UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERIA

DETECCIÓN DEL RIESGO OPERATIVO EN EL ÁREA DE TECNOLOGÍA DE INFORMACIÓN: UNA PROPUESTA DE SISTEMA DE INFORMACIÓN

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN INGENIERÍA

INGENIERÍA DE SISTEMAS – OPTIMACIÓN FINANCIERA

P R E S E N T A :

WILFRIDO PASTRANA AÑORVE

TUTOR:
M.I. ISABEL PATRICIA AGUILAR JUAREZ

MÉXICO D.F. 2005

JURADO ASIGNADO:

Presidente: Dr. SERGIO FUENTES MAYA

Secretario: Dr. JESÚS HUGO MESA PUESTO

Vocal: M.I. ISABEL PATRICIA AGUILAR JUÁREZ

1er Suplente: Dr. JAVIER SUÁREZ ROCHA

2do Suplente: M.I. NELLY RIGAUD TELLEZ

Lugar donde se realizó la tesis:

DEPARTAMENTO DE SISTEMAS DE LA DIVISIÓN DE INGENIERÍA MECÁNICA E INDUSTRIAL DE LA FACULTAD DE INGENIERÍA DE LA UNAM.

TUTOR DE TESIS:

M.I. ISABEL PATRICIA AGUILAR JUÁREZ

_____

FIRMA

AGRADECIMIENTOS

A quien le debo todo mi desarrollo profesional.

Gracias a su apoyo económico me permite dar un paso más en mi carrera.

Al Departamento de Sistemas de la División de Ingeniería Mecánica e Industrial de la Facultad de Ingeniería y en especial al Dr. Sergio Fuentes Maya por ser un ejemplo al profesionalismo.

Al Dr. Javier Suárez Rocha por la paciencia y ejemplo de orden y perseverancia.

A la M.I. Patricia Isabel Aguilar Juárez por confiar en mi trabajo.

Al Dr. Jesús Hugo Mesa Puesto y la M.I. Nelly Rigaud Téllez por ser parte del Jurado.

A todos los profesores del departamento por su dedicación en la enseñanza.

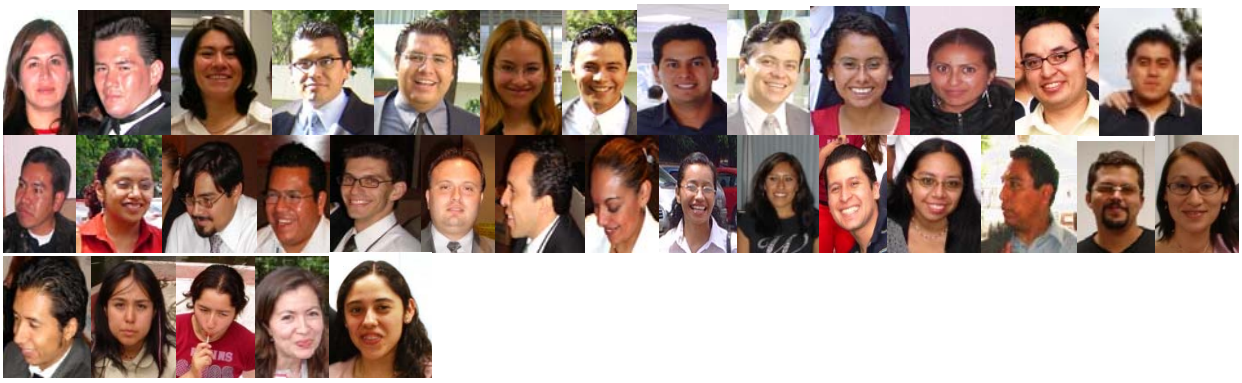
DEDICATORIA

A mi esposa, con amor y cariño.

A mis padres que siempre me dieron la libertad de ser y hacer.

A mis hermanos que cada uno es ejemplo a seguir.

A mis sobrinos como muestra de hiperactividad y sonreír a la vida.



A los compañeros y amigos, con y sin foto, que siempre estuvieron conmigo.

INDICE

RESUMEN

El propósito de esta tesis es identificar el riesgo operativo en el área de Tecnología de Información (TI) de una institución financiera y proponer un sistema de información que permita almacenar la información relacionada con los eventos y la severidad de este tipo de riesgo.

Se entiende como riesgo operativo el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos, incluyendo el riesgo legal. El estudio se apega a las recomendaciones y definiciones de riesgo operativo que el comité de Basilea emite en el segundo acuerdo de Basilea.

Para conceptualizar el área de TI, se identifican las principales variables en hardware, software y telecomunicaciones, y de esta manera, tener el marco de referencia para la identificación del riesgo operativo.

Para tener congruencia entre los objetivos, misión y visión de la empresa y el objetivo particular de identificar el riesgo operativo, se presenta la teoría de planeación estratégica y la metodología de administración de riesgo.

De esta manera se aborda la identificación del riesgo operativo para el área de TI y finalmente se propone un sistema de información para almacenar la información concerniente a los eventos; tomando en cuenta la severidad y frecuencia de los eventos para que de esta manera se pueda explotar la información y poder generar reportes, indicadores y pronósticos. De esta manera, este trabajo colabora para la medición del riesgo operativo.

ABSTRACT

The intention of this thesis is to identify the operational risk in the Information Technology department (IT) of a financial institution and proposing an information system that allows storing the information related with the events and the severity of this kind of risk.

Understanding as operational risk, the risk of loss resulting from inadequate or failed internal processes, people and systems, this definition include the legal risk. The study applies the recommendations and definitions of operational risk that Basel Committee on Banking Supervision supplies.

To understand better the IT department, the main variables (hardware, software and telecommunications) are identified, and in this way, identify the operational risk events and severities.

Being consistent among the objectives, mission and vision of the company and the specific objective of identifying the operational risk in IT department, it is presented the theory of strategic planning and the administration of risk methodology.

In this way, the operational risk identification for the IT department is studied and finally, an information system is proposed to store data related to the severity end frequency of events. After storing the data, decisions makers can generate reports, index and forecasts. In this way, this work collaborates to the measure of operational risk in financial institutions.

INTRODUCCIÓN

El riesgo operativo ha empezado a ser tema de estudio en las instituciones financieras y en particular los bancos, esto se debe a que estas instituciones son las que mayor impacto económico tienen debido a este tipo de riesgo, sin embargo no significa que las empresas no financieras estén exentas de este tipo de riesgo.

Formulación de la problemática.

Implementar la administración del riesgo operativo en las instituciones financieras es un proceso lento que requiere de una cultura hacia todo el corporativo, unidades de negocio y sucursales.

Actualmente, en Latinoamérica y en México, existen instituciones que no tienen identificadas sus unidades de negocio, y tampoco cuentan con los principios de administración del riesgo operativo. Por la trascendencia que esto tiene para las instituciones de crédito el Banco de Pagos Internacionales (BIS por sus siglas en inglés) a través del Comité de Supervisión Bancaria de Basilea y con el apoyo de los bancos centrales de los países del grupo de los 8, han generado el segundo acuerdo de Basilea o Basilea II. En él se establecen los estándares y pautas sobre la administración del riesgo y en especial el riesgo operativo.

Analizando la estructura de una empresa, en la figura I, se muestran las unidades de negocio que conforman un banco o institución financiera, estas unidades de negocio se ven afectadas por diversos tipos de riesgo, entre otros el riesgo operativo.

Los factores del riesgo operativo son:

- ✓ Procesos
- ✓ Personal
- ✓ Legal
- ✓ Sistemas o Tecnologías de Información.

Para implantar control de riesgo operativo cada uno de estos factores, debe ser administrado, monitoreado, y medido a través de indicadores o índices para así tener una visión global del cumplimiento de los objetivos.

De toda esta problemática que engloba el riesgo operativo, sólo se enfocará a estudiar el área de Tecnología de Información y su impacto de a través de los factores de procesos, Tecnología de Información o sistemas, personal, legal y el fraude por medio de los sistemas.

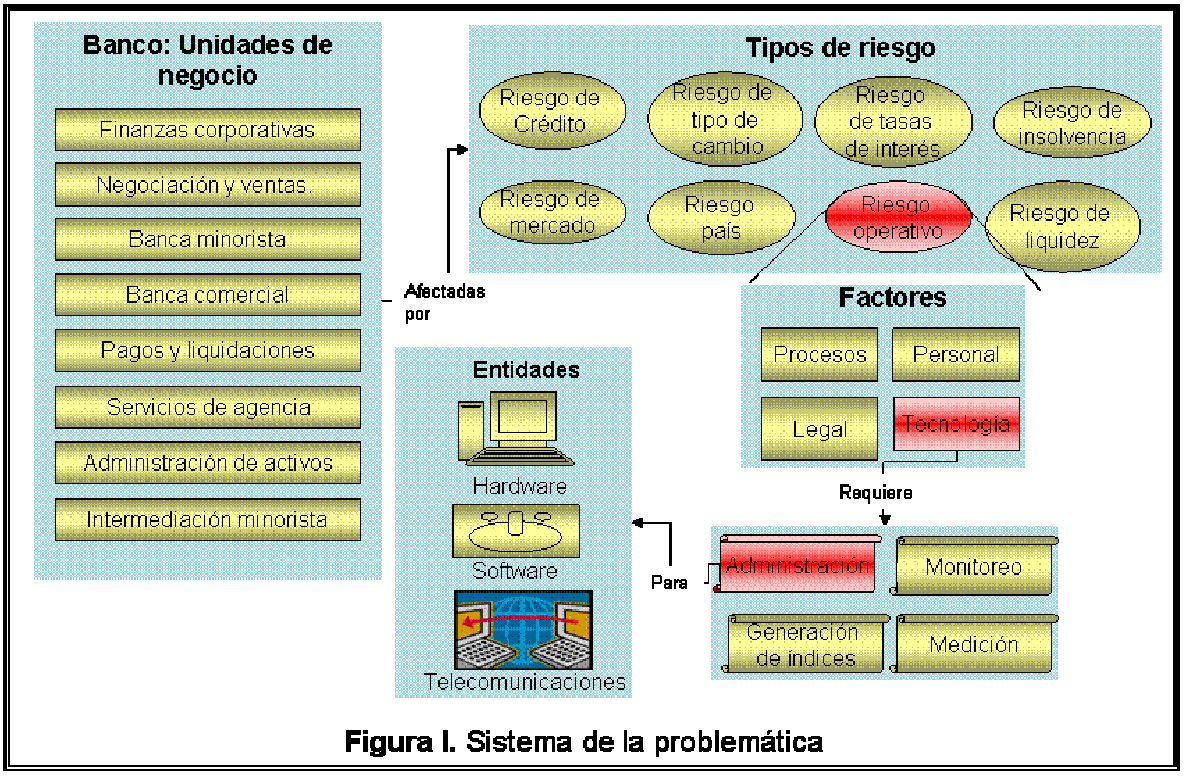


Figura I. Sistema de la problemática

Objetivo general.

El objetivo de esta investigación es detectar el riesgo operativo en el área de Tecnología de Información (TI), esto es, en software, hardware, seguridad de información y telecomunicaciones, tomando en cuenta también, los factores de procesos, personal y legal, de tal manera que permita a las instituciones financieras contar con una forma para la detección del riesgo operativo y hacer uso de la información a través de un sistema de información para generar estadísticas e indicadores que permitan mejorar la toma de decisiones para minimizar este tipo de riesgo dentro de la institución.

Hipótesis.

Tener definida la misión y visión del área de Tecnología de Información y apoyados en una metodología para identificar el riesgo operativo permitirán crear un sistema de información que procese los datos y cree información de valor para la toma de decisiones para minimizar el riesgo operativo.

Alcances de la investigación.

La investigación se enfoca en detectar el riesgo operativo en el área de TI y proponer un sistema de información para almacenar los eventos y medidas preventivas que surjan respecto a pérdidas en riesgo operativo, hacer uso de esta información, y con ella, generar indicadores de riesgo operativo en TI y así, las instituciones financieras puedan medir la frecuencia y severidad de dicho riesgo.

Limitaciones.

Por el tamaño de la problemática del riesgo operativo y el tiempo en el que se requiere terminar la investigación se detectan las siguientes limitaciones en este trabajo:

a) No presenta una solución global para el riesgo operativo.
b) No se profundiza en la administración, monitoreo y medición del riesgo operativo por no tener acceso a la información real de un banco.

Contenido.

En el primer capítulo se presenta un panorama general del riesgo operativo; se dan los antecedentes, y los conceptos, se describe la clasificación y se da un panorama de la importancia de la administración, monitoreo y medición de este tipo de riesgo en las instituciones financieras.

En el capítulo dos se hace una revisión de la infraestructura tecnológica estándar a las instituciones financieras, describiendo la función que desempeñan y la capacidad de operación que pueden ofrecer. En este capítulo sólo se presenta la variedad o diversidad tecnológica que las instituciones financieras tienen implementada para poder llevar a cabo las actividades diarias de la institución.

En el capítulo tres se presentan los dos enfoques teóricos que se usarán para proponer el prototipo del sistema de información: la planeación estratégica y la metodología para administración del riesgo.

En el capítulo cuatro, se usan las pautas para la administración del riesgo operativo que ayuda a identificar el riesgo en el área de TI, la información que se expone en este capítulo es principalmente obtenida por parte de los proveedores de tecnología.

CAPÍTULO I: ANTECEDENTES DEL RIESGO OPERATIVO.

Introducción y objetivo particular.

Con el fin de ofrecer estabilidad financiera, las instituciones financieras han buscado mecanismos que permitan medir el riesgo en sus activos. En este proceso se ha logrado diferenciar tres tipos principales de riesgos: el riesgo de mercado, el riesgo de crédito y el riesgo operativo.

El riesgo de mercado es el que se deriva de cambios en los precios de los activos y pasivos financieros y se mide por medio de los cambios en el valor de las posiciones abiertas.

El riesgo de crédito es el que se presenta cuando las contrapartes están poco dispuestas o imposibilitadas para cumplir sus obligaciones contractuales. Se mide por el costo de la reposición de flujos de efectivo si la otra parte incumple.

El objetivo de este capítulo es presentar un panorama global del riesgo operativo, los antecedentes, su evolución y la administración y métodos de medición que recientemente se han adoptado para el cálculo del requerimiento de capitales. Para finalizar el capítulo se particulariza en el riesgo tecnológico como principal área de interés del presente estudio.

1.1 Marco histórico.

A fines de 1974 y principios de 1975 se establece el Comité de Basilea en la Supervisión Bancaria (The Basel Committee on Banking Supervision) por los gobernadores de los bancos centrales del Grupo de Diez: Bélgica, Canadá, Francia, Alemania, Italia, Japón, Holanda, Suecia, Reino Unido y los Estados Unidos, además de Luxemburgo y Suiza,

El comité no posee ninguna autoridad de supervisión supranacional ni fuerza legal con las instituciones financieras, sin embargo crea estándares y pautas de supervisión e informes de recomendación con las mejores prácticas, con las expectativas de que cada autoridad tome sus medidas para implementarlas de la mejor manera de acuerdo a su sistema nacional.

A principios de los ochenta, el Comité de Basilea recomendó la administración, monitoreo y medición del riesgo que en ese momento impactaba las utilidades y, bajo ciertas condiciones, la quiebra de las instituciones financieras. De esta manera, en 1988 se consolida la primera propuesta dirigida a los bancos para la administración del riesgo de crédito. El objetivo del Nuevo Acuerdo de Basilea o Basilea I, es lograr una medición del capital regulatorio más sensible al riesgo, complementada con la profundización del proceso de supervisión bancaria y la disciplina de mercado.

En 1996 se realizó una enmienda para incorporar el riesgo de mercado, es decir, el riesgo derivado de las fluctuaciones en los precios de los activos con cotización, las tasas de interés y los tipos de cambio. Esta enmienda se realizó debido a que hasta ese momento solo se contemplaba el riesgo de crédito para medir los impactos de riesgo.

De esta manera, Basilea I establece que el capital mínimo debe ser al menos el 8% de los activos ponderados por su riesgo, tanto los registrados en el balance como la exposición de la entidad reflejada en cuentas fuera de balance.

Con esta tipificación del riesgo se pretendía tener cubiertos los riesgos que se presentaban con más frecuencia y los de mayor impacto en los bancos. A pesar de las medidas ya tomadas, en los bancos se presentaban eventos de pérdidas como los que se describen a continuación:

- ⇒ Banco Internacional de Crédito y Comercio. En 1991 los reguladores de este banco realizan un fraude por $17 mil millones de dólares de sus recursos.

- ⇒ Sumitomo Corporation, en 1996 incurrió en su más grande pérdida en el comercio excesivo de cobre. El esquema que la produce ha permanecido por más de una década y es un ejemplo clásico de comercio deshonesto, el monto de la pérdida fue de $2,857 millones de dólares.

- ⇒ General Motors. En 1996 tiene pérdidas por $1,200 millones de dólares debido a sus tres huelgas.

- ⇒ Diawa Bank. De 1983 a 1995 pierde $1,100 millones de dólares debido a las operaciones no autorizadas realizadas por un empleado que estaba a cargo de las garantías y del departamento de custodia y usó estas posiciones para orquestar su fraude.

- ⇒ Barings. Esta pérdida catastrófica se ha convertido como un punto de comparación para el riesgo operativo. La pérdida fue mayor al capital total base y a su reserva, provocando una crisis de liquidez. El empleado Nick Leeson fue el encargado de esconder las pérdidas en una cuenta especial que el mismo controlaba. Él violó las reglas de las buenas prácticas del riesgo operativo. Leeson estaba a cargo de las operaciones en ventanillas así como de la inspección por lo que pudo ocultar estas pérdidas por más de dos años hasta que se descubrieron en 1995. El monto de la pérdida: mil millones de dólares.

Ejemplos como estos, existen muchos otros más, y han sido los que llamaran la atención para crear una nueva categoría de riesgo, tomando en cuenta que este tipo de riesgo no era riesgo de crédito ni riesgo de mercado. Es así como se conceptualiza inicialmente el riesgo operativo.

1.2 Riesgo operativo.

Con el crecimiento de la red de computadoras mundial Internet, en la década de los noventas, se desarrolla vertiginosamente la tecnología en el campo de las comunicaciones y desarrollo de aplicaciones de software y sistemas en general, con el propósito de poder interactuar y ejecutar transacciones por medio de Internet, Intranet o Extranet.
Este desarrollo ha facilitado a las empresas y en particular a los bancos ofrecer servicios en “línea”, esto es que, por medio de las herramientas tecnológicas disponibles en el mercado puedan usar Internet para hacer transferencia de una cuenta a otra, consulta de

saldos, intercambio de información con clientes y proveedores y, aún más, trabajar desde un sitio remoto al corporativo y dar los mismos o mejores resultados.

Tradicionalmente el personal de atención a clientes almacenaba las transacciones que realizan los clientes, lo que requería un procesamiento y consolidación posteriores, esto implicaba realizar una doble revisión de las operaciones y se podía detectar inconsistencias o errores de captura que se pudieran cometer en las ventanillas.

Actualmente, las transacciones se realizan en tiempo real lo que hace que los bancos sean más eficientes pero están más propensos a cometer errores. Los contratos que se firman son cada vez más complejos y ya no sólo se requiere el punto de vista de un experto para poder evaluar el entorno en su totalidad, muchas de las veces los contratos incluso involucran a más de dos compañías lo que hace aún más complejo el delimitar las responsabilidades y obligaciones.

La especialización de carrera se ha convertido en un punto importante para las instituciones, las habilidades que debe tener el personal son cada vez más específicas lo que conduce a una capacitación continua para estar a la vanguardia de las necesidades del mercado. Esto implica que si la institución no mantiene un plan de desarrollo de las habilidades del personal está propensa a que las tareas no se ejecuten de la manera correcta, se cometan errores y además se pierda competitividad en el mercado.

Por otro lado, la complejidad de la infraestructura con la que están operando los bancos es cada día mayor: edificios inteligentes, equipo de telecomunicaciones especializados, servidores, seguridad de datos, políticas de acceso a los sistemas, etc. Esto impulsa la planeación de sitios alternos para operar en caso de siniestros.

Los procesos son otro punto en el que los bancos están propensos a ejecutar las tareas de manera errónea, o los procesos en sí mismos están mal diseñados lo cual repercute en la productividad y eficiencia de los resultados.

Como podemos darnos cuenta los puntos anteriores son riesgos a los que se enfrentan los bancos y no se contemplan en el riesgo de mercado ni en el riesgo de crédito. De esta manera, se define una nueva categoría de riesgo, el riesgo que se encuentra en las operaciones internas del banco o acontecimientos externos, así es como se concibe el riego operacional[1] y se define de la siguiente manera:

Primera definición: Riesgo Operativo, "Todo aquello que no era riesgo de crédito ni riesgo de mercado".

Segunda definición (Acuerdo de Basilea): "*El riesgo operativo se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal*[2]*, pero excluye el riesgo estratégico y el de reputación*".

[1] Para efectos de ésta investigación, riesgo operacional y riesgo operativo se consideran como sinónimos.

[2] El riesgo legal incluye, entre otros, la posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados entre las partes.

1.3 Administración, monitoreo y medición del Riesgo Operativo.

El riesgo operativo se encuentra en todos los niveles de la organización, desde los directivos, gerentes, operadores hasta personal de intendencia, es la razón por la que se requiere difundir una cultura en todos los niveles para la administración, monitoreo y mitigación.

Antes de iniciar con la administración, importa conocer la estructura de la organización e identificar las unidades de negocio[3] que dependiendo del tamaño pueden ser las ocho que se describen en la Tabla 1.1.

Tener identificadas las unidades de negocio en la institución, nos permitirá conocer las actividades que se realizan en cada una de ellas, lo cual facilita a identificar los riesgos potenciales.

Para poder administrar el riesgo es indispensable contar con un área encargada del riesgo operativo, y así, con cada una de las unidades de negocios, ser la responsable de:

- Documentar los procesos.
- Establecer procedimientos.
- Establecer políticas.
- Capacitación al personal.
- Documentar eventos de pérdidas.

Por otro lado, es importante clasificar las eventualidades que se presentan en cada unidad de negocio, esto con la finalidad de contar con una base de datos donde se registren las pérdidas que impactan a la institución.

En el Segundo Acuerdo de Basilea, se propone la siguiente clasificación de los eventos:

1. Fraude Interno. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales en la que se encuentra implicada, al menos, una parte interna a la empresa.

2. Fraudes externos. Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.

3. Relaciones laborales y seguridad en el puesto de trabajo. Pérdidas derivadas de actos incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación.

[3] Las unidades de negocio se caracterizan porque sus productos enfrentan distintos rivales, están dirigidos a un mercado externo y pueden trazar su propia estrategia competitiva, de lo contrario se les considera áreas auxiliares.

Tabla 1.1. Asignación de unidades de negocio.		
Nivel 1	**Nivel 2**	**Grupos de actividades.**
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, deuda, acciones, colocaciones privadas en mercados secundarios.
	Finanzas de administraciones locales y públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, productos básicos, crédito, financiación, posiciones propias en valores, préstamos y operaciones con pacto de recompra, intermediación, deuda
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos al menudeo, servicios bancarios y fideicomisos
	Banca privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y testamentarías, y asesoramiento de inversión
	Servicios de tarjetas	Tarjetas comerciales y corporativas
Banca comercial.	Banca comercial	Financiación de proyectos, bienes raíces, financiación comercial, arrendamiento financiero, préstamo, garantías y letras de cambio.
Pagos y liquidaciones	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Certificados de depósito, operaciones de sociedades para préstamo de valores
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minorista, institucionales, cerrados y abiertos
	Administración no discrecional de fondos	Agrupado, segregados, minoristas institucionales, de capital fijo, de capital variable.
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo

4. Clientes, productos y prácticas empresariales. Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos o de la naturaleza o diseño de un producto.

5. Daños a activos materiales. Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

6. Incidencias en el negocio y fallas en los sistemas. Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas

7. Ejecución, entrega y gestión de procesos. Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

En la Tabla 1.2 se muestran las subcategorías de los siete tipos de eventos mencionados anteriormente.

Tabla 1.2 Clasificación de los eventos de perdida del riesgo operativo.

Tipo de evento (Nivel 1)	Tipo de evento (Nivel 2)	Ejemplos
I. Fraude Interno	1. Actividades no autorizadas	1. Operaciones no reportadas intencionalmente 2. Operaciones no autorizadas 3. Valoración errónea de posiciones
	2. Hurto y fraude	1. Fraudes, fraudes de crédito, depósitos sin valor 2. Robo, extorsión, malversación, robo 3. Apropiación indebida de activos 4. Destrucción dolosa de activos 5. Falsificación 6. Utilización de cheques sin fondos 7. Sobornos y cohechos 8. Abuso de información privilegiada
II. Fraudes externos	3. Hurto y fraude	1. Hurto y robo 2. Falsificación
	4. Seguridad en los sistemas	1. Daños por ataques informáticos 2. Robo de información
III. Relaciones laborales y seguridad en el puesto de trabajo	5. Relaciones laborales.	1. Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
	6. Higiene y seguridad en el trabajo	1. Responsabilidad en general (resbalones, etc.) 2. Casos relacionados con las normas de higiene y seguridad en el trabajo 3. Indemnización a los trabajadores
	7. Diversidad y discriminación	1. Todo tipo de discriminación
IV. Prácticas con clientes, productos y negocio	8. Adecuación, divulgación de información y confianza	1. Abusos de confianza e incumplimiento de pautas 2. Divulgación de información 3. Quebrantamiento de acuerdo de privacidad 4. Ventas agresivas 5. Confusión de cuentas 6. Abuso de información confidencial
	9. Prácticas empresariales o de mercado improcedentes	1. Prácticas restrictivas de la competencia. 2. Manipulación del mercado 3. Actividades no autorizadas

Tabla 1.2 Clasificación de los eventos de perdida del riesgo operativo.

Tipo de evento (Nivel 1)	Tipo de evento (Nivel 2)	Ejemplos
	10. Defectos del producto	1. Productos defectuosos 2. Error de los modelos
	11. Selección, patrocinio y riesgo	1. .Ausencia de investigación a clientes conforme a las directrices 2. Superación e los límites de riesgo frente a los clientes
	12. Actividades de asesoramiento	1. Litigios sobre los resultados de las actividades sobre asesoramiento
V. Daños a activos materiales	13. Desastres y otros eventos	1. Perdidas por desastres naturales. 2. Perdidas humanas por causas externas: Terrorismo, vandalismo, etc.
VI. Incidencias en el negocio y fallas en los sistemas	14. Sistemas	1. Hardware 2. Software 3. Telecomunicaciones 4. Interrupción e incidencias en el suministro
VII. Ejecución, entrega y gestión de procesos	15. Recepción, ejecución y mantenimiento de operaciones	1. Comunicación defectuosa 2. Error de captura o introducción de datos 3. Incumplimiento de plazos o de responsabilidades 4. Ejecución errónea de modelos o sistemas 5. Falla en la entrega
	16. Seguimiento y presentación de informes	1. Incumplimiento de la obligación de informar 2. Inexactitud de informes externos
	17. Aceptación de clientes y documentación	1. Inexistencia de autorizaciones o rechazo de clientes 2. Documentos jurídicos inexistentes o incompletos
	18. Gestión de cuentas de clientes	1. Acceso no autorizado a cuentas. 2. Registro incorrectos de clientes. 3. Perdida o daño de activos de clientes por negligencia
	19. Contrapartes comerciales	1. Fallos de contrapartes distintas de clientes 2. Otros litigios con contrapartes distintas de clientes
	20. Distribuidores y proveedores	1. Subcontratación 2. Litigios con distribuidores

Para poder monitorear, administrar y medir el riesgo, es necesario contar con infraestructura tecnológica accesible a todos los niveles del banco. Dicha infraestructura

debe permitir crear perfiles de usuarios, donde se pueda dar permisos de documentación de eventos de pérdidas, generación de reportes, mantenimiento al sistema, etc.

En el momento que una institución financiera ha implementado lo anterior, podemos decir que esta lista para medir el riesgo operativo.

Métodos de medición del riesgo operativo.

Aunque hoy en día, las instituciones financieras no están obligadas a medir el riesgo operativo, se contempla que para año 2006 ya sea obligatorio.
El comité de Basilea ha propuestos tres métodos para cubrirse de las eventualidades del riesgo operativo; el método a usar por la institución financiera dependerá del nivel de administración implementado::

- Indicador Básico.
- Aproximación estándar.
- Aproximación por medición avanzada.

El método de indicador básico, es el más sencillo, los bancos que deseen aplicarlo deben reservar un capital para el riesgo operativo equivalente al promedio de los tres años previos de un porcentaje fijo de los ingresos brutos positivos (a este porcentaje se le denomina alfa, α). Al calcular este promedio se deben excluir los años en el que el ingreso bruto anual haya sido negativo o cero.

La manera de calcularlo queda de la siguiente manera:

$$K_{BIA} = [\sum (GI_{1...n} * \alpha)] / n$$

Donde:
K_{BIA} = Exigencia de capital en el Método del Indicador Básico.
GI = Ingresos brutos anuales positivos sobre los tres años previos.
n = Número de los tres años previos donde los ingresos fueron positivos.
α = 15%, parámetro establecido por el Comité de Basilea, que relaciona el capital exigido al conjunto del sector con el nivel del indicador en el conjunto del sector.

El método de aproximación estándar, se calcula de acuerdo a las unidades de negocio de la Tabla 1.1, el capital requerido para cada línea de negocio se calcula multiplicando los ingresos brutos (para el caso que los ingresos brutos de un año determinado sean negativos, el ingreso para ese año se toma como cero) por un factor denominado beta, β, asignado a la línea de negocio, como se muestra en la tabla 1.3.

El capital total se calcula como el promedio en los tres años previos de la suma del capital regulatorio de las unidades de negocio en cada año, esto es:

$$K_{TSA} = \{ \sum_{\text{años } 1-3} \max[\sum (GI_{1-8} \times \beta_{1-8}), 0] \} / 3$$

Donde:
K_{TSA} = Exigencia de capital bajo el método estándar.
GI_{1-8} = Ingresos brutos anuales en un año dado para cada una de las ocho unidades de negocio.
β_{1-8}= Porcentaje fijo determinado por el comité para cada línea de negocios.

A continuación se muestran las **β** correspondientes a las unidades de negocio, estos porcentajes son asignados por el comité de Basilea:

Tabla 1.3. Valor de la **β** por línea de negocio.	
Finanzas corporativas (β1).	18%
Negociación y ventas (β2).	18%
Banca minorista (β3).	12%
Banca comercial (β4).	15%
Pagos y liquidaciones (β5).	18%
Servicios de sucursales y filiales (β6).	15%
Administración de activos (β7).	12%
Menudeo de corretaje (β8).	12%

Aproximación por medición avanzada[4]. Este método contempla requerimientos de integración de riesgo operativo en la gestión diaria, para ello existen tres alternativas:

- Aproximación por medición interna (IMA por sus siglas en inglés).
- Aproximación por distribución de pérdidas (LDA).
- Aproximación por scoredcards.

El método de *aproximación por medición interna* obtiene la pérdida esperada por cada combinación de unidad de negocio y tipo de riesgo. Parte de bases de datos históricos para cuantificar los tipos de incidencia por línea de negocio e información de fuentes externas.

El método de *aproximación por distribución de pérdidas*, se apoya principalmente con información histórica interna de perdidas y se complementa con datos externos, para que de esta manera se pueda crear una función de distribución de los fallos por frecuencia y severidad. De esta manera se obtiene una distribución de pérdidas esperadas por unidad de negocio y tipo de riesgo.

Aproximación por scorecards. Este método parte de un capital inicial por riesgo operativo por unidad de negocio para posteriormente ir modificando de acuerdo a unos scorecards que pretenden reflejar el perfil de riesgo subyacente, el control existente y las variaciones que se produzcan en estos aspectos.

1.4 Riesgo tecnológico.

El riesgo tecnológico, dentro de la clasificación proporcionada por Basilea, se considera en la categoría “interrupción del negocio por fallas en sistemas” o “Fraudes externos”.

Las interrupciones pueden estar relacionadas con el hardware, software o las telecomunicaciones, y ser causadas por fallas, desempeño deficiente o un mal diseño en las capacidades requeridas para satisfacer las necesidades del banco.

[4] http://www.ceu.es/clubriesgos/2%20Riesgo%20Operacional%20A.%20Morillas.ppt, fecha de consulta: enero del 2005.

Relacionado con Fraudes Externos, está todo lo que corresponde a la seguridad en los sistemas, ataques informáticos y robo de información.

De esta manera se puede ejemplificar con eventos como:

- Pérdidas causadas por el impacto provocado por los virus informáticos en las operaciones diarias del banco.
- Pérdidas generadas por un pobre desempeño o fallas en los equipos de cómputo, redes y enlaces de telecomunicaciones.
- Pérdidas debido a fallas o mal diseño de las aplicaciones usadas en el banco.

Como medida para mitigar este tipo de eventualidades las instituciones financieras cuentan con políticas, procedimientos, manuales de operación y planes de contingencia que estén orientados a afrontar este riesgo.

A pesar de las medidas con las que ya se cuenta en los bancos, aún falta implementar una base de datos con los niveles de servicio de cada una de las entidades tecnológicas que se tienen en la institución.

En el siguiente capítulo se aborda la principal base tecnológica con la que cuentan los bancos y en general las instituciones financieras para poder ofrecer los servicios a sus clientes con la finalidad de poder clasificar los índices tecnológicos involucrados en estas instituciones.

1.5 Conclusiones.

La importancia que las instituciones financieras han dado a la administración, monitoreo y medición del riesgo operativo ha sido cada día mayor, esto impulsado por el comité de Basilea (Basilea II), ya que ha recomendado a los bancos e instituciones financieras calcular el requerimiento de capitales necesario para cubrirse del impacto de los eventos que se presenten.

Para que el capital reservado represente el nivel de riesgo del banco, es necesario que se establezcan políticas y procedimientos orientados a la administración, monitoreo, creación de índices y medición del riesgo operativo.

CAPÍTULO II: IDENTIFICACIÓN DE VARIABLES TECNOLÓGICAS.

Objetivo particular.

El objetivo de este capítulo es identificar las principales variables que impactan el área de sistemas que para el caso del riesgo operativo es clasificado como el riesgo tecnológico.

2.1 Hardware.

En todas las instituciones bancarias de hoy en día, se ha instalado una plataforma tecnológica de hardware diversa, con el objetivo de apoyar las necesidades de sistemas con la que cuenta la institución. Esta infraestructura se orienta a diferentes necesidades: almacenamiento de datos, servidores, comunicación, seguridad de información, etc.; en la mayoría de los casos, se cuenta con múltiples proveedores debido a que se especializan en productos específicos y pocas empresas como IBM y Cisco pueden ofrecer soluciones "globales".

Dentro de la infraestructura tecnológica de hardware se identifican tres bloques principales que proveen esta solución: las redes WAN (Wide Area Network), redes LAN (Local Area Network), y equipo de cómputo. Como se muestra en la figura 2.1.

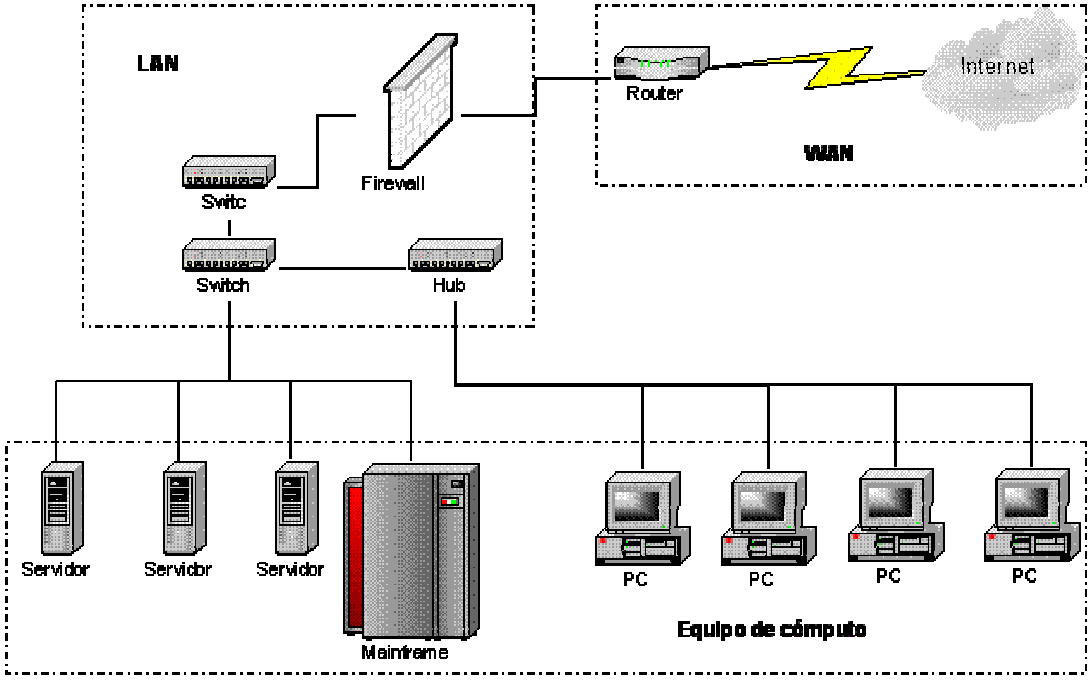


Figura 2.1 Hardware

2.1.1 Redes WAN.

Las instituciones bancarias cuentan con al menos una oficina central a la que se conectan las sucursales para el envió y recepción de información necesaria para la atención a sus clientes, a toda la infraestructura de comunicación necesaria para que la información fluya de un punto a otro, ya sea entre sucursales u oficina central se le conoce como red de área amplia, WAN por sus siglas en inglés. (Figura 2.2)

Como podemos ver, en las redes WAN encontramos diferente tipo de equipo de comunicación, estos son:

1. Enlaces de comunicación.
2. Ruteadores.

1. Los enlaces de comunicación conectan dos oficinas que geográficamente se encuentran separadas, estos enlaces los proveen empresas de telefonía como Telmex, Alestra, Avantel, etc. Cada una de estas compañías tienen una cobertura geográfica en donde pueden o no ofrecer estos servicios. De acuerdo a la tecnología disponible los enlaces pueden ser punto a punto, Frame Relay o ATM.
2. Los ruteadores. Son equipos que se usan para interconectar dos o mas redes LAN, ya sea usando enlaces WAN o puertos LAN.

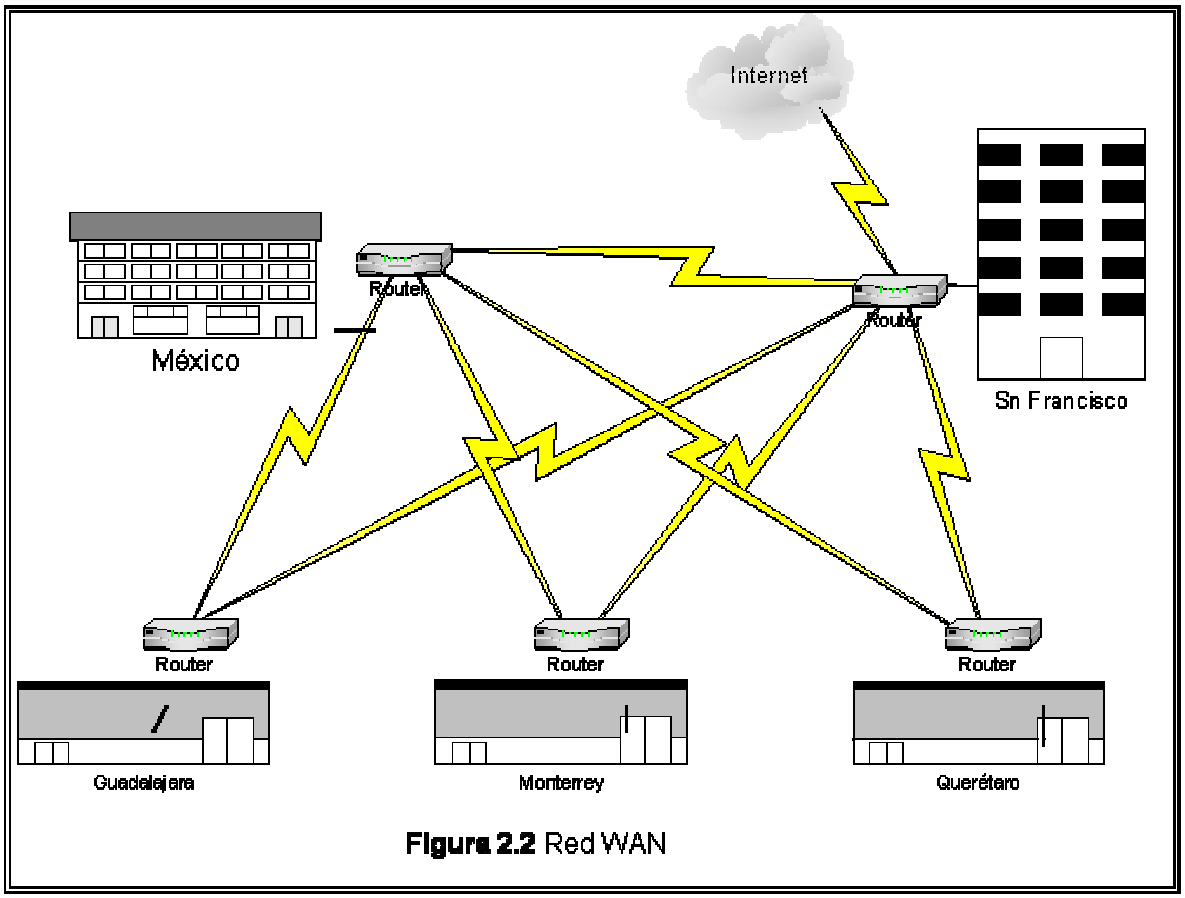


Figura 2.2 Red WAN

2.1.2 Redes LAN.

Hoy en día, tanto las empresas pequeñas, medianas y grandes cuentan con una red de datos de área local, LAN por sus siglas en inglés, cada una con características propias. En particular los bancos cuentan con esta infraestructura en sus sucursales y las oficinas centrales para interconectar las computadoras de cada uno de los empleados y los servidores centrales, así como también para conectarse a la red WAN que les permita la comunicación al exterior. Como se muestra en la figura 2.3.

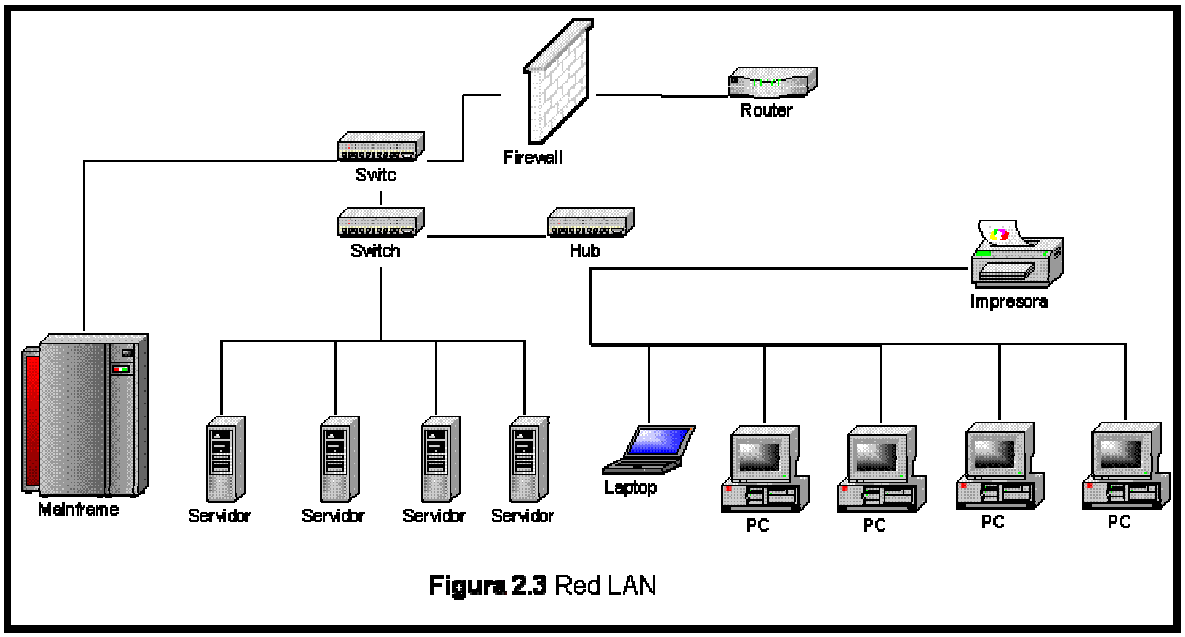


Figura 2.3 Red LAN

Para el caso de las redes LAN se cuenta con equipos de diferentes tecnologías que se instalan de manera estratégica de acuerdo a las necesidades de la misma empresa. Entre los equipos disponibles encontramos:

1. Hubs.
2. Switches
3. Firewalls.

1. Hubs. Los hubs se caracterizan por ser equipos multipuertos que comparten el mismo canal de comunicación, cuando un paquete de datos se envía desde un puerto, éste se copia a todos los puertos restantes. Inicialmente los hubs tenían una velocidad de 10 Mbps y actualmente existen de 10/100 Mbps, por sus características tecnológicas y precio este tipo de equipo ya se encuentra en decadencia. En cada puerto se conecta una computadora o servidor la siguiente imagen muestra un Hub. En la figura 2.4 se muestra uno de estos equipos.

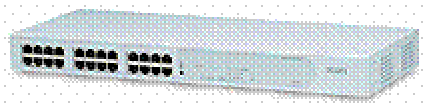


Figura 2.4. Hub

2. Switch. Un switch es un equipo con funciones equivalentes a las de un Hub, solo que este es un equipo más sofisticado ya que cuando un paquete es enviado desde cualquiera de los puertos donde se encuentra conectada una computadora o servidor, el paquete se direcciona al puerto de la computadora o servidor destino. Estos equipos cuentan con software preinstalado que permite configurarlos de acuerdo a sus características y necesidades de la empresa. De acuerdo a las necesidades de puertos existen en configuración fija y en configuración modular. Por las necesidades de configuración existen de capa 2 y capa 3. En la figura 2.5 se muestran dos modelos de estos equipos.

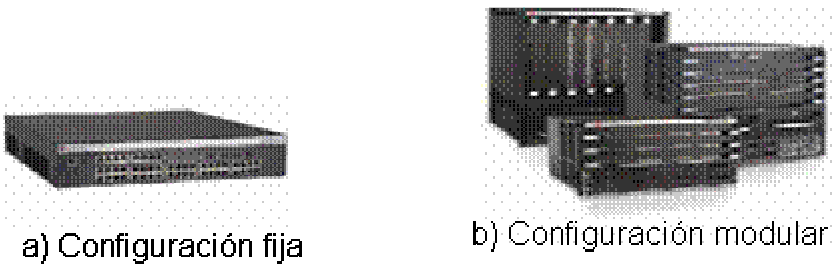


Figura 2.5. Switches

3. Firewalls. Son dispositivos de seguridad de datos que por medio de políticas permiten o niegan la entrada o salida de información de la red privada a la institución. Estos dispositivos se instalan en la conexión hacia redes con proveedores, clientes e Internet. De esta manera es posible configurarlo de varias formas, una de las más comunes es identificar la zona segura de la red y otra que se le conoce como zona desmilitarizada donde se colocará la información pública o información de interés para clientes, proveedores, accionistas, reguladores, etc. Ver Figura 2.6.

2.1.3 Cómputo

El equipo de cómputo es la otra parte fundamental que permite a los bancos y empresas en general poder ofrecer los servicios a los clientes no solo en las horas hábiles sino que se ponen parte de estos servicios disponibles las 24 horas del día los 365 días del año.

Los equipos de cómputo principales que tienen las empresas financieras son:

- Computadoras personales.
- Servidores.

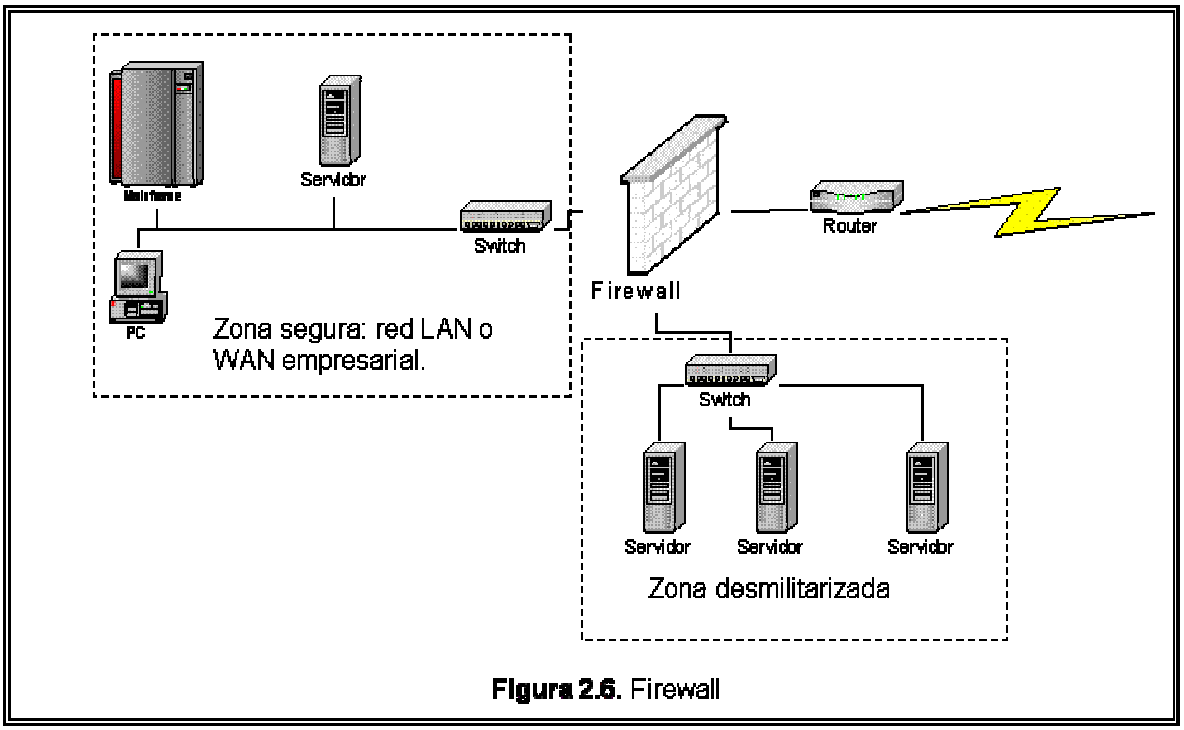


Figura 2.6. Firewall

Computadoras personales. El primer equipo denominado computadora personal fue el desarrollado por IBM, posteriormente se denominan PC compatibles con IBM. En nuestro contexto lo llamaremos computadora personal a todo aquel equipo de cómputo donde las personas realizan sus actividades de oficina o personales para la explotación e intercambio de información usando los sistemas de cómputo: PCs de escritorio Intel, Laptop, Macintosh, etc.

La característica principal de estos equipos es proporcionar los recursos necesarios para satisfacer las necesidades individuales, tales como: Memoria RAM, procesador y disco duro.

Servidores. Un servidor es una computadora o dispositivo que se encuentra conectado a red y administra o aloja recursos: impresión, aplicación y o archivos, para que los usuario permitidos puedan explotar las características de este equipo y procesar información y obtener los resultados en menor tiempo, además de contar con mejor tecnología para permitir la conexión de múltiples usuarios y múltiples aplicaciones de manera simultanea.

Los servidores se pueden clasificar de acuerdo al sector de mercado al que están orientados:

Micro y pequeña empresa.

- X86: Intel y AMD. Se caracterizan por ser equipos a bajos precios, traen configuración fija y expectativas de crecimiento limitado. Por lo general estos servidores traen capacidad como máximo para dos o tres procesadores, cavidades reducidas para expansión en discos duros, tarjetas y Memoria RAM. En la Figura 2.7 se presenta un ejemplo de este tipo de servidores.

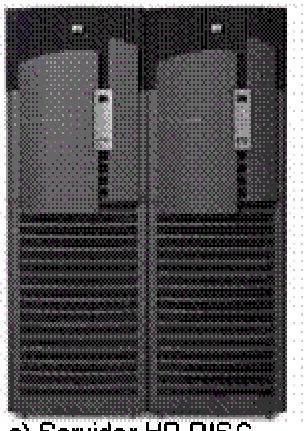
Servidor Dell Modelo:
PowerEdge 2800

Figura 2.7 Servidor para empresas chicas y pequeñas.

Mediana empresa.

- Risc.
- Spark

Los servidores con tecnología RISC y los de tecnología SPARK compiten por el mismo mercado, estos son desarrollados por HP y SUN Microsystems respectivamente. La tecnología que integran estos servidores es mejor que los X86, son escalables y en la mayoría de sus partes son redundantes. En la Figura 2.8 se muestra un ejemplo de estos servidores.



a) Servidor HP RISC
Modelo: Superdome

b) Servidor SUN SPARK
Modelo: Sun Fire 12K

Figura 2.8 Servidores para pequeñas y medianas empresas.

Empresa grande.

- Mainframe.

Este tipo de servidores están dirigidos principalmente a empresas del giro financiero, bancos principalmente. Proveen la más alta tecnología tanto en seguridad, escalabilidad, disponibilidad y desempeño. En la Figura 2.9 se presenta un ejemplo de este tipo de servidores.

Servidor Mainframe IBM Modelo: S/390 Paralel Enterprise

Figura 2.9 Servidor para empresas grandes.

2.2 Software.

El software se define como instrucciones de la computadora o datos de cualquier cosa que sea almacenado de manera electrónica.

El software lo podemos clasificar de la siguiente manera:

1. Sistema operativo
2. Aplicaciones

1. El sistema operativo, es la parte esencial en una computadora o servidor ya que es el responsable de realizar las tareas básicas, tales como: reconocer las entradas del teclado, envío de señal al monitor, controlar los dispositivos periféricos, administrar las aplicaciones y llevar una registro de permisos de acceso a archivos, directorios y aplicaciones.

   Existen diversos sistemas operativos que se instalan en plataformas de hardware que sean compatibles con el mismo para poder operar:

   Para plataforma X86: Windows 9x, Windows 2000, Windows XP, Windows 2003, Unix SCO, Linux, etc.

HP cuenta con su plataforma de hardware RISC y al mismo tiempo cuenta con su sistema operativo Unix HP-UX, Sun Microsystems sus procesadores SPARK y su sistema operativo Unix Solaris, IBM sus procesadores POWER5 y su sistema operativo Unix AIX, así como el sistema operativo MVS para los equipos mainframe 370 y compatibles, etc.

Las características de los sistemas operativos son:

- Seguridad. Para que una persona pueda entrar al sistema es necesario contar con una clave de usuario y una contraseña válidos para el sistema.
- Multiusuario. Múltiples usuarios pueden estar trabajando de manera simultánea usando los recursos del servidor.
- Multitareas. Los usuarios pueden lanzar diferentes tareas y ejecutarse de manera simultanea los procesos.
- Multiprocesador. La carga de trabajo se balancea entre los múltiples procesadores del servidor.

De esta manera el sistema operativo es una interfase entre el hardware y las herramientas que el usuario usará, a estas herramientas se le conoce como aplicaciones.

2. Las aplicaciones, son programas de software que se instalan sobre el sistema operativo, esto es, una vez instalado el sistema operativo en el servidor, se instala la aplicación.
   La diversidad de aplicaciones es amplia y muchas son compatibles con diversos sistemas operativos y esta diversidad es tan grande como las necesidades que las empresas tienen en sus actividades diarias.

   Las aplicaciones las podemos clasificar por el fin para el que fueron desarrolladas:

   - Bases de datos. Oracle, Informix, DB2, Microsoft SQL
   - ERP (Enterprise Resource Planning): PeopleSoft, SAP, etc.
   - Seguridad: Proxis, firewalls, etc.
   - Internet:
   - Software de desarrollo: C, C++, JAVA, etc.

2.3 Conclusiones

Una transacción se ejecuta exitosamente cuando se hace uso de diversos mecanismos tecnológicos. El proceso o flujo de información cuando un cliente realiza un depósito en su cuenta en una sucursal, es el siguiente:

1. El cliente llena el formato de depósito: llena los campos de propietario de la cuenta, lugar y fecha, número de cuenta, cantidad a depositar y nombre de quien realiza la operación.
2. El cajero se valida al sistema y registra la operación.
3. Finalmente, entrega un comprobante del depósito al cliente.

Pero, ¿Qué sucede realmente a nivel de comunicación en el paso dos donde el cajero registra la operación? Esto se ve en la Figura 2.10.

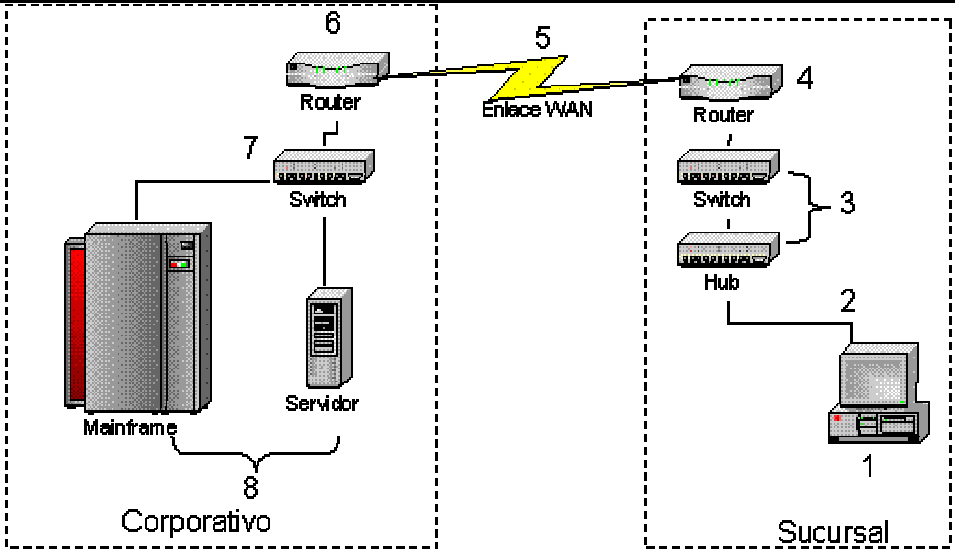


Figura 2.10 Flujo de información entre la estación de un cajero y los servidores.

El cajero, vía el sistema, registra los datos del cliente y acepta la operación.

1. La computadora, conectada con cable hacía un hub o switch, vía la tarjeta de red envía la información a los servidores en el corporativo.
2. El switch recibe los paquetes de información y los envía al ruteador.
3. El ruteador identifica el destino de la información y usa el enlace WAN.
4. El enlace WAN es la conexión que el proveedor telefónico instaló para unir las roueters de la sucursal y el del corporativo.
5. El ruteador del corporativo, envía los paquetes de información a los servidores.
6. El switch, recibe la información del ruteador y envía finalmente la información a los servidores.
7. Los servidores procesan y actualizan la información enviada por el cajero en las bases de datos.

En el flujo de información, se identifican equipos que tienen un nivel mayor de importancia para la operación del banco. No es el mismo impacto en las pérdidas si se desconecta el cable de red en la computadora del cajero, punto 2 en el diagrama, a que falle el cable o el switch que conecta la tarjeta de red del servidor.
En el primer caso solo un cajero quedará fuera de la operación. En el segundo caso se quedan fuera todas las sucursales y nadie puede registrar las operaciones del banco.

De esta manera se concluye este capítulo, no sin antes resaltar la importancia de poder identificar los puntos críticos de la plataforma de sistema y telecomunicaciones, plataforma tecnológica, que los bancos tienen instalada para poder implementar los niveles de redundancia y respaldo apropiados para que no impacten las operaciones al momento de que ocurra una falla en hardware o software.

Además es de gran importancia establecer indicadores que permitan al administrador, gerente, y director llevar una gestión integral de la plataforma tecnológica para llevar a cabo la toma de decisiones no solo de manera activa, sino que se puedan anticipar a los problemas que se estén gestando por la mismas operaciones del banco, por el deterioro tecnológico, o porque las necesidades ya sean diferentes.

CAPÍTULO III: MARCO TEÓRICO

Objetivo particular

El objetivo de este capítulo es presentar los conceptos teóricos de la planeación estratégica que permitan tener una concepción global de la empresa en estudio, además, presentar una metodología para la administración de riesgo que permita abordar el riesgo operativo en el capítulo IV.

3.1 Gestión.

En toda empresa se requiere de la definición de procesos, procedimientos, políticas y manuales organizacionales y de usuario para poder ofrecer sus productos o servicios a sus clientes.

Adicionalmente, se requiere que la empresa cuente con objetivos estratégicos, metas, estrategias etcétera para que así se conduzcan las acciones hacia la razón de ser de la empresa. Para poder evaluar los resultados en determinado periodo de tiempo es necesario un sistema de control. Como podemos ver en la Figura 3.1, llevar a cabo una gestión de la organización involucra a la organización: directivos, gerentes y personal operativo.

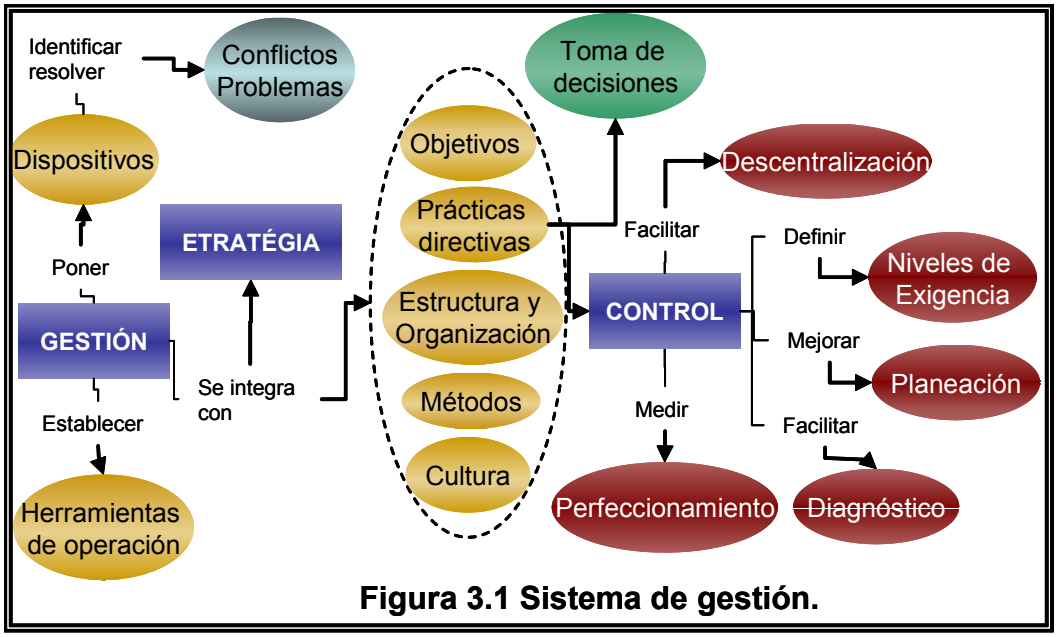


Figura 3.1 Sistema de gestión.

De manera global, Ackoff afirma que, todo sistema administrativo debería cumplir cuatro funciones básicas:

1. Identificar los problemas (Incluyendo amenazas y oportunidades),
2. Tomar decisiones,

3. Controlar las decisiones tomadas, y;
4. Proporcionar la información necesaria para realizar cada una de las tres primeras funciones.[1]

Una vez detectados los problemas, es necesario hacer uso de la información interna y externa para transformarla en acciones, actividades o procesos que se orienten al cumplimiento de objetivos y estrategias.

Es importante definir el término gestión, para ello revisamos algunas definiciones:

Paul de Bruyne describe que la gestión comprende a la vez un saber y una práctica que apela al mismo tiempo a la ciencia, es decir, a los conocimientos más o menos exactos, y al arte, esto es, al juicio y a la creatividad[2].

Desde el punto de vista de Pedro Marroquín, la gestión consiste en ejecutar las acciones conducentes para lograr un objetivo. Estas consisten en simples ordenes, trámites, presupuestos, estudios, en fin, todas las actividades que se comprenden para obtener el objetivo propuesto[3].

La gestión dentro de la empresa involucra la toma de decisiones, objetivos, estrategias, la estructura organizacional, métodos y cultura empresarial. Tomando en cuenta las definiciones anteriores, podemos definir la gestión empresarial, de la siguiente manera:

Gestión es tomar las estrategias, los objetivos, la estructura y cultura organizacional para alinearse con las prácticas directivas que, al establecer la tecnología a usar, las herramientas de operación y dispositivos para resolver conflictos y problemas se alcancen las metas y de esta manera estar siempre orientados hacia la misión y visión de la empresa.

3.2 Planeación estratégica.

Un empresario que desee iniciar u negocio, requiere identificar en primera instancia tres bloques: análisis de la organización, diseño estratégico y selección e implantación y control. Esto conduce a una desagregación jerárquica y ordenada, partiendo de la imagen objetivo, esto es la visión y misión.

El análisis de la organización contempla cuatro puntos trascendentales en la concepción de lo que se quiere hacer y a donde se desea llegar, en esta etapa se definen:

- Visión y misión,
- Análisis interno,
- Análisis externo,
- Objetivos a largo plazo u objetivos estratégicos.

[1] ACKOFF, Rusell L. Rediseñando el Futuro. México DF. Noriega Editores, 1991, p.
[2] De BRUYNE, Paul, Teoría moderna de la administración de empresas, Aguilar, Madrid, 1983, p. 287.
[3] MARROQUIN SUÁREZ, Pedro, La gestión de los sistemas de control de calidad, compañía editorial continental, México, 1989, p. 15.

El diseño estratégico y selección, es el siguiente nivel de desagregación, los puntos que se definen son:

- Diseño de estrategia maestra,
- Estrategias específicas,
- Programación y presupuestación.

Implantación y control, tercera y última etapa de desagregación se definen:

- Proyectos estratégicos de acción, y;
- Diseño de la implantación y control.

En la figura 3.5 se muestran las tres etapas de la planeación estratégica, como se puede ver, conforme se abordan etapas inferiores, se van desagregando de manera jerárquica y ordenada la visión, hasta concluir con acciones más específicas.

Para mayor detalle de la planeación estratégica consultar el anexo 2.

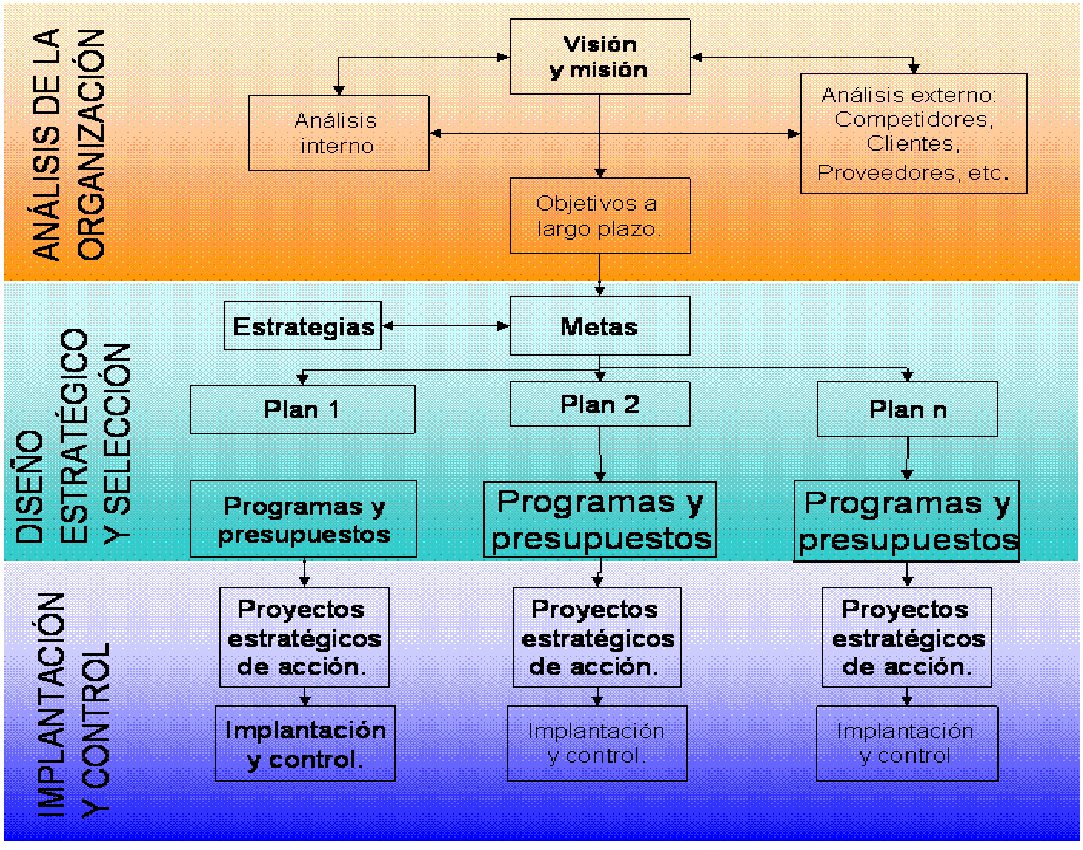


Figura 3.5. Etapas de la planeación estratégica.

3.3 Control.

La última fase de la planeación estratégica consiste en implementar un mecanismo de control dentro del sistema que se este abordando.

Ackoff asevera que el control es evaluar las decisiones y que este proceso de control involucra cuatro fases:

1. Pronosticar los resultados de las decisiones en la forma de medidas de rendimiento.
2. Reunir la información sobre el rendimiento real.
3. Comparar el rendimiento real con el pronosticado.
4. Cuando se detecta una decisión deficiente, corregir el procedimiento que la produjo y corregir sus consecuencias hasta donde sea posible.

Un indicador es un dato estadístico que hace referencia a la existencia de un fenómeno que puede dar una visión integral y además permite elaborar juicio sobre el funcionamiento de un sistema o proceso. De esta manera, un indicador de riesgo operativo es una variable aleatoria que es usada para proveer una visión de eventos futuros de riesgo operativo.

Los indicadores se caracterizan por ser útiles en la toma de decisiones, son verificables, no deben presentar sesgo estadístico o personal, deben tener una aceptación institucional, debe existir una correspondencia entre la información que provee el indicador y el fenómeno objeto de estudio, esto es, que debe ser válido. También debe ser confiable, es decir, debe medir lo mismo en diferentes momentos y en diferentes contextos y, por último, deben ser fáciles de interpretar.

Los indicadores pueden ser de gestión o de desempeño. Los primeros se enfocan a los procesos clave con los que opera la entidad.

Los indicadores de desempeño miden el logro de los objetivos de programas o actividades que reflejan el cumplimiento de la misión y de las metas de la institución o departamento, por otro lado, estos indicadores necesitan un punto de referencia contra el cual comparar. Es por eso que podemos decir que si el indicador de desempeño se aproxima al punto de referencia entonces se ha mejorado, de lo contrario, hay retroceso o se mantiene sin cambios.

3.4 Administración del riesgo.

La administración del riesgo es el segundo elemento que analizaremos como parte fundamental para el análisis del riesgo operativo.

La administración del riesgo involucra la cultura, procesos y estructuras de una organización que permita alcanzar oportunidades potenciales de negocio, de tal manera que se contrarresten los efectos adversos.

Para este proceso de administración del riesgo, se toma el estándar AS/NZ 4360 2004, un estándar preparado por los comités de Australia y Nueva Zelanda.

El proceso de administración del riesgo consiste de la aplicación sistemática de políticas de administración, procedimientos y prácticas de comunicación, establecer el contexto, identificar, analizar, monitorear y revisar el riesgo, ver figura 3.6.

a) Comunicar y consultar. Dentro del proceso de administración del riesgo, es de gran importancia que en cada paso, se consulte y se comunique. De esta manera se recomienda generar un plan de comunicación que involucre a los directamente involucrados internos y externos desde las primeras etapas del proceso. El impacto de las decisiones tomadas es considerablemente positivo desde el punto de vista de los directamente involucrados. Contar con un equipo de consulta, es útil para ayudar a definir el contexto de manera apropiada, para juntar áreas expertas diferentes para el análisis del riesgo, para asegurar que diferentes puntos de vista son apropiadamente considerados en la evaluación del riesgo y para la administración del cambio apropiado durante el tratamiento del riesgo. De esta manera se identifica a los responsables o propietarios de cada riesgo dentro de la organización y se establecen los compromisos de los stakeholders o directamente involucrados, y así, si identifican los beneficios de los controles particulares y del apoyo al plan.

b) Establecer el contexto. En este paso, se definen los parámetros básicos en los cuales el riesgo debe ser tratado y se establece el panorama para el resto de la administración del riesgo, según el estándar AS/NZ 4360 2004, para tener este contexto es necesario desglosarlo.

   El contexto externo e interno es el mismo análisis que se realiza en el punto 3.4, en la sección de análisis de la organización.
   La definición del alcance y la frontera de una aplicación para la administración del riesgo se deben tomar en cuenta los siguientes puntos:

   - Definir la organización, procesos, proyectos o actividades y establecer sus metas y objetivos.
   - Especificar la naturaleza de las decisiones que se deben tomar.
   - Definir la duración de las actividades de los proyectos o las funciones en términos de tiempo y lugar.
   - Definir el detalle de las actividades que se llevarán a cabo en la administración de riesgo.

   De esta manera es necesario establecer el rol y las responsabilidades que las diferentes áreas de la organización asumen en el proceso de la administración de riesgo; de igual manera la relación existente entre las actividades de los diferentes proyectos o las diferentes áreas.
   En la sección de desarrollo de criterios de riesgo, se deciden los criterios bajo los cuales debe ser evaluado el riesgo. Definir qué riesgo sí se considera y cuál no, esto puede decidirse por el impacto del riesgo, por la probabilidad de ocurrencia o por ambos.

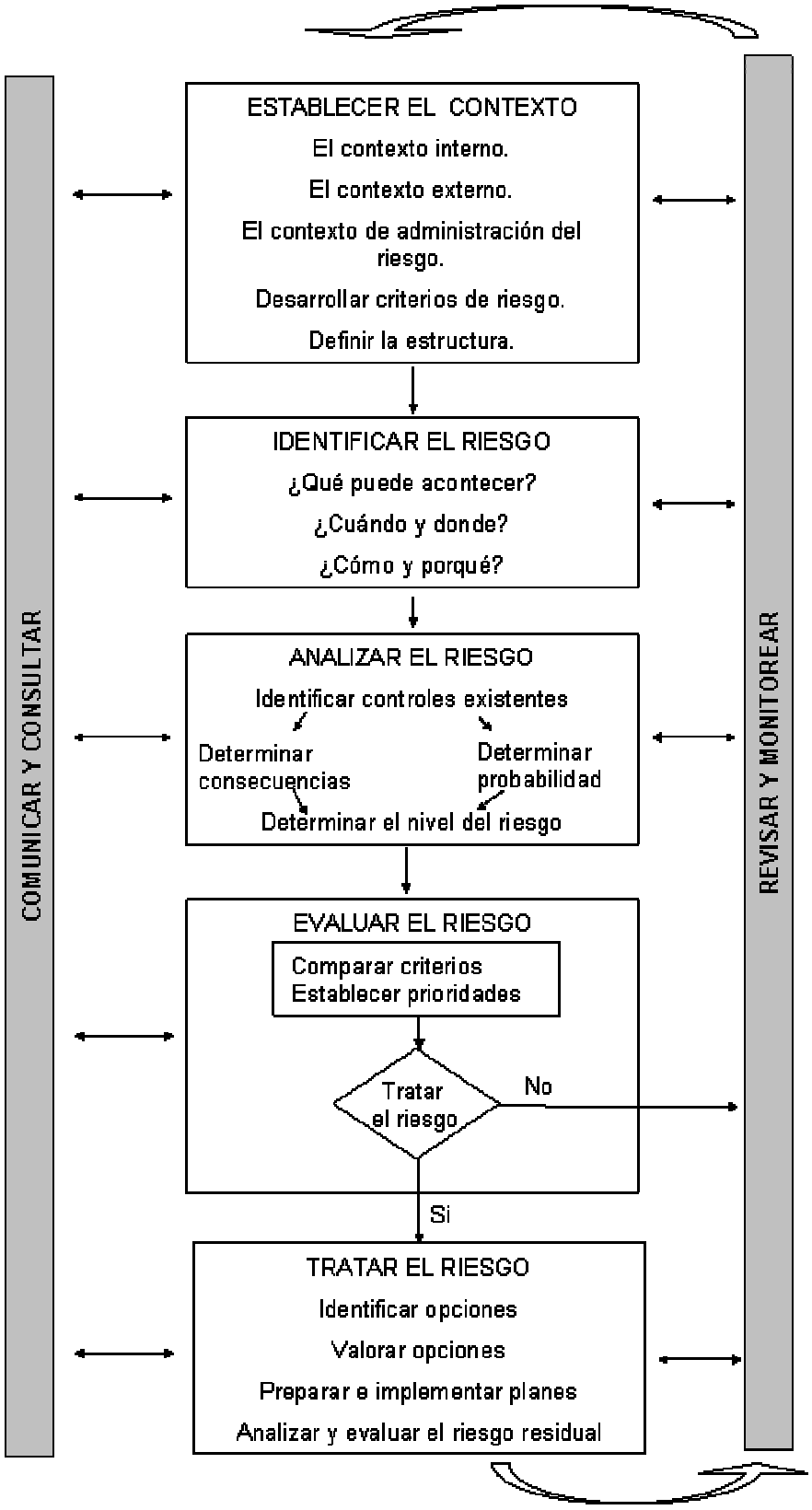


FIGURA 3.6 PROCESO DE ADMINISTRACIÓN DEL RIESGO

c) Identificar el riesgo. Este paso busca identificar los riesgos que deben ser administrados, el riesgo que no se logra detectar en este proceso se excluirá en el análisis de los pasos siguientes.

¿Qué puede suceder, cuándo y dónde? El objetivo de estas preguntas es consolidar una lista de fuentes de riesgo y eventos que pueden tener un impacto en cada uno de los objetivos identificados en este contexto. Estos eventos pueden prevenir, degradar o incluso presentar mejora considerable sobre los objetivos de la empresa.

¿Por qué y cómo puede suceder? Una vez identificado lo que puede suceder, es necesario considerar posibles causas y escenarios. Hay muchas formas en la que un evento se puede presentar. Algunas técnicas que se pueden utilizar para la identificación de riesgo pueden ser: consulta a expertos, lluvia de ideas, análisis de escenarios o alguna otra técnica participativa.

d) Analizar el riesgo. El análisis del riesgo es crear una cultura, un concepto dentro de la empresa de lo que es el riesgo. Este análisis provee una entrada para las decisiones sobre si se debe tratar o no, también pensar en las estrategias en función del costo beneficio que esto implica. Este proceso consta de dos pasos fundamentales: identificar controles existentes e identificar consecuencias y probabilidades.

- Identificar controles existentes, implica ver los procesos existentes, dispositivos o prácticas que actúan para minimizar el riesgo negativo o mejorar el riesgo positivo y valorar las fortalezas y debilidades.

- Consecuencias o severidad y probabilidades o frecuencia. Un evento puede tener múltiples consecuencias y afectar objetivos diferentes. Las consecuencias y las probabilidades se combinan para producir el nivel de riesgo. Para estimar las probabilidades y consecuencias se pueden usar técnicas de análisis estadístico. Para hacer estas estimaciones se puede acceder a fuentes de información como:

    - Registros históricos.
    - Experiencia relevante.
    - Literatura relevante.
    - Investigación de mercado.
    - Resultados de investigaciones públicas.
    - Experimentos y prototipos.

Dependiendo de la calidad y de la cantidad de la información los tipos de análisis pueden ser cualitativos, semi-cuantitativos y cuantitativos.

Para el caso del análisis cualitativo, se tiene poca información sobre la magnitud y las probabilidades por lo que se usan palabras para describir la magnitud potencial de las consecuencias que puedan ocurrir. Este tipo de análisis puede ser usado para casos en los que se inicia la administración del riesgo o para cuando los datos numéricos o las fuentes de información son inapropiados para realizar un análisis cuantitativo.

Para el análisis semi-cuantitativo, a las escalas usadas en el análisis cualitativo se les asignan valores aproximados, magnitudes de las consecuencias y probabilidades que sin ser precisas dan un rango aproximado. Es importante reconocer las limitaciones en los cálculos y las fórmulas utilizadas para no generar inconsistencias o salidas inapropiadas.

El análisis cuantitativo usa valores numéricos para las consecuencias y para las probabilidades usando datos con mayor confiabilidad. La calidad del análisis depende de la precisión y de la cantidad de la información de los valores numéricos y de la validez del modelo usado.

Cuando las formas de análisis del riesgo son imprecisas, se puede efectuar un análisis de sensibilidad para probar los efectos de incertidumbre en la suposición de datos.

e) Evaluar el riesgo. En esta fase de evaluación del riesgo, se toman decisiones basadas en los resultados obtenidos del análisis del riesgo, decidiendo qué riesgo necesita ser tratado y la prioridad que éste tendrá.
La evaluación del riesgo involucra la comparación del nivel de riesgo encontrado durante el proceso de análisis con los criterios de riesgo establecidos cuando el contexto fue considerado. En este proceso de evaluación se decide el nivel de riesgo que puede tolerar la empresa, el riesgo que se debe transferir a otras instituciones y el riesgo que no impacta a la institución.

f) Tratar el riesgo. El tratamiento del riesgo, identifica el rango de alternativas para el tratamiento de éste. Dichas alternativas pueden ser:

1. Evitar el riesgo al decidir no iniciar o continuar la actividad que se expone a dicho riesgo
2. Cambiar la probabilidad del riesgo, reduciendo la probabilidad del impacto negativo.
3. Cambiar las consecuencias, con esto se reduce su impacto. Esto se puede hacer con la creación de planes de continuidad del negocio donde se describen los procedimientos a seguir una vez acontece el evento.
4. Compartir el riesgo. Esto involucra a terceras entidades que bajo determinados acuerdos se comprometen a compartir cierto nivel de riesgo, ya sea de manera parcial o total.
5. Retener el riesgo. Una vez que el riesgo se ha modificado o compartido queda cierto nivel que se retiene o que asume la organización.

En la valoración se debe seleccionar la opción que mejor se adecue tomando en cuenta el costo de implementar cada opción contra los beneficios derivados de esto. Es importante considerar todos los costos directos e indirectos y los beneficios tangibles e intangibles y de esta manera medirlo en términos financieros.

Preparar e implementar los planes. El propósito del tratamiento de los planes es documentar cómo deben ser implementadas las opciones seleccionadas, esto puede incluir: acciones propuestas, recursos requeridos, responsabilidades, tiempos, medidas de desempeño y, reporte y monitoreo de requerimientos. Los planes deben estar integrados con el proceso de administración del presupuesto de la organización.

g) Revisar y monitorear. La revisión continua es esencial para asegurar que el plan de administración sigue siendo vigente. Los factores que pueden afectar la probabilidad y las consecuencias de un evento pueden cambiar, como también pueden cambiar los efectos de los factores de viabilidad o costo por el tratamiento de estas opciones, es la razón por la que es necesario repetir regularmente el ciclo de administración del riesgo. Monitorear y revisar también involucra aprender lecciones del proceso de administración de riesgo a través de la revisión de los eventos, el desarrollo de planes y sus impactos.

3.5 Construcción de indicadores de desempeño.

Para la construcción de los indicadores de desempeño se sugieren cinco pasos:

a) Establecer un marco conceptual o modelo teórico. Se recomienda el Enfoque Sistemas.

b) Objetivos estratégicos.

1 Imagen objetivo
2 Factores clave de éxito.
3 Prioridades

c) Elaborar una definición preliminar de los indicadores para cada uno de los factores críticos de éxito.
Se sugiere elaborar los indicadores con un enfoque participativo para que los directamente involucrados y expertos en el área definan en conjunto lo que mejor les convenga.

Para cada indicador elaborar: un nombre, fórmula de cálculo, frecuencia de cálculo, información requerida (Identificando variables, fuente y responsable de la información) y, descripción de variables que consiste en un texto que explique claramente la variable

3.6 Conclusiones.

Con los temas presentados, concluimos lo siguiente:

- Conocer los elementos teóricos de planeación estratégica permitirá que el esfuerzo de los involucrados se dirijan a un fin común.
- La planeación estratégica evitará objetivos encontrados que impidan o retracen el logro de la misión de la empresa.
- No se puede abordar un tema particular como el riesgo operativo sin tener el panorama global.
- Con la metodología presentada, se le da orden y formalidad al análisis en cuestión.
- La metodología presentada es sencilla de aplicar y tiene la ventaja de cubrir todas las fases o etapas de la administración del riesgo.

CAPÍTULO IV: PROCESO METODOLÓGICO

Objetivo.

El objetivo de este capítulo es presentar explícitamente la metodología para la administración del riesgo operativo en el área de Tecnología de Información (TI), proponer un conjunto de indicadores de riesgo operativo y un prototipo de base de datos para registrar las principales características de los eventos del riesgo operativo de TI.

4.1 Elementos clave.

En los capítulos anteriores se han abordado temas sobre el riesgo operativo, la diversidad en hardware y software con la que cuenta el departamento de Tecnología de Información, la planeación estratégica de la empresa y la metodología para la administración del riesgo. Brevemente recapitulamos los elementos clave:

Riesgo Operativo es: "*el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación*".

Dentro de la clasificación de eventos de riesgo de pérdida, las categorías relacionadas con Tecnología de Información, son:

1. Fraude externo. En la subcategoría de seguridad en los sistemas.

2. Incidencia en el negocio y fallos en los sistemas. En la subcategoría relacionada con sistemas: Hardware, software, telecomunicaciones e interrupción o incidencias en el suministro.

En el capítulo tres, se presentan las pautas para contar con una planeación estratégica de cualquier institución que tenga aspiraciones a largo plazo: planteamiento de la visión, misión, objetivos estratégicos, metas, etcétera. Esto se hace con el objetivo de que todas las tareas, actividades, proyectos, programas, y metas se encuentren enfocados a cumplir objetivos claros y específicos que define la alta dirección.

En este caso particular, se toman dichas pautas estratégicas para ser consistentes con el análisis del riesgo operativo en el área de Tecnología de Información, a través de la metodología para la administración del riesgo AS/NZ 4360 2004.

Pensando en un enfoque de sistemas, permite ver el área de TI como un conjunto de elementos interrelacionados entre sí: elementos de entrada que ingresan en un proceso de transformación para tener como salida servicios que están orientados a cumplir objetivos y programas estratégicos.

En la figura 4.1, se identifican tres partes importantes: las entradas, los procesos y las salidas.

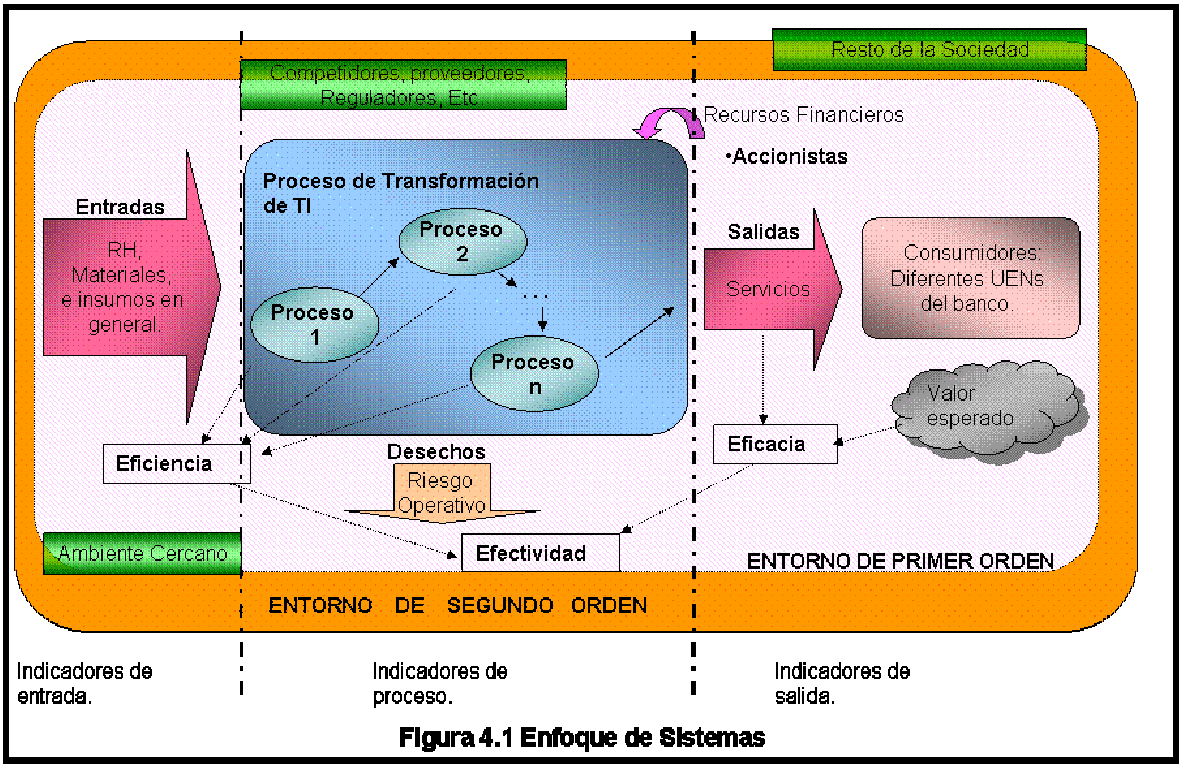


Figura 4.1 Enfoque de Sistemas

En las entradas se contemplan recursos humanos, materiales e insumos en general. En el proceso de transformación, se usan las entradas para dar valor agregado y, finalmente se tienen las salidas, que son las entradas con valor agregado.

Las salidas, esto es, los servicios que TI ofrece a las UENs del banco, son el producto final, el resultado que aportan a alcanzar objetivos y estrategias.

Los desechos, pueden ser diversos, pero aquí consideraremos como desechos todo lo que puede impactar en el logro de los objetivos estratégicos de la empresa, es decir, el riesgo en el que incurre la empresa por querer alcanzar objetivos, misión y visión. Que en este estudio se limita al riesgo operativo en el área de TI. En la figura 4.1 se muestra el proceso, y lo importante es ubicar dónde se encuentra el riesgo operativo en este sistema.

4.2 Pautas estratégicas.

El objetivo de esta sección es definir una visión, una misión y objetivos estratégicos en el área de TI, para que al momento de presentar las pautas de administración de riesgo en el punto 4.3, permita tener un horizonte más específico.

4.2.1 Análisis del entorno.

En el análisis del entorno se analizan las fuerzas externas que impactan de alguna u otra manera el área de TI. De esta manera, se analizan los competidores potenciales, productos sustitutos, proveedores, compradores y competidores directos.

Competidores potenciales. En el sector financiero, no es posible pensar que el área de TI cuente con competidores potenciales, ya que es un área de apoyo a las demás unidades de negocio y los mismos directivos establecen la estrategia que mejor le convenga a las necesidades de la institución para hacer de TI un área que de soluciones a las necesidades de las unidades estratégicas de negocio.

¿Cómo impactan los competidores potenciales al desempeño de TI?

Los competidores potenciales no ejercen ningún impacto negativo al interior de TI.

Productos o servicios sustitutos. TI es un área de servicios que no se ve afectada por servicios sustitutos. Puede darse el caso que como estrategia TI puede optar por servicios de terceros para implantar una solución o servicio y de esta manera reducir el número de empleados contratados directamente por el banco, pero el área como tal no puede ser reemplazada.

¿Cómo impactan los productos sustitutos al desempeño de TI?

Los servicios o productos sustitutos no impactan al desempeño del área de TI

Proveedores. Los proveedores del área de TI de un banco son proveedores de tecnología o representantes de éstas, empresas certificadas en la implantación o administración de un producto, hardware o software:

Hardware:

- Equipo de cómputo.
- Equipo de comunicaciones redes LAN.
- Equipo de comunicaciones redes WAN.
- Firewall.

Software:

- Sistemas operativos.
- Bases de datos.
- CRM.
- ERP.
- Firewall.
- Antivirus.
- Aplicaciones de escritorio.
- Aplicaciones desarrolladas a la medida.
- Sistemas de mensajería.
- Sistemas de monitoreo y control de equipo de cómputo, telecomunicaciones y software.

¿Cómo impactan los proveedores al desempeño de TI?

Los proveedores son parte fundamental de la calidad de las soluciones implantadas en el banco y se puede ver en varios rubros:

Los tiempos de entrega en hardware y software. Siempre que existen nuevos proyectos se requiere de los proveedores y, por ser soluciones donde se involucra tecnología especializada, los tiempos de entrega van de uno a tres meses lo que impacta considerablemente en el término de los proyectos.

Tiempos de entrega de proyectos de desarrollo de software a la medida. Siempre que se inicia un proyecto de desarrollo de software se identifican dos equipos principales de personas: el equipo conocedor de la tecnología con la que se desarrollará la solución y los directamente involucrados en la problemática que son los que están dentro de las operaciones y saben de los requerimientos de recursos humanos, financieros, etcétera. El impacto en la solución se muestra en el momento que los directamente involucrados no tienen bien definidos sus requerimientos y necesidades y los proveedores de la solución diseñan un producto con menor capacidad o con características diferentes a las que finalmente se requiere, de esta manera se impacta en el tiempo de entrega y en la asignación de mayores recursos.

Tecnología no apegada a estándares internacionales. El impacto de contar con proveedores que ofrecen aplicaciones con tecnología propia o tecnología no apegada a estándares, se refleja en que el área de TI porque se casa con la solución y con el proveedor. No puede explotar la información con otras herramientas, el servicio y mantenimiento no lo puede dar más que el propietario lo cual no tiene más alternativas.

Fallas en las funciones de diseño del hardware y /o software. Cuando se toman decisiones en la selección de un producto de hardware o software, se lleva a cabo a partir de las especificaciones que define el proveedor y pruebas básicas del producto por parte de TI. Al momento de implantar la solución en un ambiente de producción, el producto no funciona como lo dicen las especificaciones o presenta errores de diseño, generando pérdidas considerables para el banco y el proveedor como HP, IBM, Microsoft, etcétera lo mas que hace es reconocer que es problema de diseño pero que el error ya lo corrigieron en la siguiente versión del producto.

Compradores. Los compradores de los servicios que ofrece el área de TI son las mismas unidades de negocio del banco.

¿Cómo impactan los compradores al desempeño de TI?

TI depende totalmente de sus compradores, es decir, las unidades de negocio del banco. Las estrategias para el área no solo las crea e implementa la dirección de TI, sino también las demás direcciones de acuerdo a lo que mas le convenga. De esta manera pueden decidir en reducir la nómina de TI y ofrecer los servicios a terceros.

Competidores directos. Los competidores directos del área no los tiene al interior del banco, lo que si tiene son las áreas de TI de los otros bancos.

¿Cómo impactan los competidores directos al desempeño de TI?

El impacto se refleja en la eficiencia en los sistemas de cómputo, tiempo de respuesta en efectuar las transacciones y la disponibilidad de la información que los clientes requieren. De esta manera el impacto se refleja en la cantidad de transacciones realizadas contra el total de transacciones requeridas.

4.2.2 Análisis Interno.

Para realizar el análisis interno, se hace de acuerdo a las Fortalezas, Oportunidades, debilidades y amenazas que presenta el área de TI.

Fortalezas.

1. Personal actualizado en el manejo de herramientas.
2. Área de investigación para nuevas tecnologías.
3. Seguridad y control de acceso a la información electrónica.
4. Disponibilidad de información.
5. Desarrollo de aplicaciones de software para ofrecer servicios en línea.

Debilidades.

1. Rotación de personal clave.
2. Sueldos de los empleados.
3. Caída de la red de datos.
4. Respuesta lenta de los sistemas.

Amenazas.

1. Robo de información electrónica.
2. Virus informático.

Oportunidades.

1. Acceso a la tecnología.
2. Incremento de acceso de clientes desde Internet.

4.2.3 Definición de la visión y misión.

Con el análisis del entorno y el análisis interno se identifican los factores importantes que impactan en el desempeño del área de Tecnología de Información, así primero se define un horizonte de tiempo, tomando en cuenta que el banco actualmente ya tiene instalada una base de infraestructura tecnológica y tiene recursos humanos, financieros y tecnológicos, en este horizonte de tiempo se orientarán los objetivos y se definirán las nuevas estrategias.

Dadas las recomendaciones que el comité de Basilea hace a los bancos, deben contar, a partir del año 2006, con la reserva de capital para hacer frente al impacto del riesgo operativo, por tal razón el horizonte de tiempo para contar con una disciplina en la medición del impacto del riesgo operativo debe estar enfocado para los siguientes cinco años.

La idea a futuro del área esta orienta a tener el liderazgo, ofrecer la mejor seguridad y disponibilidad de datos electrónicos y mayores servicios en línea a clientes, y minimizar el impacto del riesgo operativo.

Ya se tiene la idea a futuro, ahora es importante definir cómo se podrá alcanzar esta idea a futuro. Esto se alcanzará mediante un uso efectivo de los recursos humanos, tecnológicos y financieros, cumpliendo con los objetivos en telecomunicaciones, cómputo e informática.

Una vez definidos el horizonte, la idea a futuro y los medios con los que se alcanzara la idea a futuro, se define la visión:

Visión. Para el año 2010, ser la mejor área de Tecnología de Información, comparada con las áreas de TI de los otros bancos, en ofrecer seguridad y disponibilidad de datos electrónicos, mayores servicios en línea a los clientes del banco, y minimizar el impacto del riesgo operativo mediante la efectividad en el uso de de los recursos, cumpliendo los objetivos en telecomunicaciones, cómputo e informática.

Para la definición de la misión se toman en cuenta los siguientes puntos:

1. Identificar las actividades necesarias para llegar a ser lo contemplado en la visión.

    a) Automatizar los procesos del negocio.
    b) Ofrecer disponibilidad, control de acceso y seguridad de la información almacenada y transmitida de manera electrónica al interior y exterior del banco.
    c) Implementar una metodología para la medición, administración y control del riesgo operativo

2. Identificar los productos o servicios a ofrecer.

    a) Servicio de red de datos (LAN y WAN).
    b) Servicio de cómputo (Servidores, computadoras personales, firewall, etc.)
    c) Servicio de aplicaciones y bases de datos.
    d) Disponibilidad y seguridad de la información.

3. Identificar que necesidades se deben cubrir a los clientes.
   Las necesidades de los clientes se cubren con los servicios definidos en el punto dos.

4. Identificar a los agentes internos a la empresa.

    a) Personal de base de datos.
    b) Personal de mesa de ayuda.
    c) Personal de sistemas operativos.
    d) Personal de redes (LAN).
    e) Personal de telecomunicaciones (Redes WAN)
    f) Personal de seguridad de datos.
    g) Gerentes y líderes de proyecto.
    h) Directores y accionistas.

5. Identificar la imagen al exterior: ventaja competitiva.

   La imagen para el banco y sus clientes es ofrecer servicios seguros, alta disponibilidad y tiempos de respuesta cortos en los accesos de los sistemas.

6. Identificar el alcance geográfico.

   El alcance geográfico de los servicios del área de TI es a nivel nacional.

Misión: Contar con los recursos tecnológicos, hardware y software que den solución a las necesidades del banco por medio de proveedores posicionados en tecnología apegada a estándares, para automatizar los procesos del negocio; ofrecer disponibilidad, control de acceso y seguridad de la información almacenada y transmitida de manera electrónica tanto al exterior (proveedores, reguladores y clientes) como en el interior de la misma institución, manteniendo al personal técnico actualizado en las herramientas implementadas en la institución y a los gerentes y directivos capacitados para mejorar la toma de decisiones, además, crear una cultura para la administración, medición y monitoreo del riesgo operativo y de esta manera hacer una empresa rentable.

4.2.4 Objetivos estratégicos.

Para la definición de los objetivos estratégicos es necesario definir cuatro elementos importantes:

1. Imagen objetivo.

   Lo importante respecto a la imagen objetivo es, visualizar la empresa a mediano y largo plazo respecto a los siguientes elementos:
   a. Calidad en el servicio. Este elemento se visualiza como parte esencial para el éxito del área. Contar con el personal capacitado para la administración, puesta a punto y afinación de todos los componentes tecnológicos, de tal manera que las diferentes unidades de negocio del banco cuenten con la información y el servicio en el momento que lo requieran.

   b. Productividad. La productividad de los agentes involucrados en el área se reflejará en mediano y largo plazo por el adiestramiento, experiencia y capitación sobre la base tecnológica instalada.

   c. El crecimiento. El crecimiento del área de TI es dependiente del crecimiento que se de en las unidades de negocio del banco.
   d. La eficacia. La precisión y rapidez con la que se ejecuten los procesos marcaran diferencia con las áreas de TI de otros bancos.
   e. La eficiencia. Es clave para incrementar la eficiencia establecer métodos y procedimientos para la ejecución de procesos.

2. Factores clave de éxito.
   Para identificar los factores clave de éxito se tiene que hacer para cada uno de los elementos de la imagen objetivo.

   a. Calidad en el servicio.
      i. Reproceso.
      ii. Disponibilidad.
      iii. Seguridad.
      iv. Agilidad.

   b. Productividad.
      i. Capacitación.
      ii. Adiestramiento.
      iii. Capacidad tecnológica.

c. El crecimiento.
    i. Infraestructura.
    ii. Compatibilidad de sistemas.
    iii. Escalabilidad.

d. La eficacia.
    i. Rapidez.
    ii. Precisión.

e. La eficiencia
    i. Métodos.
    ii. Procedimientos.

3. Prioridades. En las prioridades, una vez que se tienen definidos los objetivos estratégicos se establece el orden de ejecución.
4. Parámetros de evaluación. En cuanto a los parámetros de evaluación, es importante definirlos para saber el grado en el que se alcanzan dichos objetivos. Estos indicadores quedan fuera del objeto de estudio de esta investigación.

De los cuatro puntos anteriores, se redactan los objetivos estratégicos como se muestran en la tabla 4.1.

Tabla 4.1. Objetivos estratégicos del área de Tecnología de Información

Prioridad	Verbo en infinitivo	Imagen Objetivo	a través de …	Factores clave de éxito
1	Mejorar	la calidad en el servicio	a través de	• Definición y documentación de procesos. • Disponibilidad de la base tecnológica. • Seguridad de acceso a la información.
2	Incrementar	la productividad	a través de	• La capitación y adiestramiento al personal involucrado. • Implantación de base tecnológica apropiada.
3	Ser	eficaces	a través de	• La rapidez y precisión para ejecutar los procesos.
4	Aumentar	la eficiencia	a través de	• La definición de métodos y procedimientos.
5	Fomentar	el crecimiento	a través de	• La adquisición de infraestructura. • Compatibilidad y escalabilidad en los sistemas.

Una vez que se ha definido la misión, la visión y objetivos estratégicos, la empresa sabe lo que quiere llegar a ser y a través de que medios.

A partir de esto, surgen diferentes vertientes de estudio, entre otros se tiene: vigilar que la empresa se dirija en la dirección de lo que desea ser, factores que pueden impactar en la realización de los objetivos estratégicos, la misión y la visión, es decir, tomar en cuenta los riesgos intrínsecos a los procesos y acciones a los que se encuentra expuesta el quehacer de la empresa.

El resto del análisis lo enfocaremos al riesgo operativo que el departamento de Tecnología de Información se encuentra expuesto. Es importante hacer hincapié en la estrecha relación que existe entre el estudio y definición de los valores estratégicos de la empresa y, el estudio y monitoreo del riesgo que puede impedir alcanzar las metas, planes y objetivos estratégicos. Una empresa puede estar alcanzando su metas, planes y su misión y venirse a la quiebra por no tener contemplado un determinado tipo de riesgo.

Por esta razón, en el análisis del riesgo operativo para el departamento de TI, tomaremos como puntos centrales los objetivos estratégicos y, a partir de esto, aplicaremos la metodología para la administración de riesgo presentada en el capitulo anterior.

4.3 Pautas para la administración del riesgo.

Una vez analizados los puntos estratégicos para el departamento de TI, el siguiente paso es identificar y analizar el riesgo operativo al que se encuentra expuesto el área, este análisis se ejecutará apoyados en la metodología AS/NZ 4360 2004. El objetivo no es evaluar la metodología, es utilizarla para identificar el riesgo operativo al que se encuentra expuesta el área, posteriormente proponer un conjunto de indicadores y un prototipo de sistema de información para almacenar la información necesaria para medir, evaluar y monitorear dicho riesgo.

Los puntos que se abordan son los presentados en la sección 3.4 del capítulo tres y se muestran en la figura 3.6.

4.3.1 Comunicar y consultar. En el área de TI la comunicación y la consulta a expertos internos y externos son la base para que los servicios se ejecuten en tiempo y forma.

Se identifican tres principales fases de los proyectos con el objetivo de establecer el mecanismo de comunicación y consulta, estos son: la fase del diseño, fase de desarrollo e implantación y la fase de operación.

En la fase de diseño se requiere de la participación, del aporte de ideas y recomendaciones tanto de directivos y operadores de la solución en la parte interna como de expertos externos en diseño, desarrollo e implantación de soluciones para TI.

Para definir las necesidades en el entorno interno, primero se establece el equipo responsable, después se determinan los directamente involucrados, posteriormente se convoca a reunión para participar en el aporte de ideas vía lluvia de ideas o técnica TKJ. Una vez que se definen los requerimientos se propone a los expertos externos a participar en la propuesta de la solución para dichos requerimientos. Para poder evaluar a las propuestas de los expertos externos se puede acudir a técnicas de decisión de criterios múltiples como PROMÉTHÉE-GAIA, Expert Choice, etc. para seleccionar la mejor opción. En la parte de comunicar a los involucrados se generan prototipos que reflejen las necesidades del área.

En la fase de desarrollo e implantación, es importante definir los canales de comunicación entre los responsables internos y los responsables externos, de tal manera, que todos los involucrados conozcan el proceso para reportar incidencias y hacer propuestas. En esta etapa se establece la metodología a usar para el desarrollo e implementación de la solución.

En la fase de operación, la manera para comunicar y consultar es contar con un sistema de indicadores que muestren el nivel de operación o nivel de alcance de los objetivos.

4.3.2 Establecer el contexto. La definición del contexto externo y el contexto interno se abordó en la sección 4.2.1 y 4.2.2 con el nombre de análisis del entorno y análisis interno respectivamente.

Lo siguiente que se debe hacer para establecer el contexto es definir los criterios contra los que se evaluara el riesgo, así como también definir la estructura de análisis.

En la definición de los criterios, sólo se limita al riesgo operativo relacionado con los sistemas propiedad del banco y responsabilidad de TI. Esto se desagrega en tres subcategorías:

- Fraude interno y externo. En la subcategoría de seguridad en los sistemas.
- Fallas en los sistemas. Hardware, software y telecomunicaciones.
- Fallas en la ejecución de las actividades por parte del personal involucrado.

Las demás categorías de riesgo operativo y otros tipos de riesgo quedan fuera de este contexto.

La estructura de análisis consiste en revisar los diferentes elementos de hardware, software, telecomunicaciones y seguridad, dentro los sistemas que se encuentren expuestos al riesgo operativo que impacten en los objetivos estratégicos del departamento de TI.

En cuanto al rol y responsabilidad, los encargados de identificar y reportar el riesgo son los directamente involucrados en la administración, configuración, desarrollo o instalación de dispositivos, software, etc. El área de riesgo será la responsable de valorar el costo beneficio del esfuerzo dirigido para minimizar el riesgo operativo.

En cuanto al tipo de riesgo operativo que se va tratar, es aquel que por su impacto y por su probabilidad genere pérdidas mayores al costo incurrido por implementar la infraestructura, y demás recursos necesarios para su administración.

4.3.3 Identificar el riesgo.

Para identificar el riego al que se encuentra expuesto el área de TI, se hacen las siguientes preguntas: ¿Qué puede suceder, cuando y donde? ¿Por qué y cómo puede suceder?

Estas dos preguntas se desarrollarán para la parte de hardware, software, telecomunicaciones, seguridad en los sistemas, fallas en el personal, procesos y legal.

¿Qué puede suceder en el hardware, cuando y donde?

1. Respecto a los servidores que alguno de sus componentes, procesador, disco duro, memoria, tarjeta de red, etc. deje de funcionar cuando este dando servicio en cualquier parte de la red de datos del banco.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder por no dar mantenimiento preventivo a los equipos o por irregularidad en el voltaje en la corriente eléctrica, por terminar el ciclo de vida de los componentes del servidor o por fallas de fabricación. En la mayoría de las veces el mismo sistema envía advertencia de las fallas de hardware. En ciertas ocasiones por ser un componente indispensable para el servidor simplemente el sistema no inicia.

2. El cableado de la red de datos puede ser desconectado de manera accidental en la parte donde esta conectado al servidor o del lado del swich cundo la red este en operación la red.

   ¿Por qué y cómo puede suceder?

   El cableado de servidores o estaciones de trabajo puede ser desconectado por los mismos responsables por no tener identificados y etiquetados los nodos de red o por personal que desconoce la función e importancia del nodo de red.

3. Los componentes de los switches y de los ruteadores, puertos, fuentes de poder, procesador, etc., dejen de funcionar cuando la red de datos este en servicio.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder por falta de mantenimiento preventivo al equipo de la red de datos, por variación en el voltaje de la corriente eléctrica o por fallas de fabricación.

4. Que el equipo de respaldo de energía eléctrica, plantas, UPS, etc., no funcione al momento que se presente un corte en el suministro de energía.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder por no probar antes el equipo de respaldo de energía ni la planta generadora lo sucede al momento que se presenta el corte al suministro.

5. Destrucción del hardware de un centro de datos.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder por una catástrofe en el edificio de procesamiento de datos. Se puede dar por terremoto, vandalismo, terrorismo, huracán, etc.

¿Qué puede suceder en el software, cuando y donde?

1. Que el sistema operativo o las aplicaciones no soporten la carga de trabajo de las aplicaciones instaladas cuando exista la mayor carga de requerimientos.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder por las características de los recursos de hardware o por las características del software, esto depende del número de transacciones que el servidor atienda por segundo, los síntomas son que el tiempo de respuesta del servidor es cada vez mayor o incluso la caída del sistema o aplicación.

2. Que el sistema operativo o las aplicaciones no funcionen como fueron diseñada, esto es, que presenten fallas de diseño y desarrollo.

   ¿Por qué y cómo puede suceder?

   Esto sucede porque el proveedor del sistema no prueba el sistema ante todo el universo de escenarios posibles en las que pudiera trabajar y cuando en una empresa se presenta, el sistema arroja resultados erróneos o consume el 100% de los recursos de hardware

3. Que las aplicaciones y sistemas operativos no se encuentren actualizados con recomendaciones del proveedor.

   ¿Por qué y cómo puede suceder?

   Esto se puede presentar por no actualizar a los responsables del sistema en las nuevas versiones del producto. Los proveedores de software emiten actualizaciones de mejora o corrección de problemas detectados en el sistema con el fin de mejorar su producto. Esto puede suceder de diferentes maneras, no detectando componentes de hardware, corrigiendo errores de funcionalidad o seguridad o dando funcionalidades adicionales.

¿Qué puede suceder en telecomunicaciones, cuándo y dónde?

1. Interrupción en la comunicación de los enlaces de la red WAN.

   ¿Por qué y cómo puede suceder?

   Puede suceder por que el proveedor tenga problemas con sus equipos, de mantenimiento preventivo o de manera accidental se corten las comunicaciones cuando la red WAN este operando.

2. Que los equipos de telecomunicaciones, ruteadores, antenas, etc., presenten fallas en sus componentes.

   ¿Por qué y cómo puede suceder?

   Esto se presenta debido a la falta de mantenimiento preventivo a los equipos, por problemas de suministro de energía eléctrica o por cumplir su ciclo de vida.

¿Qué puede suceder en la seguridad de los sistemas, cuándo y dónde?

1. Que los sistemas operativos o las aplicaciones presenten problemas de seguridad de acceso.

   ¿Por qué y cómo puede suceder?

   Esto sucede porque el fabricante del sistema operativo, por falta de control en el sistema de seguridad, deja "puertas abiertas" y las personas que estudian a fondo el sistema, normalmente hackers o piratas informáticos, las explotan y usan para dañar el sistema, robar información o atacar con virus informático.

2. Que se presente un ataque de virus a la red del corporativo.

   ¿Por qué y cómo puede suceder?

   Esto sucede por las razones explicadas en el punto anterior y, además, por no contar con sistema de antivirus en la empresa o por tenerlo y no mantenerlo actualizado con las ultimas actualizaciones de virus.

3. Que usuarios mal intencionados hacker, congestionen o bloquee los servidores que se publican a Internet.

   ¿Por qué y cómo puede suceder?

   Esto sucede porque existen usuarios en Internet que saben de la funcionalidad de los sistemas y envían cientos o miles de solicitudes al servidor, quitándole tiempo al procesador para atender a las solicitudes de los clientes.

4. Que un hacker, viole la seguridad de los sistemas y cause daño a la información o realice operaciones fraudulentas.

   ¿Por qué y cómo puede suceder?

   Porque sabe de las debilidades de los sistemas de seguridad y conocen de las aplicaciones que existen al interior del banco, la forma en la que se realiza es desde una computadora conectada a la red de Internet se viola la seguridad y se realizan las operaciones no permitidas.

¿Qué puede suceder en las actividades del personal, cuando y donde?

1. Que la red WAN se sature por información enviada entre las diferentes localidades.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder porque la cantidad de información intercambiada entre diferentes localidades es mayor a la capacidad de de los enlaces WAN y se requiera administrar de mejor manera el ancho de banda y la información transmitida. Esto se puede dar al momento que un usuario de una localidad envía información a un usuario de otra localidad sin considerar el tamaño de los archivos y las capacidades de los enlaces WAN.

2. Que la red LAN se sature.

   ¿Por qué y cómo puede suceder?

   Esto se debe a la cantidad de información enviada entre las computadoras y servidores de tal manera que se rebasa el umbral máximo de envio recepción.

3. Mala administración o configuración de los sistemas o equipos, así como también mal funcionamiento de aplicaciones propietarias.

   ¿Por qué y cómo puede suceder?

   Que el personal no este capacitado o adiestrado para la administración o configuración de los equipos, aplicaciones o sistemas operativos, de igual manera que no estén capacitados para el desarrollo de sistemas.

4. Que las aplicaciones no cubran las necesidades del negocio.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder porque las personas que toman las decisiones de selección de la aplicación no cuentan con los elementos y herramientas para poder realizar la mejor selección del producto o, si se trata del desarrollo de una aplicación, los directamente involucrados no conocían en su totalidad el negocio o no lo supieron expresar al momento de establecer los requerimientos.

5. Que el tiempo necesario para el diseño, desarrollo e implantación de un sistema sea mayor al establecido al inicio del proyecto.

   ¿Por qué y cómo puede suceder?

   Esto se puede presentar por dos razones, una puede ser por falta de conocimiento y adiestramiento por parte de los encargados del desarrollo o implantación de la solución o, porque el usuario final no sabe lo que requiere y los requerimientos se cambien en el transcurso del proyecto.

6. Que las aplicaciones no se desarrollen conforme a estándares.

   ¿Por qué y cómo puede suceder?

   Puede suceder porque el personal desconoce los estándares que predominan en el mercado, porque el proveedor de la solución no desea que terceros manipulen o conozcan la arquitectura o funcionalidad del sistema y se puede ofrecer como una solución más económica porque se casa a solicitar servicios al mismo proveedor.

7. Que el tiempo de entrega en la adquisición del hardware se retrase.

   ¿Por qué y cómo puede suceder?

El equipo de hardware se importa, los retrasos en los tiempos de entrega principalmente se deben a problemas aduanales o problemas de inventario por parte del proveedor.

¿Qué puede suceder en los procesos, cuando y donde?

1. Puede suceder que no exista procesos documentados y cada empleado lo ejecute a su manera, esto puede suceder a nivel operativo, a nivel administrativo o a nivel de regulación cuando se ejecuten las actividades, se documente o se reporte.

   ¿Por qué y cómo puede suceder?

   Esto puede suceder porque el proceso no se ha identificado como una actividad cotidiana y el usuario ejecuta las actividades y tareas de acuerdo a su contexto sin tener en cuenta el contexto real del proceso.

2. Puede suceder que los procesos y procedimientos existan pero simplemente no se aplican. Esto puede pasar a nivel operativo, a nivel administrativo o a nivel de regulación cuando se ejecuten las actividades, se documente o se reporte.

   ¿Por qué y cómo puede suceder?

   Esto puede ser causa de que los procesos no son fáciles de ejecutar y el usuario decide abandonar su ejecución.

3. Puede suceder que la aplicación de los procesos sea incorrecta. Esto puede pasar a nivel operativo, a nivel administrativo o a nivel de regulación cuando se ejecuten las actividades, se documente o se reporte.

   ¿Por qué y cómo puede suceder?

   Puede pasar por error del personal o por falta de conocimiento en la aplicación del proceso.

4. También puede pasar que los procesos estén documentados pero el usuario o empleado desconoce dichos procesos. Puede darse a nivel operativo, a nivel administrativo o a nivel de regulación.

   ¿Por qué y cómo puede suceder?

   Esto puede pasar porque no existen mecanismos de difusión de los procesos hacia todos los departamentos de la institución.

¿Qué puede suceder en cuestiones legales, cuando y donde?

1. Actualmente con el uso de Internet las operaciones entre clientes, proveedores y competidores es cada vez mas frecuente, de esta manera en el momento que se establecen contratos con clientes, proveedores y competidores existe responsabilidad de parte del área de TI y puede pasar que surjan problemas de incumplimiento de contrato ya sea por parte del banco, o por parte del cliente, proveedor o competidor. Esto se presenta cuando se ejecuten los compromisos a medias o no se ejecuten.

¿Por qué y cómo puede suceder?

Los incumplimientos de contrato por parte del banco pueden generarse en el momento de no tener la infraestructura funcionando en las condiciones ofrecidas a clientes, proveedores y competidores.

2. También puede suceder que en la integración del contrato con clientes, proveedores y competidores, por la complejidad que estos representan, no se analicen ni se establecen de manera precisa las cláusulas del mismo, generando espacio, rendija o boquetes donde los otras entidades puedan sacar ventaja de esta debilidad en la definición del contrato.

   ¿Por qué y cómo puede suceder?
   Esto puede suceder por que los contratos actuales involucra la participación de personal con perfiles diferentes y al momento de la integración solo se encuentran los responsables de la firma del contrato.

Después de haber identificado el riesgo, estamos en condiciones de crear un árbol jerárquico de fuentes de riesgo, estos se muestran en las tablas 4.1 y 4.2

4.3.4 Analizar el riesgo.

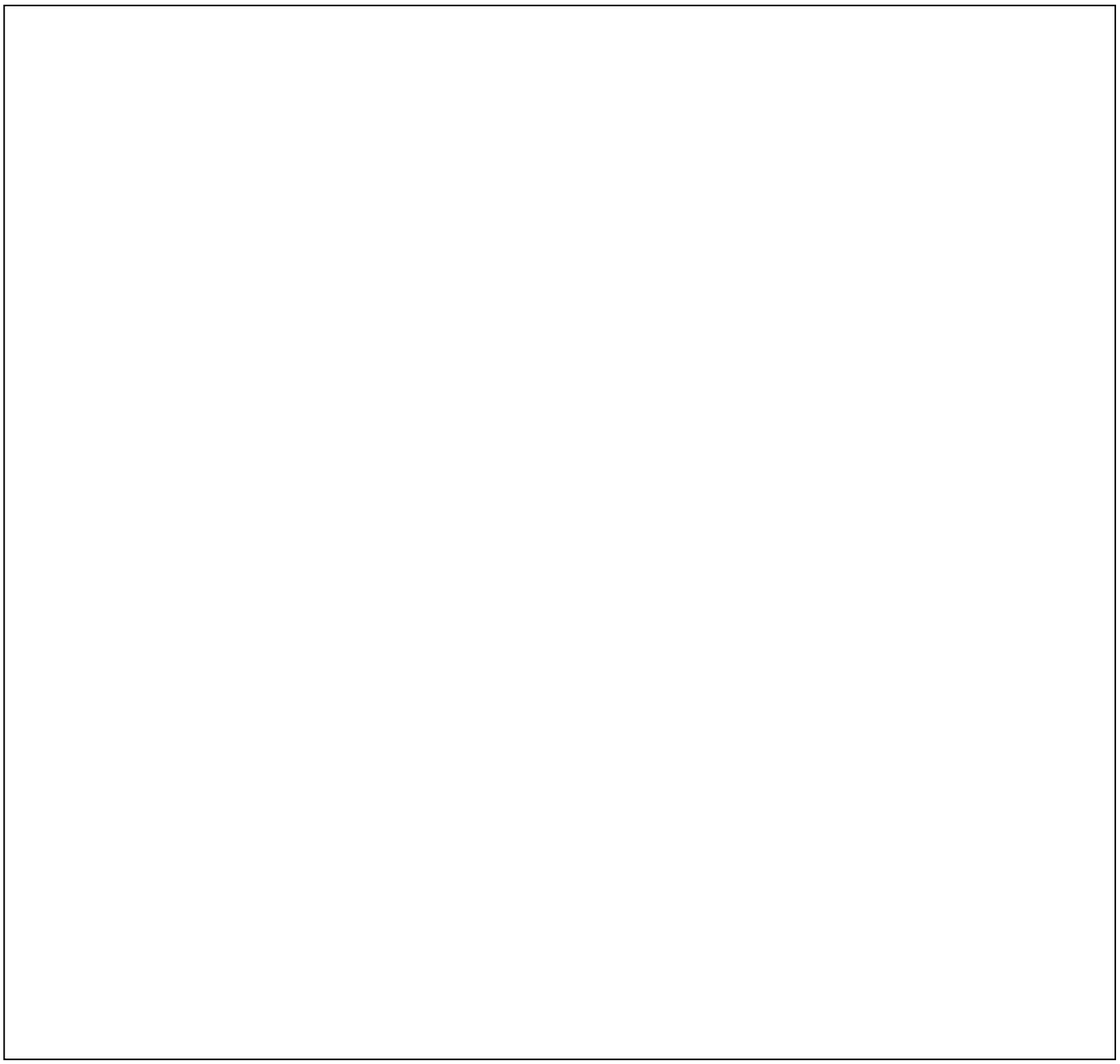
Analizar el riesgo implica desarrollar una cultura, un panorama de entendimiento respecto al riesgo ya que esto será el principal insumo para decidir si el riesgo necesita ser tratado y así determinar la mejor estrategia respecto al costo beneficio.

En esta etapa se identifican las consecuencias y las probabilidades con las pueden ocurrir, así como también, los factores que afectan a las consecuencias y probabilidades.

Como primer paso iniciamos por evaluar los controles existentes en el área de TI orientados a minimizar.

¿Qué controles existen para minimizar el riesgo en el hardware?

Independientemente del tipo de hardware, el área de TI da mantenimiento preventivo y correctivo a servidores y switches y ruteadores.



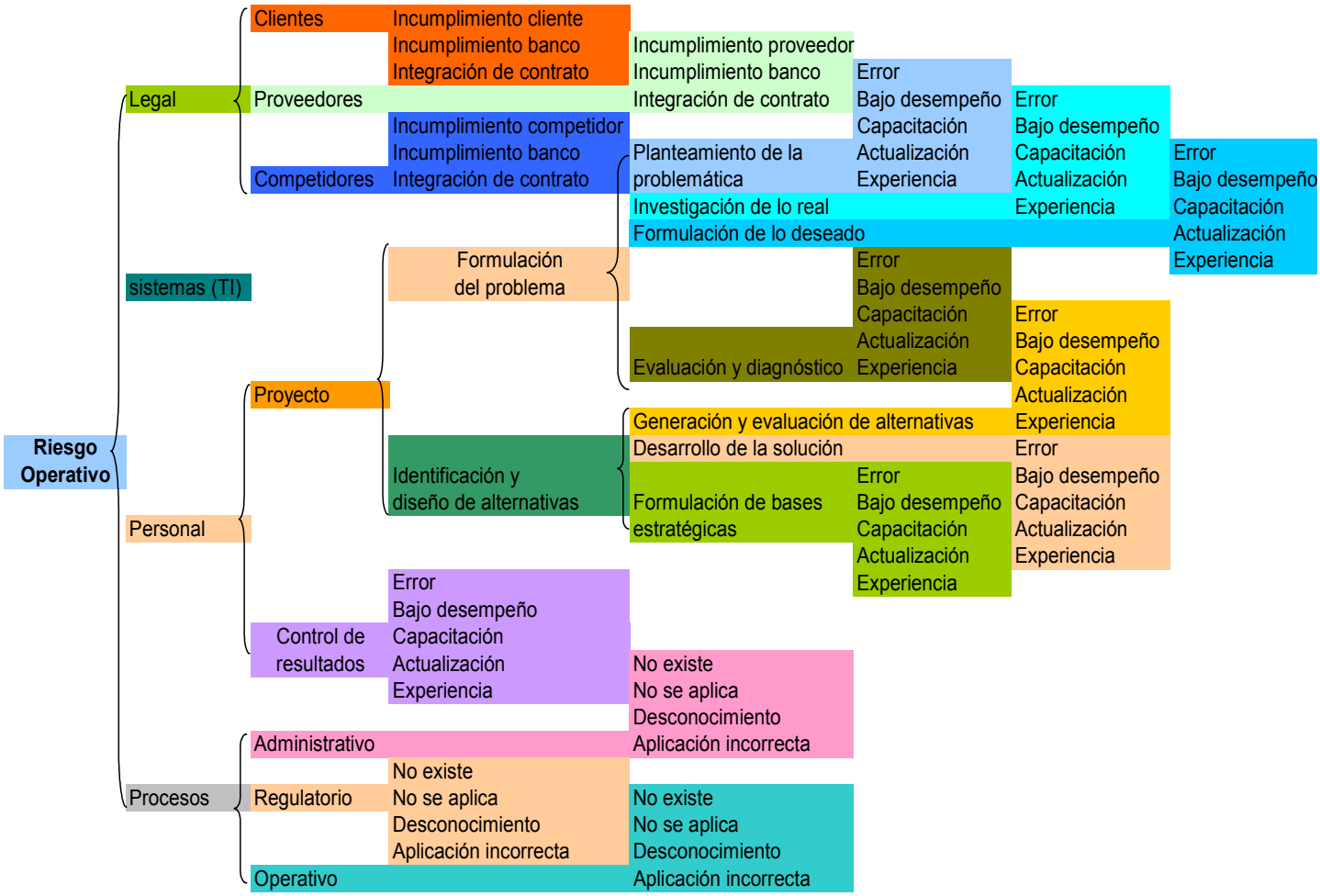


Figura 4.2. Árbol de riesgo operativo provenientes de riesgos legal, personal y procesos

Para el caso de servidores, dependiendo de lo crítico de las aplicaciones se instalan dispositivos redundantes, ya sean discos duros, tarjetas de red o procesadores. Para equipos que deben estar en servicio las 24 horas del día los 365 días del año existen sistemas, llamados clusters, que son de alta disponibilidad que son diseñados para seguir operando si alguna de los componentes falla.

Para evitar desconexión de nodos de la red de datos, los nodos deben estar etiquetados, si TI cuenta con una red de datos certificada por el proveedor la red se entrega etiquetada.

Cuentan con sistema de software para el monitoreo del hardware, para saber si el equipo esta en servicio o no.

Para respaldarse contra una catástrofe social o natural TI instala sitios alternos de procesamiento donde se replica toda la información del negocio, de tal manera que siempre se garantice el servicio a los clientes.

¿Qué controles existen para minimizar el riesgo en el software?

Igual que en el punto anterior, se conecta con un sistema de monitoreo de aplicaciones de tal manera que en tiempo real se sepa si esta funcionando o no.

Para el desarrollo de aplicaciones a la medida se cuenta con equipo de pruebas para valorar los escenarios posibles de funcionalidad. De igual manera se encuentran los responsables de investigar actualizaciones de los sistemas, quienes valoran los cambios que el proveedor ofrece o para el caso de las aplicaciones propietarias actualizarlas de acuerdo a las nuevas necesidades.

Se cuenta con un sistema de respaldo de la información del banco, dependiendo de la velocidad de cambio de los datos, el respaldo puede ser desde cada hora o diario. En el sistema de respaldo no solo se toma en cuenta lo crítico de la información que se esta respaldando, sino también la importancia de resguardar la información respaldada en un lugar seguro.

¿Qué controles existen para minimizar el riesgo en telecomunicaciones?

En relación a los enlaces WAN con proveedores, lo que se hace es contratar un enlace redundante con un segundo proveedor para seguir operando en caso de que uno falle con el servicio.

¿Qué controles existen para minimizar el riesgo en la seguridad de los sistemas?

En lo que concierne a seguridad el área de TI pone varios niveles de seguridad, estos son:

a) Saber la identidad del usuario, para esto se requiere una autenticación (dar un usuario y contraseña), autorización (saber que es lo que el usuario puede hacer en el sistema) y tener una bitácora de las operaciones que el usuario realizó.
b) Seguridad perimetral. Esto se logro con la instalación de firewalls que son dispositivos de hardware y software que tienen el control de los servicios que están permitidos ser usados del exterior a la red datos y viceversa.
c) Privacidad de datos. Para evitar que la información pueda ser interceptada entre el origen y destino, se cifran los datos creando una red privada de datos (VPN: Virtual Private Network) para lograr esto existen métodos como IPSec.[1]

¿Qué controles existen para minimizar el riesgo en las actividades del personal?

La institución tiene como control capacitar y adiestrar a sus empleados para el manejo de las herramientas usadas en la institución.

Se firma un contrato de confidencialidad de información para evitar el mal uso de la información propiedad del banco.

Separación de actividades. Con la finalidad de que un empleado no tenga el control completo sobre las actividades claves se separan para asignarlas a más de uno.

[1] IPSec es un conjunto de protocolos desarrollados por la IETF para poder intercambiar información (paquetes) de manera segura en la capa IP.

Tomando en cuenta que el personal puede irse a huelga o cerrar el edificio de procesamiento de datos se usan los centros alternos de procesamiento.

Se documentan las actividades que se realizan por medio de procedimientos para el caso de contingencia.

Una vez que se han determinado los controles existentes en el área de TI, el siguiente paso consiste en determinar las consecuencias que enfrenta el área por cada tipo de riesgo, además, establecer la probabilidad con la que se presentan en la institución.

Para definir las consecuencias y probabilidades es necesario tener acceso a los registros históricos y experiencia de la institución, si la institución cuenta con los registros y se tiene acceso a esta información se puede realizar un análisis cuantitativo. El problema que actualmente están enfrentando las instituciones financieras en el país es que no cuentan con registros para hacer un análisis cuantitativo es la razón por lo que están partiendo con análisis cualitativos y, para este estudio, no es posible tener acceso a la información del área de TI.

Las preguntas que se deben hacer para determinar las consecuencias y las probabilidades son:

¿Cuáles son las consecuencias económicas cada vez que el evento X se presenta en el área de TI?

¿Con que frecuencia se presentan durante el mes o durante el año?

De los resultados obtenidos con las preguntas anteriores se determina el monto de las pérdidas por concepto de los eventos del riesgo operativo en el área de TI.

4.3.5 Evaluar el riesgo. Una vez que el riesgo ha sido identificado y enlizado, el siguiente paso es evaluar que riesgo se tratará de minimizar, ya sea por las consecuencias o por la frecuencia que con la que se presenta.

En este proceso de evaluación se clasifica a los eventos de acuerdo a los parámetros que se establecen en el contexto, de tal manera que se catalogue a los eventos que no serán tratos porque cuesta más su administración que los costos en los que se incurre por que se presenten.

4.3.6 Tratar el riesgo.

En esta etapa se clasifica el riesgo de acuerdo a la manera que será tratado. Un grupo de actividades expuestas a cierto nivel de riesgo simplemente se dejaran de hacer para que de esta manera se evite la exposición al riesgo.
Otro grupo de actividades expuestas al riesgo se tomaran acciones para reducir la probabilidad de ocurrencia, otra categoría se reducirá la severidad, en otro grupo se compartirá el riesgo con terceros.

4.3.7 Revisar y monitorear.

El proceso de revisar y monitorear es un proceso cíclico y periódico porque las consecuencias y probabilidades cambian dependiendo de la tecnología usada, multas

impuestas por las autoridades reguladoras, cultura del riesgo operativo, medidas etc. Por esta razón se debe revisar cada año las consecuencias y frecuencia con la que se presentan los eventos.

Para poder monitorear se requiere contar con indicadores que permitan saber si se esta cumpliendo con el objetivo de minimizar el riesgo operativo en el área. Por esta razón, se profundiza esta sección con la propuesta de un conjunto de indicadores.

Para esto dividiremos los indicadores en: indicadores de desempeño tecnológico, indicadores de impacto del riesgo e indicadores de prevención del riesgo.

Indicadores de desempeño tecnológico.

Estos indicadores informan el nivel de rendimiento o desempeño en el que se encuentra el hardware o software, con el objetivo de ser preactivos en la toma de decisiones al llegar a cierto umbral predefinido por el proveedor como crítico. Para este tipo de indicadores, actualmente existen herramientas de monitoreo en tiempo real por lo que dentro del prototipo del sistema de información no se contemplan mas sin embargo es de gran importancia monitorearlos en tiempo real. Los indicadores propuestos en esta categoría son:

Uso de la red de datos LAN. Actualmente la tecnología usada en las redes de datos de área local es Ethernet, token ring no se aborda por ser una tecnología que va saliendo del mercado.

Las redes Ethernet, no importando la velocidad de transmisión 10 Mbps, 100 Mbps o 1000 Mbps se tiene como umbral de buen funcionamiento el 20% de su capacidad. Si en promedio se rebasa este umbral el servicio se degrada requiriendo mayor tiempo para acceso de datos o incluso perder conexión entre equipo o aplicación.

Uso de los enlaces WAN. Para los enlaces WAN se recomienda un porcentaje de uso del 90%. Es importante monitorear la carga de información de los enlaces entre localidades porque de esta manera se ve si han aumentado los requerimientos de envío y recepción de información o las aplicaciones no están siendo desarrolladas o configuradas de manera apropiada.

Uso de procesador de servidores. Para que los servidores tengan un buen desempeño se recomienda que el porcentaje de uso sea menor o igual al 75% de su capacidad, si se rebasa este porcentaje el desempeño se degrada, los tiempos de respuestas son mayores y corre el riesgo de que el sistema se “caiga”.

Indicadores de impacto del riesgo.

En esta sección se proponen indicadores de impacto del riesgo en los principales factores de medición del riesgo operativo, estos son: Tecnología de Información,
Personal, procesos e impacto legal.

Tecnología de Información.

Fiabilidad. Se define como el tiempo en el que un sistema o componente desempeña sus funciones sin ninguna falla visible al usuario. La fiabilidad se calcula de la siguiente manera:

$$\text{Fiabilidad} = \frac{\text{(Tiempo requerido en operación) - (tiempo sin operación)}}{\text{Suma de interrupciones}}$$

El nivel de fiabilidad dependerá de cada institución financiera dependiendo de sus servicios y clientes. Puede haber componentes del sistema que no son de alta prioridad y se acepten más interrupciones. El nivel de fiabilidad aplica para hardware, telecomunicaciones, seguridad y aplicaciones.

Disponibilidad. Es la probabilidad que un sistema este en operación en cualquier momento del tiempo programado para su uso. Se calcula de la siguiente manera:

$$\text{Porcentaje de disponibilidad} = 100\ X\ \frac{\text{(Tiempo requerido en operación) - (tiempo sin operación)}}{\text{Tiempo requerido en operación}}$$

Las empresas se enfocan a mejorar la disponibilidad de las aplicaciones y hardware y de maneara consecuente se mejora la fiabilidad.

Cuando hay acuerdos de niveles de servicio las empresas proveedoras del servicio o aplicación se comprometen a niveles de servicio del 99.99% o si no se trata de un servicio crítico hasta de un 99.9% de disponibilidad, esto implica que en 365 días al año solo puede estar fuera de servicio el sistema una u ocho horas respectivamente.

Estabilidad de software. La estabilidad de software se refiere a las actividades y recursos que las instituciones invierten para lograr que los sistemas se mantengan funcionando con las características diseñadas y que no tengan errores de programación. De esta manera se define el indicador:

$$\text{Impacto promedio por estabilidad de software:} = \frac{\text{Monto total por perdidas en estabilidad de software}}{\text{Numero total de perdidas}}$$

Infecciones de virus. Todas las empresas cuentan con sistema de antivirus para evitar ataques a las computadoras y servidores, aunque se cuente con estos sistemas, existen ataques que impactan en el desempeño de las actividades del personal. Para esto se requiere llevar un registro de las veces en que la empresa es atacada por virus y las pérdidas que se generan por ello.

$$\text{Impacto promedio por infección de virus:} = \frac{\text{Monto total por perdidas de infección de virus}}{\text{Numero total de infecciones}}$$

Violación a la seguridad. Contar con un registro por fecha de los ataques a los sistemas, seguridad perimetral y confidencialidad de la información, así como también determinar su impacto económico.

$$\text{Impacto promedio por violación a la seguridad:} = \frac{\text{Monto total por perdidas de violación a la seguridad}}{\text{Numero total de violaciones}}$$

Personal. Para identificar los indicadores que impactan en la parte de persona, estos se dividen en: control de resultados, formulación de problemas e identificación y diseño de alternativas.

En control de resultados, se tienen los siguientes:

Errores. Se calcula el impacto promedio por errores del personal.
Bajo desempeño. Se calcula el impacto promedio debido a que el personal no realice sus actividades por tener un bajo desempeño.
Capacitación. Es el impacto promedio debido a que el personal no esta capacitado en realizar sus actividades.
Actualización. Se calcula el impacto promedio debido a que el personal no se actualiza para realizar sus actividades.
Experiencia. Se calcula el impacto promedio debido a falta de experiencia del personal.

En lo que respecta a proyectos se tienen formulación de problemas e identificación y diseño de alternativas.

Formulación de problemas.

Planteamiento de la problemática.
Investigación de lo real.
Formulación de lo deseado.
Evaluación y diagnóstico.

El impacto promedio de cada una de las cuatro categorías anteriores, se calcula sumando el impacto resultante de errores, bajo desempeño, capacitación, actualización y experiencia entre el total de eventos registrados de estas cinco subcategorías.
Para el caso del prototipo, se hace el cálculo promedio a nivel de formulación de problemas.

Identificación y diseño de alternativas.

Generación y evaluación de alternativas.
Desarrollo de la solución.
Formulación de bases estratégicas.

El impacto promedio de cada una de las tres categorías anteriores, se calcula sumando el impacto resultante de errores, bajo desempeño, capacitación, actualización y experiencia entre el total de eventos registrados de estas cinco subcategorías.

En el prototipo el cálculo se hace a nivel de identificación y diseño de alternativas.

Procesos. Los indicadores respecto a los procesos se dividen en:

Administrativos.
Regulatorios
Operativos.

Para el cálculo del impacto de los tres puntos anteriores, se hace sumando el impacto registrado en las subcategorías: no existe, no se aplica, desconocimiento, aplicación incorrecta entre el total de eventos registrados en todas las subcategorías.

Legales. Los indicadores respecto al impacto legal se presentan en tres categorías:

Clientes.
Proveedores.
Competidores.

Para el calculo del impacto de cada uno de los puntos anteriores se hace sumando todos los eventos registrados en las subcategorías: incumplimiento cliente, incumplimiento banco e integración de contratos; entre el total de eventos registrados en las tres subcategorías.

Indicadores de prevención del riesgo. Para identificar los indicadores de prevención del riesgo se piensa en la inversión que el departamento hace para reducir este impacto. De igual manera que para el impacto del riesgo, se analizan los factores de Tecnología de Información, personal, procesos y legal.

Tecnología de Información.

Mantenimiento.
Disponibilidad.
Seguridad.
Bajo desempeño.
Redundancia.

Para calcular la inversión realizada en los cinco rubros anteriores se suma el total de inversión hecha en cada categoría de hardware: servidores, computadora, laptop, impresora, hub, switch, ruteador, LAN, WAN y firewall.

Personal.

Capacitación. En el proceso de capacitación se hace apto al personal para realizar sus tareas o actividades. En general se trata de una capacitación técnica relacionada con productos o herramientas que se usan en la institución. Este proceso consiste de un promedio de 160 horas para capacitación de software y tecnologías de hardware, tales como: Microsoft, IBM, HP y CISCO.

Para calcular las horas promedio de capacitación por empleado durante el año, HPC, para el área de TI, se define de la siguiente manera:

$$\text{Horas promedio de capacitación en el periodo por empleado.} = \frac{\text{Total de horas de capacitación a empleados de TI durante el año}}{\text{Total de empleados en TI}}$$

Actualización. La actualización prepara al personal para el manejo de las nuevas propiedades de las herramientas y aplicaciones que los proveedores emiten en las nuevas versiones de sus productos. Se requiere de un total de 40 horas promedio para la actualización por persona (esto se toma en base a los productos de proveedores como Oracle, Microsoft y HP).

Para calcular las horas promedio de actualización por empleado, se define de la siguiente manera:

$$\text{Horas promedio de capacitación en el periodo por empleado.} = \frac{\text{Total de horas de actualización a empleados de TI durante el año}}{\text{Total de empleados ya capacitados}}$$

Para los siguientes puntos se calcula la inversión orientada a la prevención del riesgo, teniendo en cuenta a lo que puede acontecer en proyectos y control de resultados.

Error.
Bajo desempeño.
Capacitación.
Actualización.
Experiencia.

Procesos

Para calcular la inversión en cada una de las categorías siguientes se suma la inversión hecha en las subcategorías: No existe, No se aplica, Desconocimiento y Aplicación incorrecta.

Administrativo.
Regulatorio.
Operativo

Legal

Para calcular la inversión en cada una de las categorías siguientes se suma la inversión realizada en: Incumplimiento cliente, Incumplimiento banco e integración de contrato.

Clientes
Proveedores
Competidores.

4.4 Prototipo del sistema de información.

Una vez identificado el riesgo, el siguiente paso es proponer una herramienta que permita llevar un registro de los eventos del riesgo que impactan a la institución, que permita calcular la severidad y la frecuencia de los eventos. Por otro lado el sistema debe ser capaz de registrar las acciones que la institución realice enfocadas a la prevención del riesgo.

El sistema de información integrado por la base de datos y la aplicación que procesa la información, permitirán a la institución usar la experiencia acumulada, para mejorar la toma de decisiones en la institución respecto a la prevención del riesgo.

De esta manera el sistema de información se compone de dos partes fundamentales: la base de datos y la interfase al usuario que permitirá almacenar y explotar la información de la base de datos.

4.4.1 Modelo de base de datos.

Diseñar un modelo de base de datos que permita almacenar los datos de eventos para obtener los indicadores, frecuencia y severidad, medidas preventivas, etcétera, es dar un paso muy importante para la medición y control del riesgo operativo.

La base de datos propuesta es una base de datos relacional, donde cada tabla representa una entidad de información y se relaciona con otras tablas por medio de identificadores únicos en la tabla, estos identificadores se denominan llaves primarias. El objetivo de la base de datos es poder almacenar la información de la empresa: empleados, direcciones, UENs, departamentos, así como también la información propia del negocio o problemática. En este caso es la información referente al riesgo operativo.

Del riesgo operativo, es fundamental poder registrar la frecuencia de los eventos y la severidad que estos tienen para la institución y las acciones que se toman para prevenir el riesgo. La severidad de cada evento puede ser de dos tipos: directa e indirecta y para el registro en la base de datos se requiere registrar ambos tipos.

La severidad directa es aquella que al presentarse un evento se deja de tener un ingreso específico o se incurre en una multa establecida por una entidad reguladora.

La severidad indirecta, cada institución debe estimar el impacto de acuerdo a experiencias propias, al tamaño del negocio y al volumen de operaciones ejecutadas. Por ejemplo: cuando se presenta una caída o lentitud en los sistemas, no hay una forma directa de estimar las pérdidas.

Esta base de datos esta compuesta por las siguientes tablas: Departamento, Empleado, Medidapreventiva, Puesto, Registroevento, Riesgo, y UEN.

La tabla Departamento, tiene como objetivo almacenar los diferentes departamentos que constituyen cada UEN y tambien registra las áreas de apoyo a como recursos humanos y TI. Los campos son los siguientes:

- Iddepartamento. Registra el identificador de cada departamento.
- Descripción. En este campo se almacena el nombre del departamento.
- IdUEN. Se registra el identificador de la UEN a la que pertenece el departamento.

El campo IdUEN determina la UEN a la que pertenece dicho departamento.

La tabla Empleado, tiene como objetivo almacenar la información correspondiente al empleado y la relación con las otras tablas, se compone de los siguientes campos:

- Idempleado: Es un identificador único que se le asigna al empleado y se convierte en llave primaria de la tabla.
- Nombre: Nombre del empleado.
- Apaterno: Apellido paterno.
- Amaterno: Apellido materno.
- Email: Correo electrónico del empleado.
- Direcciónтrabajo. Almacena la dirección donde se encuentra la oficina del empleado.
- Direccioncasa. Almacena la información del domicilio en el que vive el empleado.
- Iddepartamento. Es el identificador del departamento al que pertenece el empleado.
- Idpuesto. Es campo indica el identificador del puesto que tiene el empleado.

Los campos Iddepartamento y Idpuesto indica el departamento y el puesto al que pertenece el empleado.

La tabla Medidapreventiva, tiene como objetivo almacenar la información de las acciones realizadas por la organización para disminuir el impacto del riesgo. Los campos que se contemplan son los siguientes:

- Idmedidapreventiva. Es este campo se almacena el identificador de la medida preventiva.
- Descripción. En este campo se almacena el nombre de la acción para prevenir el riesgo.
- Idriesgo. En este campo se registra el riesgo al que se esta atacando con la medida preventiva.
- Fechainicio. Se registra la fecha en la que inicia la medida preventiva.
- Fechafin. Se registra la fecha en que termina la aplicación de la medida preventiva.
- Costo. Se registra el costo de la medida preventiva.
- Entidadbeneficiada. En este campo se registra el número de entidades beneficiadas con la medida preventiva.
- Observación. En este campo se almacena información adicional.

La tabla Puesto, tiene como objetivo llevar el registro de los puestos que existen en cada departamento de cada UEN. Los campos definidos son:

- Idpuesto: Es un identificador único para cada puesto.
- Descripción: Este campo registra el nombre del puesto.
- Iddepartamento: Es el identificador del departamento al que pertenece el puesto.

La tabla Registroevento, es la tabla principal, su objetivo es almacenar la información de cada evento de riesgo que se presenta en la institución. Los campos considerados son:

- Fechainicio: Se registra la fecha en la que inicia el evento
- Fechadeteccion. Se registra la fecha en la que se detecta el evento.
- Fechafin. Se registra la fecha en la que el evento es controlado.
- Perdidadirecta. Es el impacto económico que causo directamente el evento.
- Perdidaindirecta. Se almacena la perdida económica causada de manera indirecta el evento.
- Idriesgo. Registra el identificador del evento.
- Idempleado. Registra el identificador del empleado responsable del evento, este identificador se obtiene de la tabla empleado.
- Idmedidapreventiva. En este campo se registra si al evento sucedido ya se había tomado medida preventiva.
- Observación. En este campo se redacta alguna observación o comentario referente al acontecimiento del evento.

La tabla Riesgo, es un catálogo que tiene una estructura tipo árbol, con el objetivo de clasificar el riesgo y sus subcategorías. Esta tabla se compone de los siguientes campos:

- Idriesgo, es lo que identificara de manera única al riesgo o la categoría.
- Descripción. Es el nombre que se le da al riesgo o subcategoría
- Idparent este campo indica la dependencia jerárquica de las categorías del riesgo.

Esta tabla tiene la particularidad que el proceso de captura de información inicia con el nodo raíz y posteriormente se agregan los hijos, nietos, etc.

La tabla UEN, tiene como objetivo almacenar información referente a las. Distintas unidades estratégicas de negocio de la institución, los campos son los siguientes:

- IdUEN. Es el identificador de la UEN.
- Descripción. En este campo se registra el nombre con la que se denomina cada UEN.

4.4.2 Interfase de usuario

La interfase al usuario es la parte del sistema por medio del cual el personal encargado cargará la información necesaria a la base de datos para posteriormente generar información que de valor a la toma de decisiones.

En este prototipo funcional se contempla que el sistema de información permita ingresar los datos a la base, genere reportes, estadísticas, mantener actualizada la base de datos, crear perfiles de usuario para que se den privilegios de acceso al sistema y genere un archivo de frecuencia y severidad de los riesgos presentados en el banco. Este mismo sistema, en etapas posteriores podrá usar la información histórica para el modelado estadístico. Más aun, poder integrarlo al sistema central del banco para poder monitorear y detectar transacciones con altas probabilidades de riesgo. Para llegar a implementar dicho sistema se requiere de un esfuerzo coordinado entre las líneas de negocio,

responsables de la administración del riesgo y un equipo de expertos dedicados durante meses o incluso años en el desarrollo de dicho sistema.

Para efectos de este estudio se presenta un prototipo de sistema de información con una funcionalidad básica que permite a la institución financiera ir registrando los eventos, frecuencia de ocurrencia, responsable y severidad. Por otro lado, permite registrar las acciones que se implementan para minimizar el riesgo y el costo que esto implica con el objetivo de comparar los beneficios de la administración del riesgo contra el costo de la administración.

La interfase al usuario se compone de altas, bajas y cambios a datos de:

- Empleado
- UEN
- Departamento
- Puesto
- Riesgo
- Evento
- Medida preventiva.

Por otro lado se encuentran los reportes, que son los datos de los eventos procesados y clasificados en una manera preestablecida.

Para ver mas detalle del prototipo del sistema de información ver el anexo 1.

4.5 Conclusiones.

En este capítulo se presenta la planeación estratégica como un eje de dirección, y prever barrearas para el logro de una visión y misión. No es posible abordar objetivos y tareas sin que los directamente involucrados tengan en mente qué es lo que se quiere alcanzar y de que se deben proteger que pueda impedir lo deseado.

La metodología AS/NZ 4360 2004 guía de manera sistemática y ordenada el proceso de identificación del riesgo. Esta fase concluye con la identificación de la estructura de riesgo para el área de TI.

La estructura de riesgo identificada con la metodología, es el insumo principal para el diseño del prototipo del sistema de información y en particular el diseño de la base de datos.
Por la forma en la que se va abordando el tema, tanto la estructura de la identificación del riesgo, como la propuesta del sistema de información se encuentran acordes con los objetivos, misión y visón del área de Tecnología de Información, lo cual hace de la información consistente y útil para la cualquier área de TI de una institución financiera.

El prototipo del sistema de información se puede tomar como base para el diseño, desarrollo de in sistema de información acorde a las necesidades particulares de una institución financiera.

5. Conclusiones generales

En el presente estudio se define la visión, misión y objetivos estratégicos con el fin de identificar la razón de ser del área de TI. Una vez definida esta razón de ser, el estudio se enfoca a identificar el riesgo operativo para el área de TI apoyados de la metodología AS/NZ 4360 2004, la que permite identificar el riesgo de manera sistemática y ordenada. Una vez que se tiene identificado el riesgo se cuenta con el insumo para la propuesta del prototipo funcional y de esto se concluye lo siguiente:

1. Definir la visión, la misión y objetivos estratégicos permite que las funciones de los departamentos y del personal converjan hacia un mismo fin: la razón de ser del área o empresa.

2. Una vez identificada la razón de ser de la entidad en estudio (TI), se identifica de manera consistente y asertiva el riesgo operativo apoyados en una metodología como la AS/NZ 4360 2004.

3. El prototipo funcional, presenta una estructura de diseño y arquitectura tecnológica viable para el desarrollo e implantación de un sistema de información en una institución en particular.

4. En este prototipo se presenta una estructura inicial importante para el desarrollo e implantación de un sistema de información desarrollado a la medida de las necesidades de la institución.

5. Este prototipo se diseña de acuerdo a las recomendaciones y definiciones del segundo acuerdo de Basilea, cada institución bancaria tiene la libertad de desarrollar su propia metodología siempre y cuando minimice el impacto del riesgo operativo.

6. La facilidad de almacenar y procesar datos del riesgo operativo para generar información de valor y mejorar la toma de decisiones respecto a su impacto y su prevención es el primer paso para cumplir con el requerimiento de capitales respecto al riesgo operativo.

7. Identificar el riesgo y contar con un sistema de información son las dos primeras etapas de una metodología para la medición del riesgo operativo dentro de una institución financiera. Las siguientes etapas son: 1) Registrar los eventos de riesgo operativos que se presenten en cada una de las unidades estratégicas de negocio y áreas de apoyo. 2) Mapear los procesos de cada unidad estratégica de negocio y asignar los riesgos operativos a los que se encuentra expuesto. 3) Con los datos almacenados en el sistema de información modelarlos para la toma decisiones. 4) Crear una relación de riesgo y medida preventiva con el objetivo de minimizar el riesgo operativo. 5) Hacer el cálculo del capital que se debe reservar para hacer frente al riesgo operativo. Cada uno de estos cinco puntos son líneas de investigación para posteriormente integrarlas en una metodología para el cálculo de la reserva de capital para el riesgo operativo

8. El objetivo del estudio se cumple, se presenta una estructura apegada a la estrategia del negocio, se identifica el riesgo operativo y se crea un prototipo que es consistente con la problemática y la razón de ser del negocio. De esta manera se confirma la hipótesis planteada.

Anexo 1. Plataforma tecnológica para el prototipo del sistema de información propuesto.

Aunque el prototipo del sistema de información esta diseñado en una tecnología abierta y escalable, en particular el prototipo se particulariza en una base de datos, servidor de aplicaciones y páginas web, interface de usuario y hardware:

Base de datos: Postgres versión 7.2. El diseño de la base de datos se muestra en la figura A1.

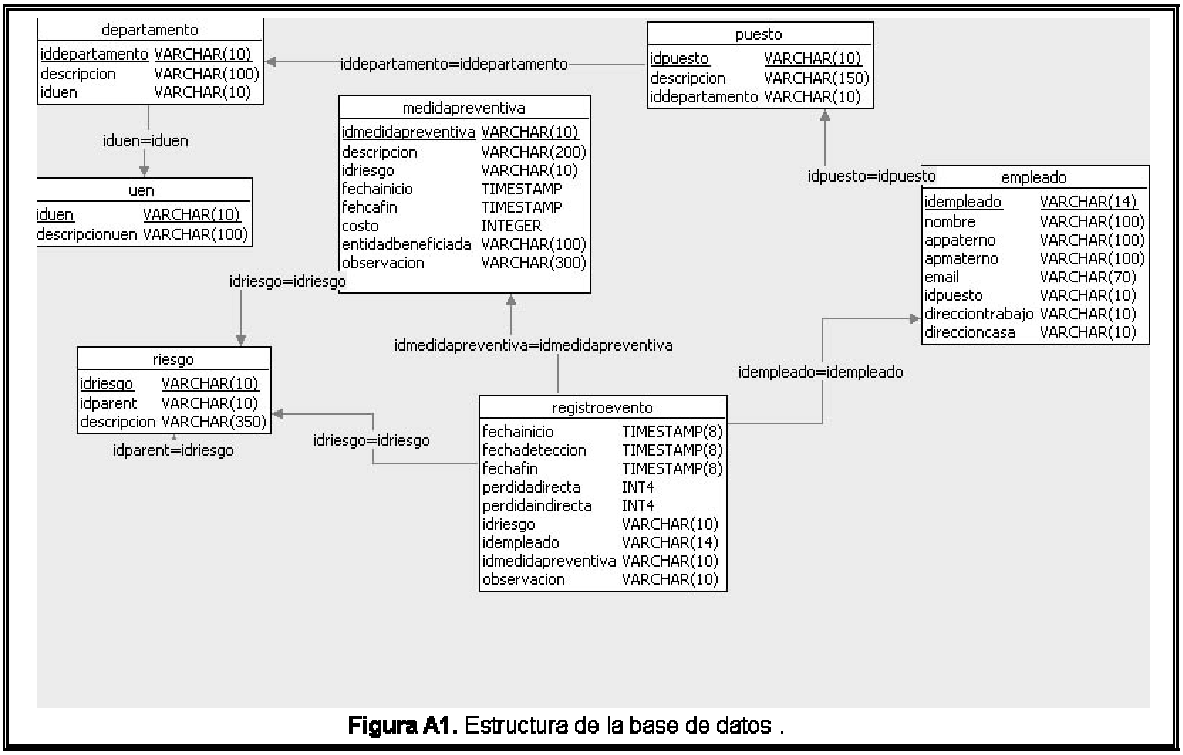


Figura A1. Estructura de la base de datos .

El escript para crear la base de datos con las características determinadas en el diseño es el siguiente:

```
CREATE TABLE DEFAULT_SCHEMA.uen (
       iduen VARCHAR(10) NOT NULL
     , descripcionuen VARCHAR(100) NOT NULL
     , PRIMARY KEY (iduen)
);

CREATE TABLE DEFAULT_SCHEMA.departamento (
       iddepartamento VARCHAR(10) NOT NULL
     , descripcion VARCHAR(100) NOT NULL
     , iduen VARCHAR(10) NOT NULL
     , PRIMARY KEY (iddepartamento)
     , CONSTRAINT fk_departamento_1 FOREIGN KEY (iduen)
```

```
                  REFERENCES DEFAULT_SCHEMA.uen (iduen) ON DELETE NO
ACTION ON UPDATE NO ACTION
);

CREATE TABLE DEFAULT_SCHEMA.puesto (
       idpuesto VARCHAR(10) NOT NULL
     , descripcion VARCHAR(150) NOT NULL
     , iddepartamento VARCHAR(10) NOT NULL
     , PRIMARY KEY (idpuesto)
     , CONSTRAINT fk_puesto_1 FOREIGN KEY (iddepartamento)
                  REFERENCES DEFAULT_SCHEMA.departamento (iddepartamento)
ON DELETE NO ACTION ON UPDATE NO ACTION
);

CREATE TABLE DEFAULT_SCHEMA.empleado (
       idempleado VARCHAR(14) NOT NULL
     , nombre VARCHAR(100) NOT NULL
     , appaterno VARCHAR(100) NOT NULL
     , apmaterno VARCHAR(100)
     , email VARCHAR(70) NOT NULL
     , idpuesto VARCHAR(10) NOT NULL
     , direcciontrabajo VARCHAR(10) NOT NULL
     , direccioncasa VARCHAR(10) NOT NULL
     , PRIMARY KEY (idempleado)
     , CONSTRAINT fk_empleado_1 FOREIGN KEY (idpuesto)
                  REFERENCES DEFAULT_SCHEMA.puesto (idpuesto) ON DELETE
NO ACTION ON UPDATE NO ACTION
);

CREATE TABLE DEFAULT_SCHEMA.riesgo (
       idriesgo VARCHAR(10) NOT NULL
     , idparent VARCHAR(10)
     , descripcion VARCHAR(350) NOT NULL
     , PRIMARY KEY (idriesgo)
     , CONSTRAINT fk_riesgo_1 FOREIGN KEY (idparent)
                  REFERENCES DEFAULT_SCHEMA.riesgo (idriesgo) ON DELETE
NO ACTION ON UPDATE NO ACTION
);

CREATE TABLE DEFAULT_SCHEMA.medidapreventiva (
       idmedidapreventiva VARCHAR(10) NOT NULL
     , descripcion VARCHAR(200) NOT NULL
     , idriesgo VARCHAR(10) NOT NULL
     , fechainicio TIMESTAMP NOT NULL
     , fehcafin TIMESTAMP NOT NULL
     , costo INTEGER NOT NULL
     , entidadbeneficiada VARCHAR(100)
     , observacion VARCHAR(300)
     , PRIMARY KEY (idmedidapreventiva)
     , CONSTRAINT fk_medidapreventiva_1 FOREIGN KEY (idriesgo)
                  REFERENCES DEFAULT_SCHEMA.riesgo (idriesgo) ON DELETE
NO ACTION ON UPDATE NO ACTION
);

CREATE TABLE DEFAULT_SCHEMA.registroevento (
       fechainicio TIMESTAMP(8) NOT NULL
     , fechadeteccion TIMESTAMP(8) NOT NULL
```

```
     , fechafin TIMESTAMP(8) NOT NULL
     , perdidadirecta INT4 NOT NULL
     , perdidaindirecta INT4 NOT NULL
     , idriesgo VARCHAR(10) NOT NULL
     , idempleado VARCHAR(14) NOT NULL
     , idmedidapreventiva VARCHAR(10)
     , observacion VARCHAR(10) NOT NULL
     , CONSTRAINT fk_acontecimientoriesgo_2 FOREIGN KEY (idempleado)
                  REFERENCES DEFAULT_SCHEMA.empleado (idempleado) ON
DELETE NO ACTION ON UPDATE NO ACTION
     , CONSTRAINT fk_acontecimientoriesgo_3 FOREIGN KEY
(idmedidapreventiva)
                  REFERENCES DEFAULT_SCHEMA.medidapreventiva
(idmedidapreventiva) ON DELETE NO ACTION ON UPDATE NO ACTION
     , CONSTRAINT fk_acontecimientoriesgo_1 FOREIGN KEY (idriesgo)
                  REFERENCES DEFAULT_SCHEMA.riesgo (idriesgo) ON DELETE
NO ACTION ON UPDATE NO ACTION
);
```

Servidor de aplicaciones y páginas web. El servidor de aplicaciones y páginas web es la aplicación que se encuentra entre la base de datos y la interfase del usuario. Para esto se usa el software Orión 7.0.5.

Interfase de usuario. Para el desarrollo de la interfase del usuario, esto es, para el desarrollo de páginas HTML y código para crear la conexión con la base de datos se usa Dream Weaver XX, JDK 1.5, JSP y servlets.

A continuación se muestran las pantallas del prototipo, para la carga de información a la base de datos y los reportes que se proponen.

El prototipo del sistema de información esta compuesto de tres partes importantes: Validación de usuario, mantenimiento a la base de datos y reportes.

Validación de usuario. En esta ventana se identifica el usuario para determinar el perfil con el que se accesa al sistema, solo se definen tres: Administrador, usuario para mantener el sistema y usuario para consulta del sistema. La ventana para la validación se muestra en la figura A2.

Mantenimiento a la base de datos. La interfase para dar mantenimiento a la base de datos se encuentra dividida en para realizar altas, bajas y cambios en lo que respecta a empleado, UEN, Departamento, Puesto, Riesgo, Evento y Medida preventiva.

En las figuras A3, A4 y A5 se muestran las pantallas para realizar el alta, baja y cambios a los datos del empleado:

Figura A3. Alta de datos de un empleado.

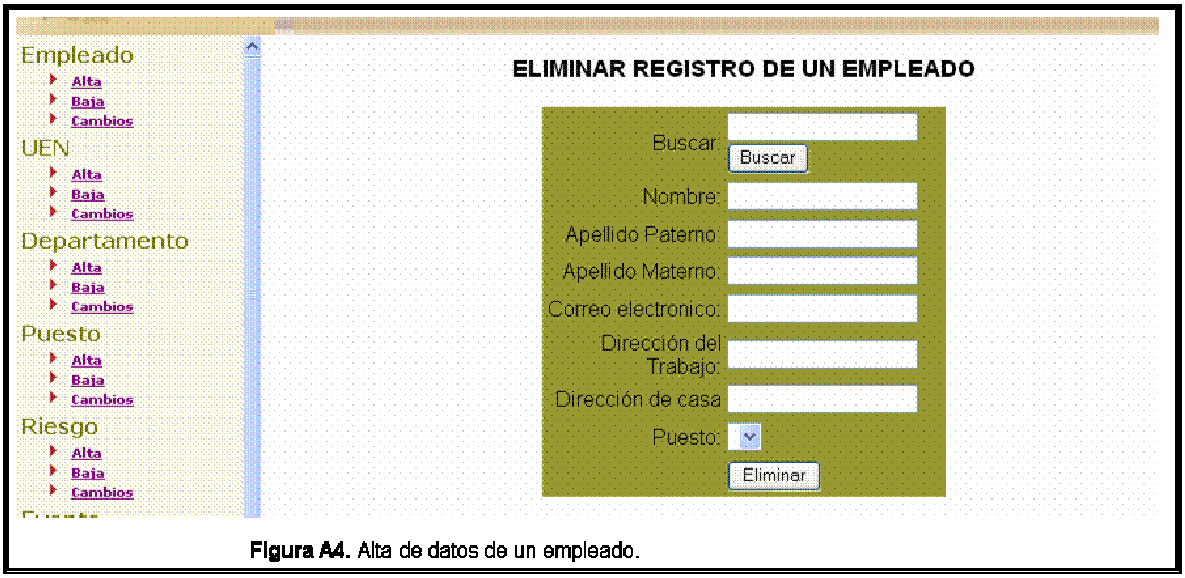


Figura A4. Alta de datos de un empleado.

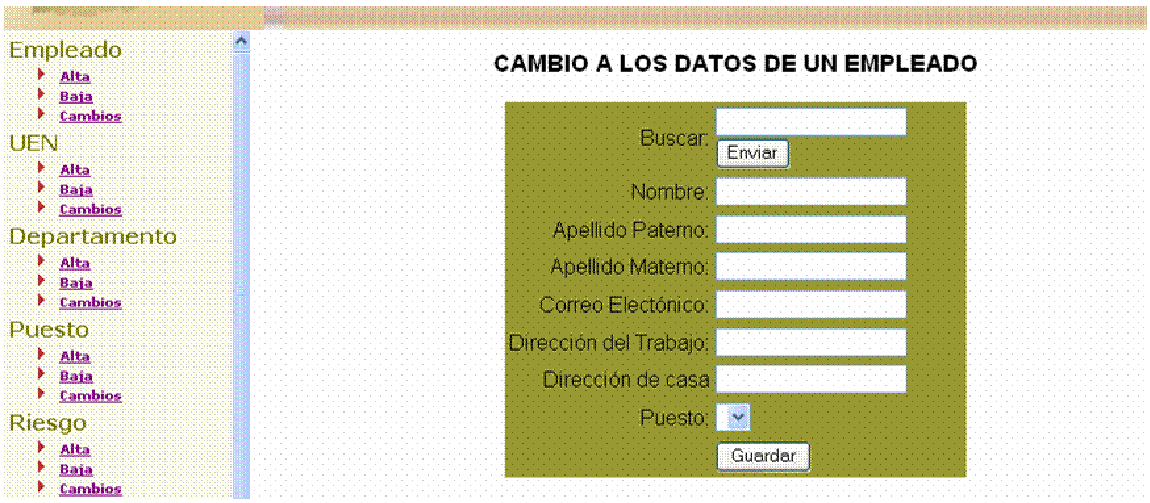


Figura A5. Cambios a los datos de un empleado.

En las figuras A6, A7 y A8, se muestran las pantallas para alta baja y cambios a una UEN.

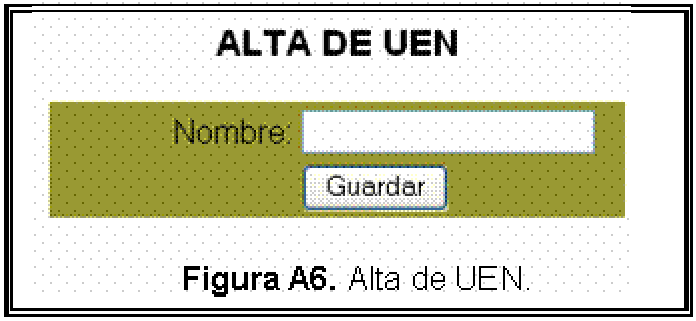


Figura A6. Alta de UEN.

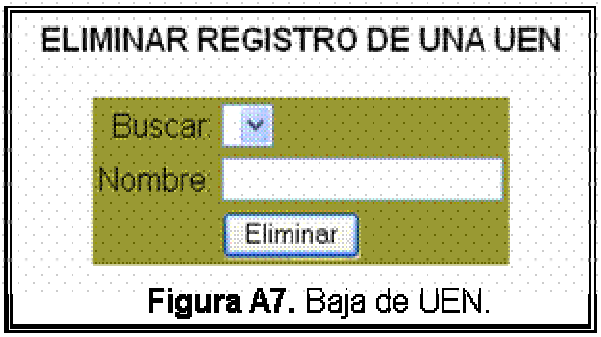


Figura A7. Baja de UEN.

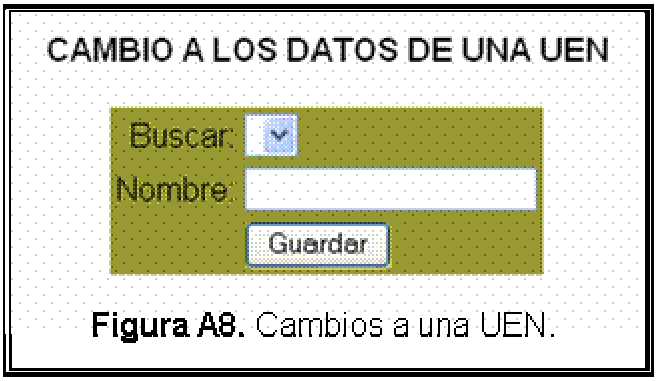


Figura A8. Cambios a una UEN.

En las figuras A9, A10 y A11 se muestran las pantallas para realizar las altas, bajas y cambio de un departamento.

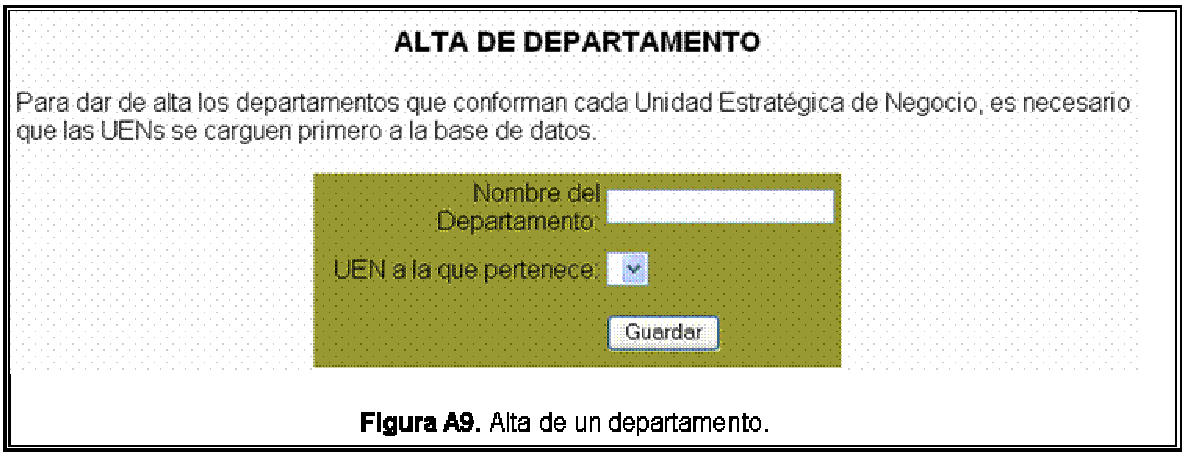


Figura A9. Alta de un departamento.

Figura A10. Baja de un departamento.

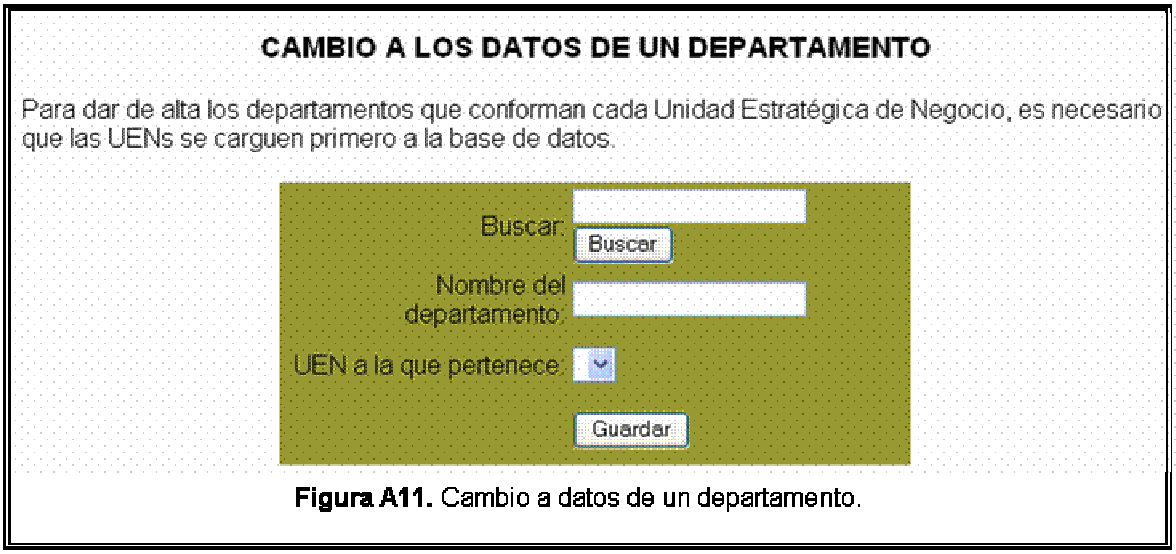


Figura A11. Cambio a datos de un departamento.

En las figuras A12, A13 y A14 se muestran las pantallas para altas, bajas y cambios de un puesto.

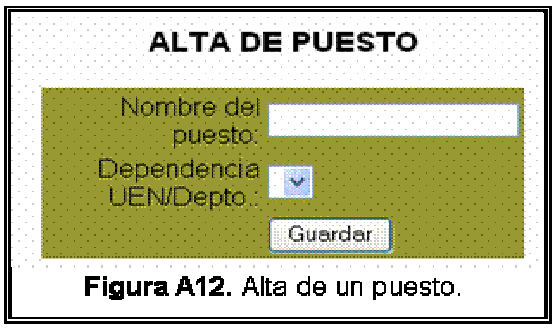


Figura A12. Alta de un puesto.

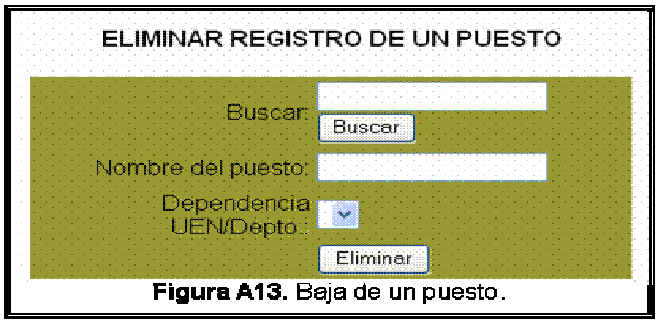


Figura A13. Baja de un puesto.

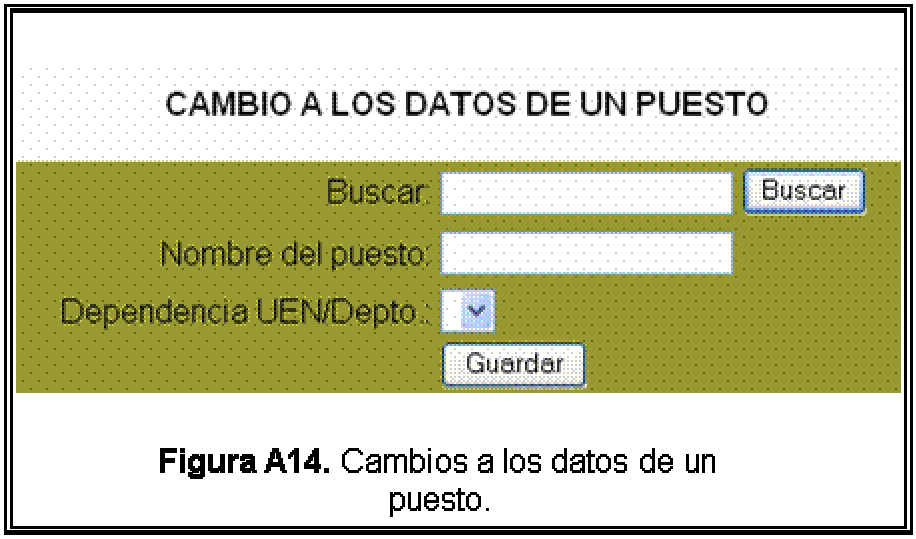


Figura A14. Cambios a los datos de un puesto.

En las figuras A15, A16 y A17 se muestran las pantallas para las altas, bajas y cambios a un riesgo.

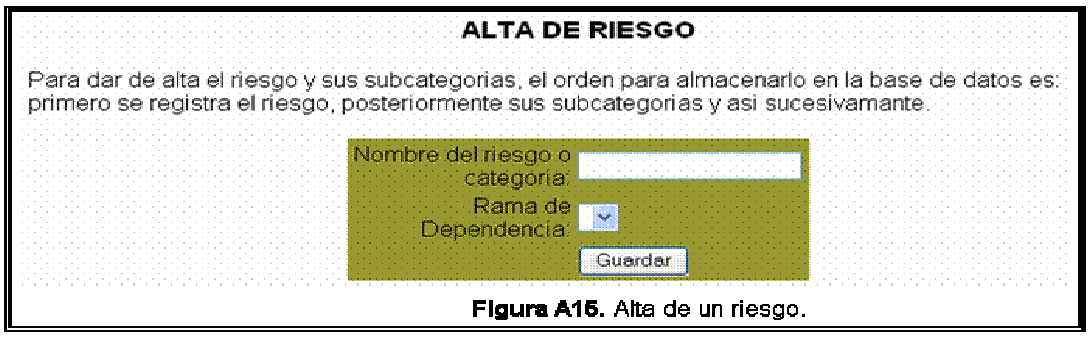


Figura A15. Alta de un riesgo.

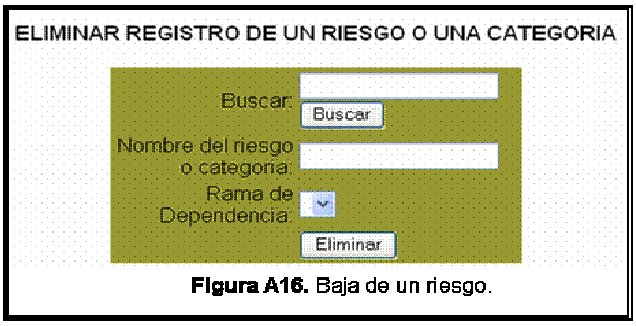


Figura A16. Baja de un riesgo.

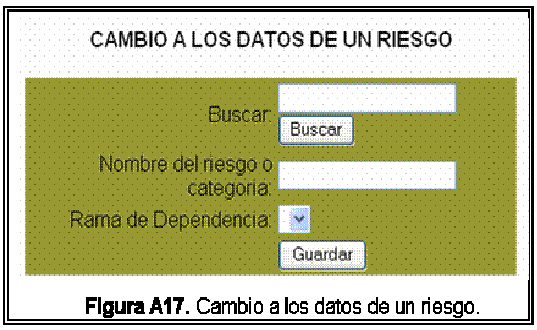


Figura A17. Cambio a los datos de un riesgo.

En las figuras A18, A19 y A20 se muestran las pantallas para las altas, bajas y cambio a los datos de un evento.

Figura A18. Alta de un evento.

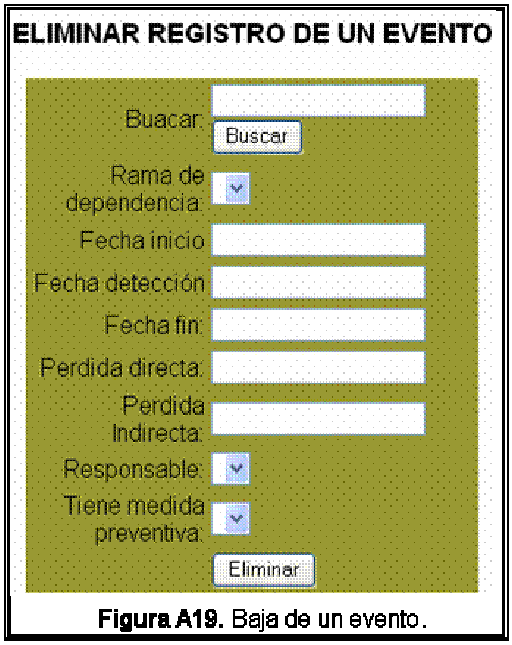


Figura A19. Baja de un evento.

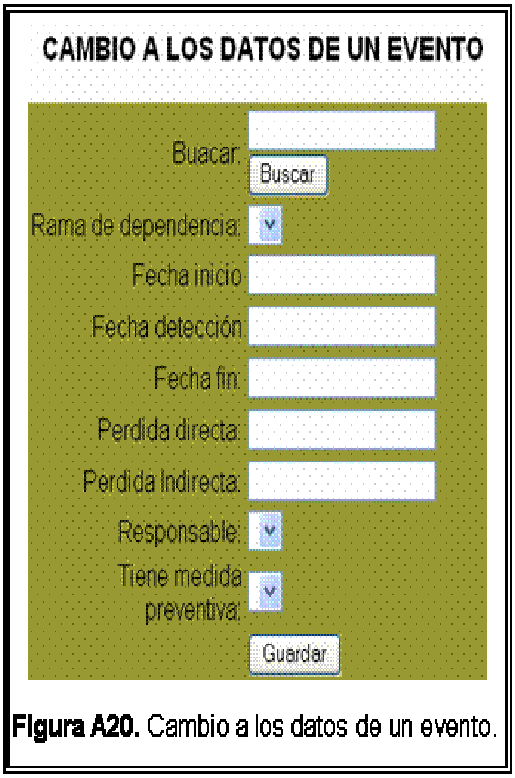


Figura A20. Cambio a los datos de un evento.

Figura A21. Alta de una medida preventiva.

En las figuras A21, A22 y A23 se muestran las pantallas para realizar las altas, bajas y cambios a los datos de una medida preventiva.

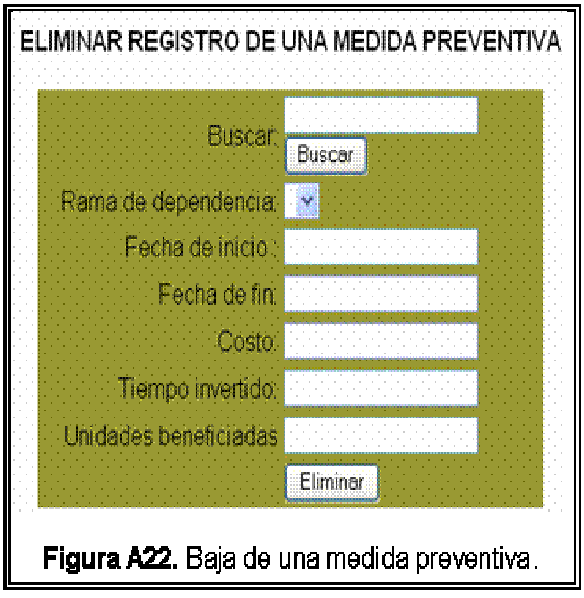


Figura A22. Baja de una medida preventiva.

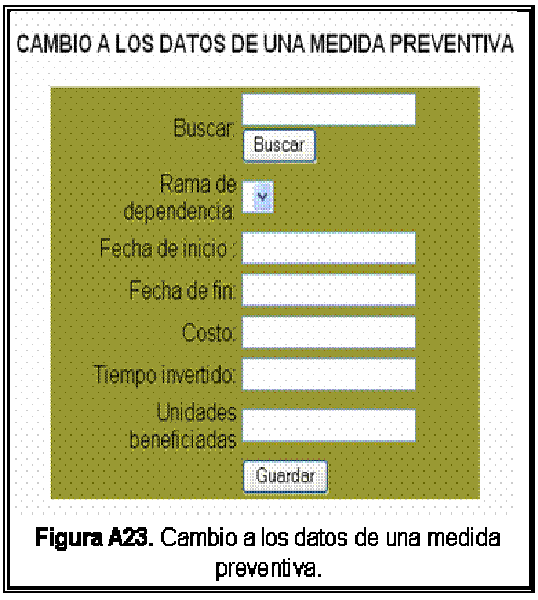


Figura A23. Cambio a los datos de una medida preventiva.

En las figuras A21, A22 y A23 se muestran las pantallas para realizar las altas, bajas y cambios a los datos de una medida preventiva.

Anexo 2. Planeación estratégica.

Todo emprendedor inicia con una idea en mente sobre el negocio que desea establecer, para esto se requiere identificar en primera instancia tres bloques: análisis de la organización, diseño estratégico y selección e implantación y control. Esto conduce a una desagregación jerárquica y ordenada, partiendo como punto cumbre la imagen objetivo, esto es la visión y misión.

El análisis de la organización contempla cuatro puntos trascendentales en la concepción de lo que se quiere hacer y a donde se desea llegar, en esta etapa se definen:

- Visión y misión,
- Análisis interno,
- Análisis externo,
- Objetivos a largo plazo u objetivos estratégicos.

El diseño estratégico y selección, es el siguiente nivel de desagregación, los puntos que se definen son:

- Diseño de estrategia maestra,
- Estrategias específicas,
- Programación y presupuestación.

Implantación y control, tercera y última etapa de desagregación se definen:

- Proyectos estratégicos de acción, y;
- Diseño de la implantación y control.

En la figura A2_1 se muestran las tres etapas de la planeación estratégica, como se puede ver, conforme se abordan etapas inferiores, se van desagregando de manera jerárquica y ordenada la visión, hasta concluir con acciones mas específicas.

El proceso para definir la visión y la misión se inicia con la situación en la que se encuentra la empresa, UEN o departamento, esto es, realizar un análisis externo e interno.

El análisis externo, inicia con ubicar la empresa en el pasado, presente y futuro, posteriormente se realiza un análisis de las fuerzas del mercado: competidores directos y potenciales, proveedores, productos sustitutos y compradores.

Para el análisis interno, se realiza una indagación sobre las fortalezas, debilidades, oportunidades y amenazas, poniendo especial atención en la cultura, los directamente involucrados o stakeholders, estructura organizacional, capacidades en términos de personas, sistemas y procesos.

Las fortalezas, como su misma definición lo indica, “es una virtud cardinal que confiere valor” y dentro de una empresa los puntos importantes que dan valor son: recursos humanos, procesos, productos y servicios y recursos financieros.

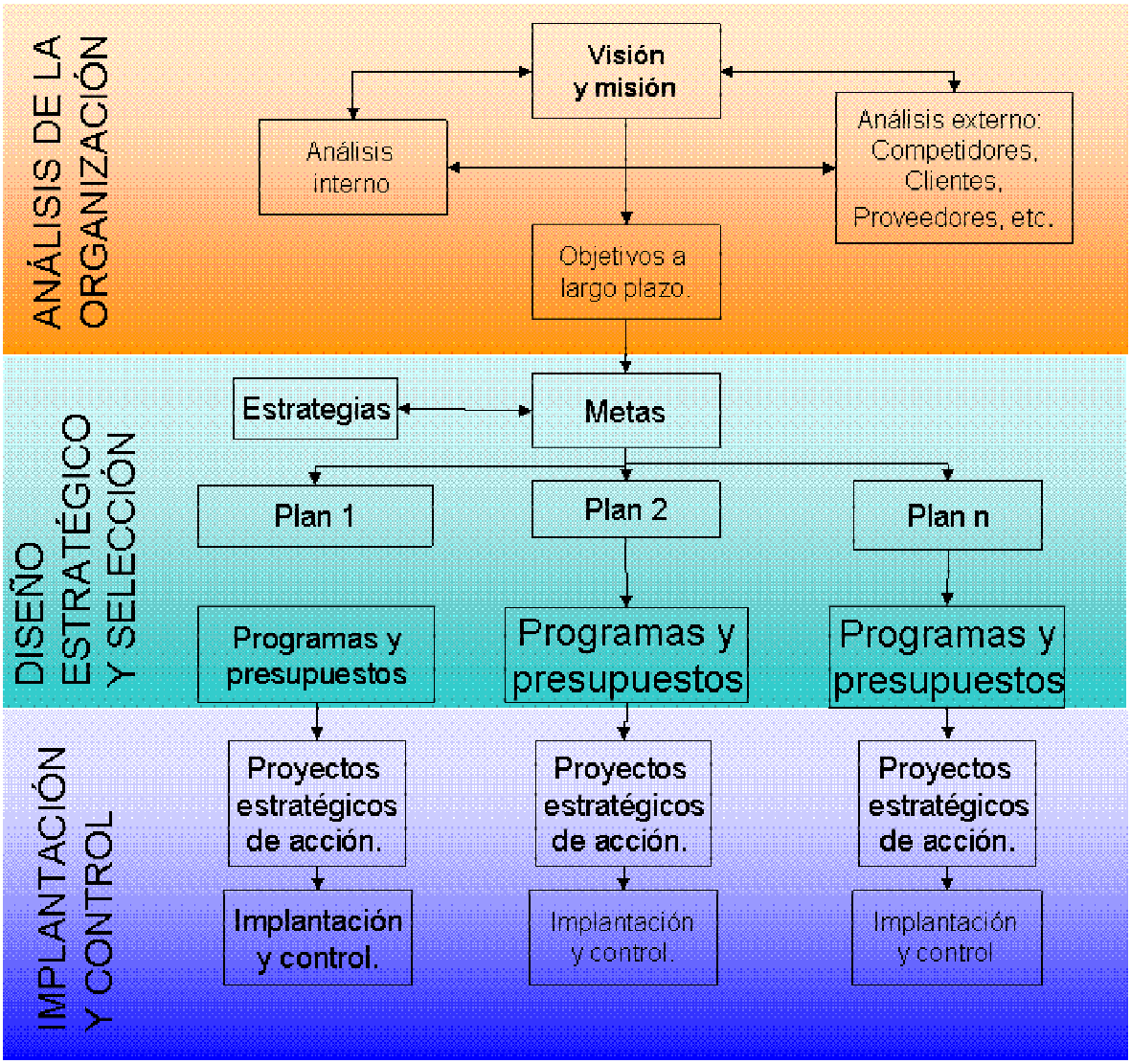


Figura A2 _1. Etapas de la planeación estratégica.

Las debilidades son las principales áreas de flaqueza o decaimiento que presenta la empresa en sus áreas clave de tal manera que se puedan tomar acciones para superarse.

Las oportunidades son eventos o circunstancias coyunturales que pueden presentarse en un futuro impactando de manera positiva en la organización. Estas oportunidades se pueden presentar en el mercado, clientes, industria, gobierno, competencia y tecnología.

Las amenazas, al contrario de las oportunidades, son eventos negativos que se presentan en el exterior de la organización y que impactan en los resultados esperados.

Una vez que se tienen los resultados del análisis interno y externo, se toman como insumo para la definición de la visión y misión. De esta manera, se obtiene la idea a futuro, las fortalezas que se tienen y el horizonte de tiempo en el que se desea alcanzar[1].

Así, la estructura de la visión queda de la siguiente manera:

"En **HORIZONTE DE TIEMPO**
ser **IDEA A FUTURO**
a través de **FORTALEZAS**."

La visión se debe caracterizar por ser fácil de entender, breve en su redacción, inspirar y tener retos, ser consistente con la misión, debe ser el punto al que se deben enfocar todos los esfuerzos en la empresa, y debe ser flexible para su ejecución.

Una vez definida la visión, esto es, la imagen objetivo, a lo que la empresa aspira, lo siguiente es definir la misión. Esta etapa consiste en traducir la imagen de la visión en objetivos y retos específicos en un plazo determinado. Para esto es importante hacer el análisis de los siguientes puntos:

1. Identificar las actividades necesarias para llegar a ser lo contemplado en la visión.
2. Identificar los productos o servicios a ofrecer,
3. Identificar qué necesidades se deben cubrir a los clientes.
4. Identificar a los agentes internos a la empresa.
5. Identificar la imagen al exterior: ventaja competitiva.
6. Identificar el alcance geográfico.

Con estos seis puntos se identifican las actividades, productos y servicios, los clientes, agentes internos, ventaja competitiva y el alcance geográfico. Con estos puntos definidos se escribe de manera clara, precisa y breve la misión de la empresa.

Objetivos a largo plazo. Según la definición del diccionario general de la lengua española, un objetivo es una meta o un fin que se desea alcanzar. En nuestro contexto, buscamos definir objetivos estratégicos, objetivos que se desprendan de la misión establecida por la empresa.

De esta manera un objetivo estratégico, lo definimos como una serie de acciones encaminadas hacia un fin, la misión, y sirve como marco de referencia para orientar las estrategias, metas, planes, programas y proyectos. Estos objetivos son cualitativos y su alcance es a largo plazo y se le da seguimiento por medio del logro de una sucesión de metas ordenadas y cuantificables. Los objetivos estratégicos los definen los miembros de la alta dirección y los gerentes de las áreas estratégicas. Para su definición se requiere de cuatro elementos importantes: 1) Imagen Objetivo, 2) Factores clave de éxito, 3) Prioridades, y 4) parámetros de evaluación.

La imagen objetivo, es una visualización clara a futuro de la situación de la organización en cuanto a los elementos de liderazgo, productividad, eficacia, calidad, rentabilidad, crecimiento, etcétera.

[1] Para la definición de la visión y la misión se recomienda aplicar técnicas participativas para la planeación como TKJ

Para detectar los factores clave de éxito, es necesario identificar las áreas estratégicas de la empresa, tales como: recursos humanos, tecnología, finanzas, productos y servicios, organización, etcétera. Dentro de cada una de estas áreas ver cuales son los factores clave de éxito y con esto definir los objetivos estratégicos.

Una vez que se cuenta con los objetivos a largo plazo que permitirán alcanzar la imagen objetivo, entonces es necesario asignarles prioridad para así determinar el orden de ejecución.

Una vez que se han definido los objetivos estratégicos, se está en capacidad de entrar a la fase de diseño estratégico y selección. En esta etapa se definen las metas, las estrategias, los planes, proyectos y presupuesto.

Las metas, se definen como los fines específicos al que se dirigen las acciones de alguien en puntos específicos de tiempo. Estas metas se desprenden directamente de los objetivos a largo plazo.
Las estrategias se entienden como la dirección general en la cual van a ser alcanzados los objetivos. Dichas estrategias se orientan para cumplir una o más metas y tratan de:

1. Consolidar las fortalezas,
2. Eliminar debilidades,
3. Aprovechar las oportunidades,
4. Minimizar el impacto de las amenazas, y;
5. Alcanzar los objetivos estratégicos.

Estas estrategias se dirigen al interior de la empresa hacia las áreas críticas: tecnología, recursos humanos, procesos, etcétera y se le denominan estrategias operativas. Por otro lado se encuentran las estrategias para tener una mejor posición competitiva de los productos y servicios en el mercado, estas son las estrategias de negocio.

Un plan, la real academia de la lengua española, lo define como un modelo sistemático de una actuación pública o privada, que se elabora anticipadamente para dirigirla y encausarla.

De esta manera, un plan de acción, lo definimos como un paquete de programas y proyectos integrados sistemáticamente y de manera anticipada, guiados por una o más estrategias, con el objetivo de alcanzar las metas.

Una vez definidos los planes, es necesario desagregar a mayor detalle los programas y proyectos. Estos programas y proyectos se definen como el conjunto de actividades que requieren de recursos (humanos, financieros, tecnológicos, etc.) por medio de las cuales se implantan las estrategias y las metas son alcanzadas.

En la figura A2_2 se muestra la relación que existe entre los elementos de decisión estratégica:

1. Las metas son pasos específicos para el logro de objetivos.
2. Las metas se establecen para mostrar los resultados de las estrategias.
3. Las metas se alcanzan a través de los planes.
4. Las estrategias se implantan por medio de los planes.

5. Los planes se alcanzan por medio de los programas y proyectos.

En la etapa de implantación y control se ejecutan las acciones correspondientes para terminar los proyectos, una vez implantados se requiere tener el control.

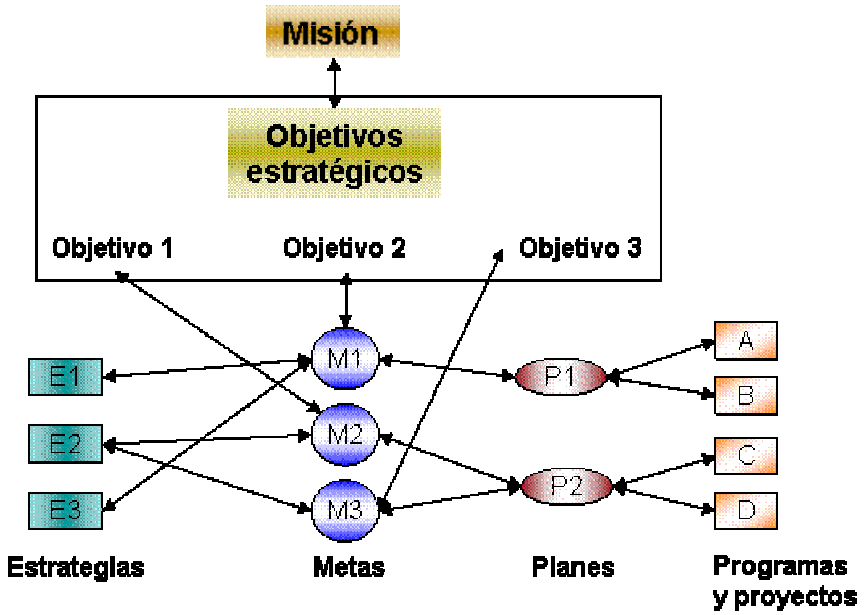


Figura A2 _2. Relación entre elementos estratégicos.

Bibliografía.

ACKOFF, Rusell L. Rediseñando el Futuro. México DF. Noriega Editores, 1991, 332 p.

CHORAFAS, Dimitris N, Operational Risk Control with Basel II, Oxford, Editorial Elsiever Butterworth Heineman, 2005, 357 p.

CORONA FUENTES, Rafael, Estratégia el cambio en la proyección del pensamiento empresarial, México DF. SICCO, 2001, 178 p.

CRUZ, Marcelo G. Modeling, measuring and hedging operational risk, England, John Wiley & Sons, 2003, 330 p.,

DA COSTA LEWIS, Nigel, Operational Risk with Excel and VBA, Hoboken New Jersey, John Wiley & Sons, 2004, 267 p.

DATE, C.J. Introducción a los sistemas de bases de datos, Vol I. (5ª edición)" Addison Wesley Iberoamericana, 1993, 860 p.

FRANKLIN, Enrique Benjamín, Auditoria administrativa. México, Editorial McGraw Hill, 2000

FROST, Crist, ALLEN, David, PORTER, James y BLOODWORD, Philip. Operational Risk and Resilience. Oxford, Butterworth Heinemann, 2001, 306 p.

HOFFMAN, Duglas G. Managing Operacional Risk, USA John Wiley & Sons. 2002, 534 p.
KAPLAN, Robert S y NORTON, David P., Cuadro de Mando Integral, Barcelona España, Gestión 2000, 2002. 321 p.

HUSSAIN, Amanat. Managin Operational Risk in Financial Markets. Oxfort, Butterworth Heinemann, 2000, 271 p.

MARTINEZ, Eduardo y ABORNOZ , Mario, Indicadores de ciencia y tecnología: estado del arte y perspectivas. Caracas Venezuela, Editorial Nueva sociedad UNESCO, 1998

PACHECO, Juan Carlos y CASTAÑEDA, WIDBERTO, Indicadores Integrales de gestión, Colombia, McGraw Hill, 2002. 184 p.

PORTER, Michael E. Estrategia competitiva. Técnicas para el análisis de los sectores industriales y de la competencia. CECSA, México DF, Vigésima tercera reimpresión 1997.

Risk Management, Standards Australia and Standard New Zealand, 2004, 29 p.

ROJAS ARCE, Jorge Luis, Pautas para formular la visión y misión de una organización, Tesis para obtener el grado de maestro (planeación), México DF, 2004.
SÁNCHEZ GUERRERO, Gabriel, Marco Teórico para la evaluación, México DF, 1995, 29 p.
ROB, Peter, Coronel, Carlos. Sistemas de bases de datos: diseño, implementación y administración. México DF 2004: International Thomson

BELLY, Pablo, http://www.gestiopolis.com/canales/gerencial/articulos/59/niveles.htm, revisado 7 de enero del 2005.

Price Water House Coopers, http://www.pwcglobal.com/es/esp/ins-sol/spec-int/gestionriesgo.pdf, fecha de consulta: 5 de febrero del 2005.

Comité de Supervisión Bancaria, Convergencia internacional de medidas y normas de capital, Basilea (Suiza), 2004, publications@bis.org, http://www.bis.org/publ/bcbs107esp.pdf, fecha de consulta: 3 de marzo del 2005.

http://www.ceu.es/clubriesgos/2%20Riesgo%20Operacional%20A.%20Morillas.ppt , fecha de consulta: enero del 2005.

http://www.cisco.com/ar/NetworkSecurity.swf, fecha de consulta: febrero del 2005.

http://www.audit.ucsb.edu/icguideline.html, fecha de consulta: febrero del 2005.

http://www.webopedia.com/TERM/I/IPsec.html, fecha de consulta: abril del 2005.