia de grados de dependencia e interrelación entre documentos circulantes (información)	1: Medio Bajo	3: Medio Alto	MEDIO	No se tiene mecanismos de seguimiento.	0: No Controlado	MEDIO
008	FI008	Procesos de seguimiento de información inadecuados	1: Medio Bajo	2: Medio	MEDIO	No se tiene mecanismos de seguimiento.	0: No Controlado	MEDIO
009	FI009	Existencia de redundancia en flujos de información	2: Medio	2: Medio	MEDIO	No se tiene mecanismos establecidos	0: No Controlado	MEDIO
010	FI010	Procesos de recepción de información (cargos) no adecuados o no establecidos	2: Medio	2: Medio	MEDIO	Hay normas con relación a la entrega de documentos.	3: Razonable	BAJO

Tabla 13: Riesgos Asociados a TI: (Flujo de Información)

		EVALUACION DE RIESGOS ASOCIADOS A TECNOLOGIA DE INFORMACION

Factor Crítico / Proceso en Evaluación:	Clasificación de Información

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	NIVEL DE RIESGO	CONTROLES ASOCIADOS	NIVEL DE CONTROL	RIESGO RESIDUAL ACTUAL
001	CS001	Ausencia de inventario clasificado de recursos de tecnologia de informacion	3: Medio Alto	2: Medio	MEDIO	Se tiene un inventario con una clasificación primaria	2: Parcial	MEDIO BAJO
002	CS002	Ausencia de responsables de los activos de informacion	2: Medio	2: Medio	MEDIO	Se tiene definido las responsabilidades, y esta se actualiza permanentemente.	3: Razonable	BAJO
003	CS003	Ausencia de proteccion adecuada a los activos de informacion	3: Medio Alto	2: Medio	MEDIO	En el C.C. se tiene mecanismos de protección de activos, en otras instancias aun no.	2: Parcial	MEDIO BAJO
004	CS004	Inadecuada manipulacion de los medios que contienen la informacion clasificada	2: Medio	3: Medio Alto	MEDIO ALTO	No hay mecanismos de seguimiento de información crítica.	1: Bajo	MEDIO
005	CS005	Inexistencia o procedimientos inadecuados de asignacion de responsabilidades de activos de informacion	2: Medio	2: Medio	MEDIO	Se tiene definido las responsabilidades, y esta se actualiza permanentemente.	3: Razonable	BAJO
006	CS006	No se ejecutan procedimientos para clasificar la información circulante en físico o electrónico	2: Medio	2: Medio	MEDIO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO
007	CS007	No hay un plan de despliegue de clasificación de seguridad operativo	3: Medio Alto	3: Medio Alto	MEDIO ALTO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO ALTO
008	CS008	Ausencia o desuso de metodologia de clasificacion de seguridad	3: Medio Alto	2: Medio	MEDIO	No se tiene establecida una política de clasificación de información.	0: No Controlado	MEDIO

Tabla 14: Riesgos Asociados a TI: (Clasificación de Información)

		MEDIDAS DE MITIGACION A IMPLEMENTAR - EVALUACION DE RIESGOS DE TI

NUM ORDEN	COD RIESGO	DESCRIPCION DE EVENTOS DE RIESGO	NIVEL DE RIESGO	RIESGO RESIDUAL ACTUAL	CONTROLES ASOCIADOS	CONTROLES A IMPLEMENTAR
001	DS001	Ausencia de requerimientos funcionales de validación de la información de entrada para generación o modificación de sistemas	Medio Alto	Medio Alto	No se está validando ni realizando pruebas de validación de información de entrada, se utiliza información continua	Implementar piloto de pruebas de calidad de información, Se está requiriendo formatos estándares a usuarios que envían información
002	DS003	Ausencia o deficiencia de metodología de desarrollo de sistemas	Medio	Medio	La metodología de desarrollo de sistemas está en proceso de formalización y despliegue	Implementación de Plan de Desarrollo de Sistemas, dentro del marco del PSI
003	DS004	Ausencia o no utilización de estándares de desarrollo	Medio	Medio	Aun no se han establecido mecanismos de procesos estándares.	Implementación de Plan de Desarrollo de Sistemas, dentro del marco del PSI
004	DS007	Ausencia de tecnología de administración de proyectos	Medio	Medio	Se tiene un módulo de administracion de proyectos, pero no se está utilizando	Actualización del módulo de proyectos en NOTES, documentar los perfiles de SW.
005	ST001	Mal uso de información del banco por parte de terceras empresas	Medio Alto	Medio	No existen políticas de acuerdos de confidencialidad formal, el control es muy informal	Implementar documento de acuerdo de confidencialidad adendum a principales contratos
006	ST003	Robo y divulgación de información	Medio Alto	Medio Alto	No se están ejecutando controles	Implementación de Políticas de seguridad en contratos con terceros, aplicación de programas de etica profesional aplicadas en contratos vigentes
007	ST004	Contratos sin inclusión de compromisos, responsabilidades y clausulas de penalidad	Medio	Medio	Los contratos tienen clausulas de penalidad, pero no establecen mecanismos de confidencialidad.	Adecuar las clausulas de penalidad con los acuerdos de confidencialidad
008	ST005	Ausencia de controles a la seguridad de terceros	Medio Alto	Medio Alto	No existen mecanismos de control	Solicitar esquemas de seguridad de información y negociar la adecuación a los sistemas de seguridad del Banco, agregar adendum al contrato
009	ST006	No se realizan procesos de control de la sensibilidad de información en manos de terceros.	Medio	Medio	No existen mecanismos de control	Formar el comité de evaluación (testeo) de sensibilidad de información

010	*ST009*	*No existen procesos de monitoreo de servicios o estos son deficientes*	*Medio Alto*	*Medio*	*No se monitorea permanentemente el servicio, unicamente en el caso de reportes de falla.*	*Implementar los grupos de seguimiento de servicios prestados por terceros, adecuar formatos de eventos de riesgo y formatos de ocurrencia de incidencias*
011	*ST010*	*No se lleva un adecuado registro de contratos según sensibilidad de información expuesta a terceros*	*Medio*	*Medio*	*Se tiene un inventario de contratos, pero no tiene clasificación de importancia y sensibilidad, el responsable aplica muchas veces su experiencia.*	*Automatizar los registros de contratos, aplicar clasificación de nivel de importancia y sensibilidad propuesto por riesgos.*
012	*SO003*	*Tiempo de respuesta alto en sistemas en linea*	*Medio*	*Medio*	*No se están ejecutando procesos de control mas alla de verificar la linea en los incidentes*	*Inicio de proceso Batch despues de las 5 PM, utilizar y reportar usando formato de ocurrencia de incidencias, evaluar y clasificar segmentos de ocurrencia mayor*
013	*SL007*	*Administración de derechos de perfiles no realizado por un área especializada en seguridad informática*	*Medio Alto*	*Medio Alto*	*No existe area de seguridad informatica implementada, solo el MOF*	*Implementar de personal al area ya aprobada*
014	*SL008*	*Uso de distintas claves y perfiles distintos para cada aplicativo*	*Medio Alto*	*Medio Alto*	*No hay planificación para uso de Single SignOn*	*Implementar politicas de seguridad de accesos bajo la administración de seguridad de información*
015	*SL010*	*Ausencia de documentos de clasificación de perfiles de usuario para cada aplicativo*	*Medio*	*Medio*	*Se implementara una base de datos de perfiles de usuario, se administra actualmente de modo informal.*	*Se está implementando el documento de perfil de aplicativo via formato de Planeamiento Estratégico de TI.*
016	*SP001*	*Error en la manipulacion de los sistemas de informacion utilizados en personal*	*Medio Alto*	*Medio*	*No existen mecanismos de control formales*	*Asignación de responsabilidades formales a nivel de usuario, especificación de niveles de escalamiento*
017	*SP004*	*Robo de informacion*	*Medio*	*Medio*	*No existen mecanismos de control formales*	*Diseñar módulos de autenticidad y auditoría para acceso a sistemas de usuario, Difusión de políticas de seguridad*
018	*SP005*	*Abuso de accesos a los sistemas de informacion*	*Medio*	*Medio*	*Se controla via aplicativo host pero no hay limites de acceso.*	*Implementar máximo número de accesos por día*
019	*SP008*	*Desconocimiento de las amenazas y problemas de seguridad de informacion*	*Medio*	*Medio*	*No hay programas de despliegue implementados actualmente*	*Difusión y capacitacion de cultura de riesgos*
020	*SP009*	*No existen definidas políticas de reemplazo de personal ausente*	*Medio Alto*	*Medio*	*Se aplican reemplazos ante la necesidad, no hay planes de reemplazo ni escalabilidad*	*Implementación de mecanismos de escalabilidad para procesos y actividades de personal*

021	*PR002*	*No existe redundancia en los respaldos de información*	*Alto*	*Medio*	*Se realizan dos copias de respaldo sin embargo no en todos los aplicativos*	*Implementación de red de fibra óptica entre centros de cómputo, políticas de respaldo de información*
022	*PR004*	*No existencia de redundancia en los equipos de comunicación y líneas de comunicación*	*Medio Alto*	*Medio Alto*	*No existe dicho mecanismo de redundancia a la fecha.*	*Implementación de red de fibra óptica entre centros de cómputo, políticas de respaldo de información*
023	*PR005*	*Pérdida de información de respaldo (por robo, deterioro de dispositivos de almacenamiento)*	*Medio Alto*	*Medio Alto*	*No hay mecanismos de control*	*Esquema formal de procedimiento dual*
024	*PR006*	*Daños en los equipos de grabación y generación de respaldo*	*Medio Alto*	*Medio*	*No se tienen mecanismos de control, existe un control correctivo de equipos*	*Revisar contratos de mantenimiento preventivo o correctivo, contactos de servicios menores*
025	*PR007*	*Ineficiente sistema de rotación de respaldo de información*	*Medio*	*Medio*	*No hay mecanismos de rotación establecidos, se realizan de manera primaria unicamente*	*Documentar los procesos aplicando controles de copia, ciclos de rotación y actualización según políticas de respaldo*
026	*FI001*	*Existencia de medios inseguros para trasladar información*	*Medio*	*Medio*	*No se tiene un control sobre los mecanismos de traslado de información*	*Esquema formal de procedimiento dual*
027	*FI003*	*Deficiencias en el transporte físico a entidades externas*	*Medio*	*Medio*	*No se tiene un control sobre los mecanismos de traslado de información*	*Esquema formal de procedimiento dual*
028	*FI005*	*Inexistencia de documentación de nivel de sensibilidad de información*	*Medio*	*Medio*	*No existen clasificación de información*	*Implementar proyecto de clasificación de información y difundirlo a la institución*
029	*FI008*	*Procesos de seguimiento de información inadecuados*	*Medio*	*Medio*	*No se tiene mecanismos de seguimiento.*	*Implementar proyecto de clasificación de información y difundirlo a la institución, adecuar sistema de control documentario en NOTES*
030	*FI009*	*Existencia de redundancia en flujos de información*	*Medio*	*Medio*	*No se tiene mecanismos establecidos*	*adecuar sistema de control documentario en NOTES*
031	*CS004*	*Inadecuada manipulacion de los medios que contienen la informacion clasificada*	*Medio Alto*	*Medio*	*No hay mecanismos de seguimiento de información crítica.*	*Implementar proyecto de clasificación de información y difundirlo a la institución*
032	*CS006*	*No se ejecutan procedimientos para clasificar la información circulante en físico o electrónico*	*Medio*	*Medio*	*No se tiene establecida una política de clasificación de información.*	*Implementar proyecto de clasificación de información y difundirlo a la institución*

033	*CS007*	*No hay un plan de despliegue de clasificación de seguridad operativo*	*Medio Alto*	*Medio Alto*	*No se tiene establecida una política de clasificación de información.*	*Implementar proyecto de clasificación de información y difundirlo a la institución*
034	*CS008*	*Ausencia o desuso de metodologia de clasificacion de seguridad*	*Medio*	*Medio*	*No se tiene establecida una política de clasificación de información.*	*Implementar proyecto de clasificación de información y difundirlo a la institución*

Tabla 15: Medidas de Mitigación a implementar