UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

METODOLOGÍA DE ANALISIS DE RIESGOS EN LOS SISTEMAS DE INFORMACION DE UNA EMPRESA BANCARIA

T E S I S

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

Antonio Alejandro Cordero Rosado

LIMA - PERU
1999

A mis padres, Lady y Antonio,
por su constante apoyo y estímulo,
por sus enseñanzas y su ejemplo,
siempre serán mis mejores maestros.

A mi hermano Francisco,
por su apoyo y su ejemplo.

Y a todos mis amigos y profesores
de la Universidad,
por las enseñanzas y experiencias
compartidas que, sin duda,
forman parte indesligable
de mi formación profesional.

Agradecimientos

El autor desea expresar su profundo agradecimiento a todas aquellas personas que lo apoyaron de diferentes maneras durante el desarrollo del presente trabajo de investigación: al personal de la Superintendencia de Banca y Seguros, por las facilidades brindadas y el apoyo del equipo de trabajo de la Unidad de Riesgos en Tecnología de Información, del cual me enorgullezco en formar parte; a mis asesores, por sus valiosas sugerencias; y a los profesores y compañeros de la Facultad de Ingeniería Industrial y de Sistemas de la UNI, por sus palabras de apoyo y aliento, que me comprometieron aún más a culminar el presente trabajo de manera satisfactoria. Una mención especial a mis padres Lady y Antonio, y a mi hermano Francisco, por su constante apoyo y comprensión. Sin ello, este trabajo no hubiera podido ser culminado.

Lima, 7 de diciembre de 1999

Antonio Alejandro Cordero Rosado

INDICE

DESCRIPTORES TEMATICOS:

Riesgos, Banca, Metodología, Auditoría de sistemas, Seguridad informática, Plan de contingencia, COBIT, Banca por Internet, Año 2000

RESUMEN EJECUTIVO

Las empresas se encuentran expuestas a diversos riesgos, entiéndose *riesgo* como la ocurrencia de eventos que generan consecuencias adversas en el logro de los objetivos de la empresa. En particular, las empresas bancarias se encuentran expuestas a un conjunto específico de riesgos, propios de la naturaleza de sus operaciones. Los riesgos asociados al uso de la tecnología de información constituye uno de estos riesgos.

Las empresas bancarias son cada vez más dependientes del uso de la tecnología de información para la continuidad de sus operaciones diarias. Sin embargo, conforme crece esta dependencia, se encuentran cada vez más expuestas a los riesgos asociados al uso intensivo de esta tecnología. Frente a ello, surge la necesidad de contar con una metodología sistemática que permita analizar dichos riesgos y evaluar las actividades de control implementadas para administrar estos riesgos.

El estudio realizado permitió identificar diez áreas de riesgo en los sistemas de información a los que se encuentran expuestas las empresas bancarias. Estas áreas de riesgo fueron agrupadas en cuatro dominios: Planeamiento y Organización, Adquisición, Desarrollo e Implementación, Operaciones, y Monitoreo y Control.

La Metodología desarrollada como resultado del estudio, considera seis fases de ejecución: Inicio, Identificación de riesgos, Evaluación de actividades de control, Medidas correctivas, Calificación y Reporte Final. En el desarrollo de la fase 3, se elaboraron Guías de Evaluación para cada una de las diez áreas de riesgo identificadas inicialmente.

El desarrollo de la metodología tomó como referencia el modelo COBIT de la Asociación ISACA, el Modelo de Análisis de Riesgos de la Reserva Federal de Estados Unidos, y la metodología MAGERIT del Consejo Superior de Informática de España, entre otras fuentes metodológicas de referencia.

INTRODUCCION

El informe que se presenta a continuación representa la culminación de un trabajo de investigación iniciado en junio de 1998, y convertido en tema de tesis profesional en enero de 1999. El tema central del estudio es el diseño de una metodología de análisis de riesgos en los sistemas de información en las empresas bancarias. Durante el tiempo en que se desarrolló este trabajo, se revisó bibliografía especializada relacionada al tema, y se hizo uso intensivo de la nueva herramienta que tienen a disposición los investigadores actuales: la red Internet. Por medio de Internet, se obtuvieron artículos publicados por especialistas en el tema, así como por organismos internacionales. Asimismo se sostuvieron entrevistas con consultores y especialistas en Sistemas de Información, cuyos valiosos aportes enriquecieron enormemente el estudio desarrollado. A continuación se presenta una breve descripción del problema analizado y se señala el contenido del presente informe.

Descripción del problema

El uso adecuado de la tecnología de información como soporte para el logro de los objetivos y metas de una organización, se ha convertido en un factor crítico de éxito para cualquier empresa que desee ser competitiva en el escenario actual de los negocios, caracterizado por la globalización de los mercados, la necesidad de satisfacer a clientes cada vez más exigentes y la búsqueda de mayor eficiencia en el uso de los recursos.

La afirmación anterior resulta especialmente válida para las empresas del sector bancario. El uso de la tecnología de información se ha expandido hacia todos los

niveles de la organización de las empresas bancarias, no solamente en el procesamiento de las transacciones financieras diarias, sino también como soporte en algunos procesos de toma de decisiones, como la calificación de créditos, y la compra y venta de títulos-valores. Asimismo, el desarrollo de nuevos productos financieros, cuya valorización se realiza a través de sofisticados modelos matemáticos, ha sido posible gracias al uso de la tecnología de información. Además, el desarrollo de Internet y de las redes de comunicaciones, no sólo ha permitido minimizar las restricciones geográficas para el crecimiento y desarrollo de las empresas del sector, sino que ha permitido abrir nuevos canales de distribución de los servicios bancarios al público en general.

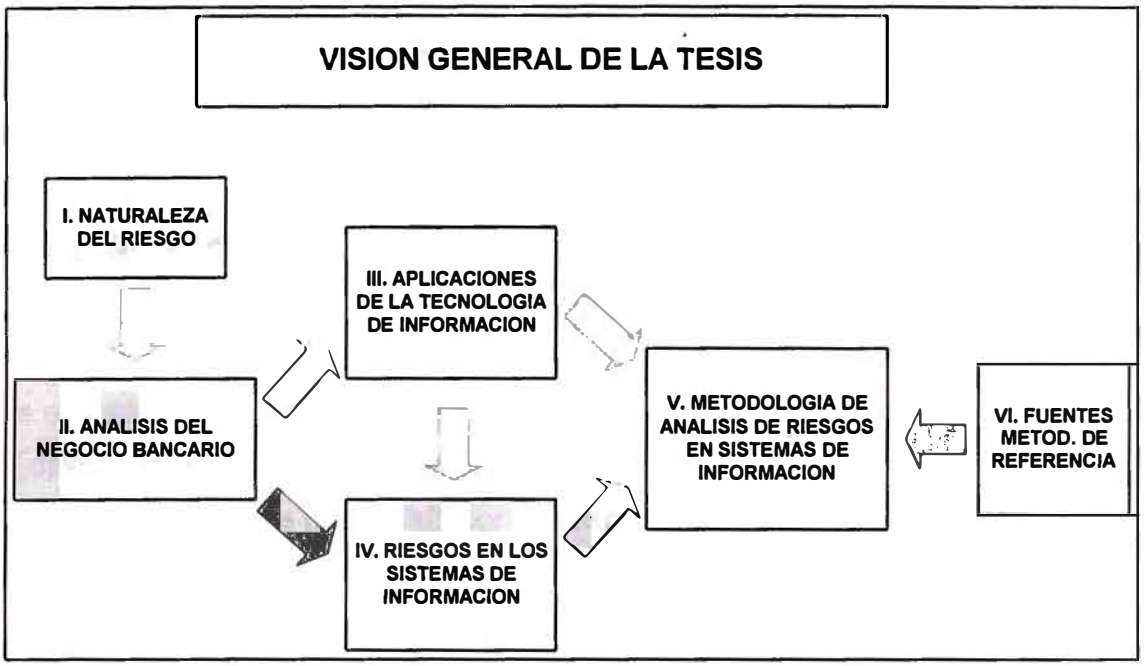
Sin embargo, conforme las empresas bancarias hacen un uso más intensivo de la tecnología de información para sus operaciones diarias, se encuentran expuestas en mayor grado a los riesgos asociados al uso de esta tecnología. Estos riesgos están relacionados con posibles pérdidas en el patrimonio de la empresa bancaria, debido a fallas en sus sistemas de información, accesos no autorizados a dichos sistemas, fraudes electrónicos, inadecuados procesos de adquisición de hardware o software de aplicación, errores en los proyectos de desarrollo de sistemas de información, entre otros aspectos.

Frente a esta situación, *resulta necesario* contar con una metodología estructurada que permita analizar de una manera sistemática los riesgos a los que está expuesta una empresa bancaria debido al uso intensivo de la tecnología de información. Este marco metodológico debe permitir la identificación de aquellas áreas en las cuales la empresa tenga un mayor grado de exposición a estos riesgos, y la definición de las acciones a tomar a fin de mitigar sus efectos.

El presente estudio se orienta precisamente a satisfacer esta necesidad, mediante el diseño de una metodología para el análisis de riesgos en los sistemas de información de una empresa bancaria. Esta metodología puede ser aplicada tanto por la empresa bancaria como por los supervisores bancarios.

Contenido del informe

El informe se divide en seis capítulos a lo largo de los cuales se describen los principales aspectos de la metodología diseñada, de acuerdo al siguiente esquema:



En el Capítulo I se describe brevemente la naturaleza del riesgo desde una perspectiva sistémica, y se mencionan algunos casos que ilustran la necesidad de contar con una metodología estructurada para el análisis de los riesgos en los sistemas de información.

En el Capítulo II se señalan las principales características y riesgos existentes en el negocio bancario, así como las principales operaciones y procesos de este negocio. Se incluye además una breve descripción del sistema bancario peruano, señalando los elementos de este sistema, los organismos de regulación y supervisión, así como un análisis de la coyuntura actual del sistema.

En el Capítulo III se describen las principales aplicaciones de la tecnología de información en las empresas bancarias, los cuales configuran la arquitectura de sistemas de información en estas empresas. Esto incluye los sistemas transaccionales que permiten automatizar las operaciones bancarias, los sistemas de soporte a la toma de decisiones, el manejo de transacciones a través de la banca electrónica, el uso de Internet y el comercio electrónico.

En el Capítulo IV se señalan los riesgos a los que se encuentra expuesta la empresa debido al uso de sus sistemas de información. Se describe un modelo de análisis que identifica cuatro dominios y diez áreas de riesgo, las cuales son descritas en detalle.

En el Capítulo V se describen los principales aspectos de la metodología propuesta para el análisis de riesgos en los sistemas de información de una empresa bancaria. Se describen las áreas de riesgo identificadas, así como los procedimientos generales y específicos de análisis por cada área.

En el Capítulo VI se señalan las principales fuentes metodológicas tomadas como referencia para el diseño de la metodología propuesta en el capítulo anterior. Se mencionan el estándar COBIT de la Asociación ISACA, la metodología utilizada por la Reserva Federal de Estados Unidos, así como la metodología MAGERIT del Consejo Superior de Infrormática de España, entre otras fuentes.

CAPITULO I

LA NATURALEZA DEL RIESGO

1.1. Introducción

En el presente capítulo se describe brevemente la naturaleza del riesgo en el entorno empresarial, desde una perspectiva sistémica. Se menciona asimismo la necesidad de una adecuada administración de riesgos, y se finaliza el capítulo con una descripción de casos ilustrativos en sistemas de información.

1.2. Naturaleza sistémica del riesgo

El riesgo en un concepto utilizado para expresar nuestra preocupación acerca de la ocurrencia de posibles eventos en un ambiente de incertidumbre. Dado que el futuro no puede ser predecido con total certidumbre, es necesario considerar la ocurrencia de un conjunto de eventos posibles. Cada uno de estos eventos puede tener un efecto material (es decir, una consecuencia significativa) en la empresa y en el logro de sus objetivos. Los eventos que generan efectos negativos en el logro de los objetivos de la empresa son denominados 'riesgos', y aquellos eventos con efectos positivos son denominados 'oportunidades'.

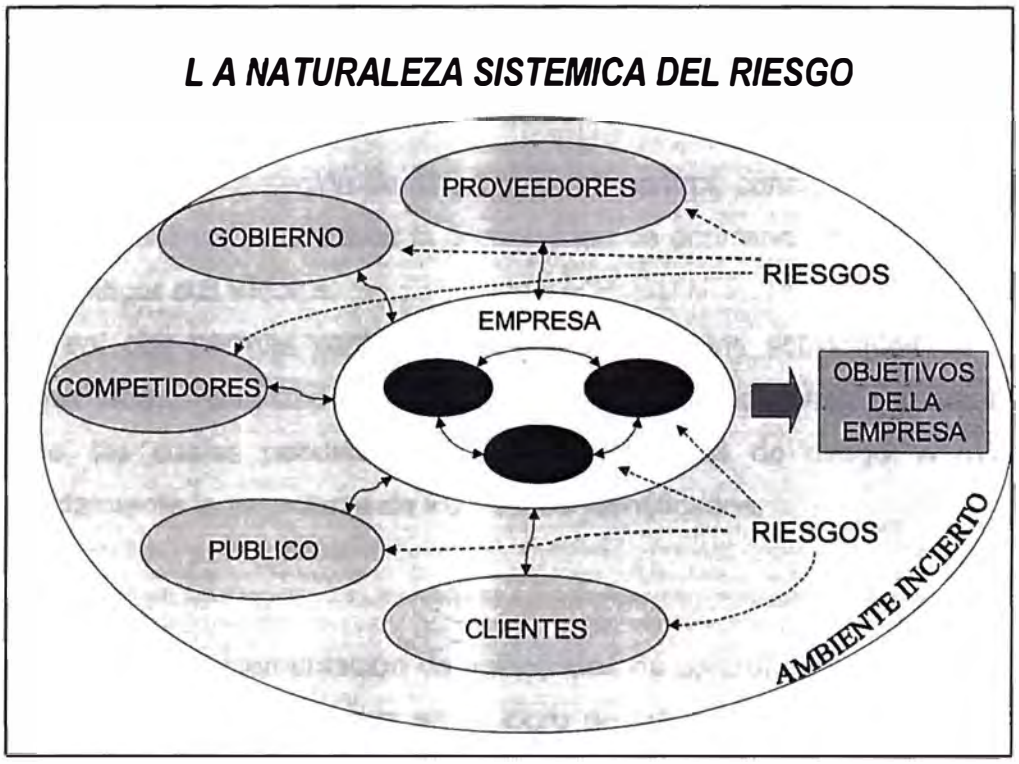
Desde una perspectiva sistémica, debe señalarse que los riesgos pueden estar asociados a cada uno de los elementos del entorno interno o externo de la empresa:

a. *Los elementos del entorno interno* incluyen a los procesos de negocio de la empresa, el personal, los sistemas de información, la estructura organizativa de la empresa, etc. Así por ejemplo, algunos de los riesgos asociados a estos

elementos incluyen: robo de información confidencial o sabotajes causados por personal descontento o con actitudes anti-éticas, falla en los sistemas de información que soportan los procesos críticos de la empresa, etc.

b. *Los elementos del entorno externo* incluyen a los proveedores, los clientes, la competencia, el gobierno, el público en general, entre otros. Algunos de los riesgos asociados a estos elementos incluyen: fallas en proveedores de servicios críticos, restricciones establecidas por dispositivos legales, cambios en las preferencias de los clientes, etc.

En el esquema siguiente se grafica lo expresado anteriormente:



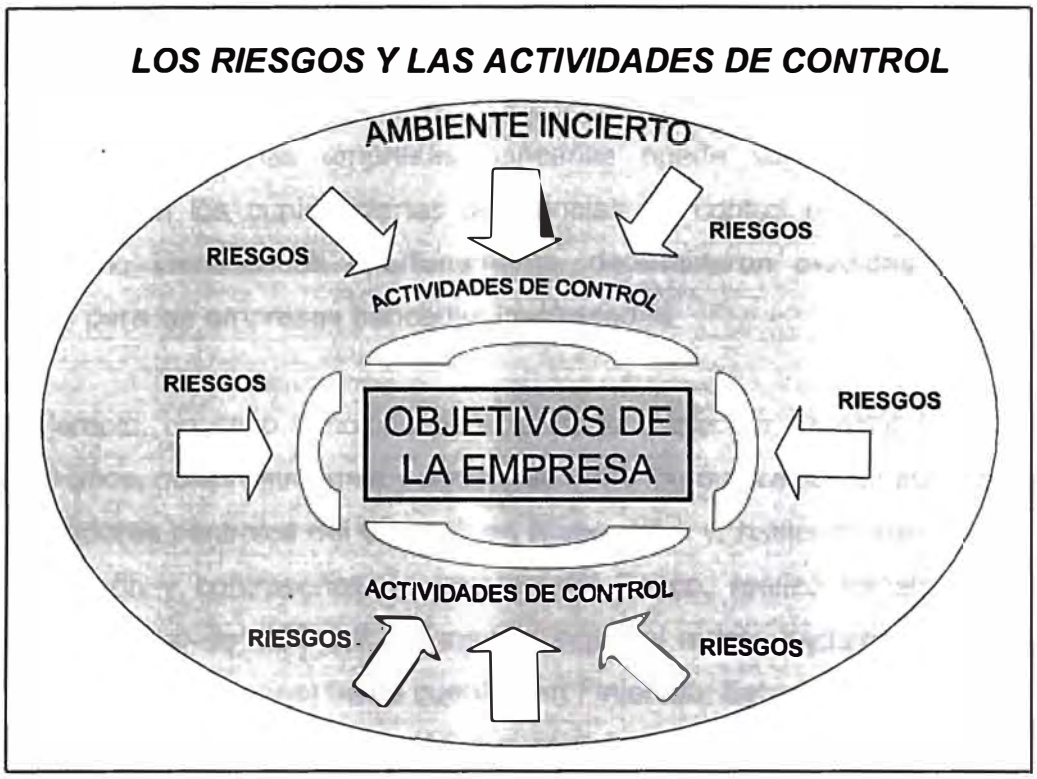
La existencia de ambientes inciertos es una característica normal en el mundo empresarial. La toma de decisiones en los negocios de hoy en día se realiza sobre ambientes de incertidumbre, tomando en consideración los riesgos y oportunidades existentes en el entorno de la empresa, así como los objetivos de la organización.

1.3. Administración de riesgos

Los riesgos no pueden ser eliminados completamente, sin embargo pueden ser adecuadamente administrados. Un adecuado sistema de administración de riesgos, debe incluir los siguientes aspectos:

a. *Identificación de riesgos*, que incluye el análisis y evaluación de todas las fuentes de riesgo existentes en el entorno interno y externo de la empresa. Esta tarea puede realizarse utilizando diversas técnicas que incluyen el uso de cuestionarios, encuestas, discusiones en grupo, métodos heurísticos, análisis de escenarios, árboles de decisión, etc.
b. *Evaluación de riesgos*, que incluye un análisis de la probabilidad de ocurrencia y el impacto que tienen los riesgos identificados en el logro de los objetivos de la empresa.
c. *Definición e implementación de actividades de control*, consistentes en medidas y acciones destinadas a reducir la probabilidad de ocurrencia de los riesgos, así como a mitigar sus efectos.
d. *Monitoreo*, que permite controlar la efectividad de las actividades de control implementadas. Asimismo deben monitorearse las condiciones cambiantes del entorno, las cuales pueden originar nuevas fuentes de riesgo, o modificar sustancialmente la naturaleza de los riesgos identificados.

De esta manera, la implementación de actividades de control permite a la empresa tener un mayor nivel de confianza en el logro de sus objetivos, considerando los riesgos a los que se encuentra expuesta. El esquema siguiente describe la relación entre riesgos y actividades de control para el logro de los objetivos de la empresa.



La administración de riesgos es de especial importancia para las empresas bancarias y financieras. Estas empresas se encuentran expuestas a un conjunto de riesgos, propios de la naturaleza de las operaciones que realizan, frente a los cuales deben utilizar adecuados sistemas de administración de riesgos, que les permita identificar y evaluar los riesgos a los que se encuentran expuestas, así como definir e implementar las actividades de control que sean necesarias. En particular, los riesgos asociados al uso intensivo de los sistemas de información constituyen sólo un tipo especial de riesgo a los que se encuentran expuestas estas empresas, cuya ocurrencia puede originar importantes pérdidas financieras a las empresas bancarias.

1.4. Casos ilustrativos de riesgos en sistemas de información

La importancia de contar con una metodología que permita analizar de manera estructurada y sistemática los riesgos en los sistemas de información a los que se encuentran expuestas las empresas bancarias puede ser ilustrada mediante algunos casos en los cuales ciertas deficiencias de control en los sistemas de información no identificadas oportunamente, determinaron pérdidas financieras importantes para las empresas bancarias involucradas.

Así por ejemplo, un caso conocido es el protagonizado por Vladimir Levin, joven ruso de 30 años, quien entre junio y agosto de 1994 logró acceder sin autorización a los computadores centrales del Citibank en Nueva York y, haciendo uso de códigos de identificación y contraseñas de clientes del Banco, realizó transferencias de fondos por un total de US$ 3,7 millones (aunque el monto inicialmente estimado ascendía a US$ 10 millones) hacia cuentas en Finlandia, Estados Unidos, Holanda, Alemania e Israel, controladas por él y sus cómplices, ocasionando una importante pérdida financiera y de reputación a uno de los bancos más grandes de Estados Unidos. Levin fue arrestado en 1995 en el aeropuerto de Londres, extraditado y sentenciado posteriormente por un tribunal norteamericano a 36 meses de prisión[1].

Otro de los casos comunes relacionados con la seguridad de la información, consiste en el robo de información confidencial relacionada con las tarjetas de crédito. El más reciente de los casos descubiertos fue realizado en Perú. En agosto de 1999, la División de Investigación de Estafas de la Policía Nacional del Perú descubrió una estafa por cerca de medio millón de dólares realizada por una organización delictiva que operaba en Lima, Costa Rica, Estados Unidos y Japón. Esta organización, en complicidad con dos empleados de una empresa bancaria peruana, había logrado vulnerar las cuentas bancarias secretas de por lo menos 362 clientes que poseían tarjetas Visa-Oro. Luego de obtener los números de las tarjetas de crédito, estos números eran utilizados para realizar compras a través de Internet de pasajes aéreos nacionales e internacionales, los cuales eran

posteriormente revendidos a precios de ocasión a través de una empresa que tenía oficinas en Lima, San José de Costa Rica, Miami, Nueva York y Tokio. Una vez descubiertos, los estafadores fueron detenidos y puestos a disposición del Ministerio Público por delito contra el patrimonio y contra la fé pública[2].

Los ataques de virus informáticos también representan una amenaza importante para el funcionamiento de los sistemas de información de una empresa, particularmente para los usuarios de computadores personales. El 26 de abril de 1999 -conmemorando el 13° aniversario del desastre nuclear de Chernobyl- el virus del mismo nombre atacó a cientos de miles de computadores personales en Turquía y Corea del Sur, eliminando toda la información de sus respectivos discos duros. En Estados Unidos se reportaron cerca de 2200 computadores afectados, mientras que en la India fueron cerca de 10 000, incluyendo negocios pequeños y bancos medianos, los cuales perdieron información valiosa de sus sistemas de cómputo[3].

Los tres casos mencionados en los párrafos anteriores representan sólo una pequeña parte de la gran cantidad de amenazas existentes en los sistemas de información, en especial en aquellos pertenecientes a las empresas bancarias. La diversidad de estas amenazas hace necesario su análisis mediante una metodología estructurada y sistemática. La elaboración de tal metodología fue el objetivo de la presente investigación, y será descrita en los siguientes capítulos.

Notas

1. Publicado en Internet por CNN en febrero de 1998, bajo el título "Internet robber sentenced. Levin may not face additional jail time for first known 'Net bank robbery'". (http://cnnfin.com/digitaljam/9802/24/robber/)
2. Publicado en el diario 'El Comercio' de Lima, el sábado 14 de agosto de 1999.
3. Publicado en Internet por el Detroit Free Press el 28 de abril de 1999, bajo el título ***"Chernobyl virus strikes hard at Asia, Middle East and U.S. home users"***, escrito por Chris Allbritton. (http://vh1380.infi.net/tech/qvirus28.htm)

CAPITULO II

EL NEGOCIO BANCARIO

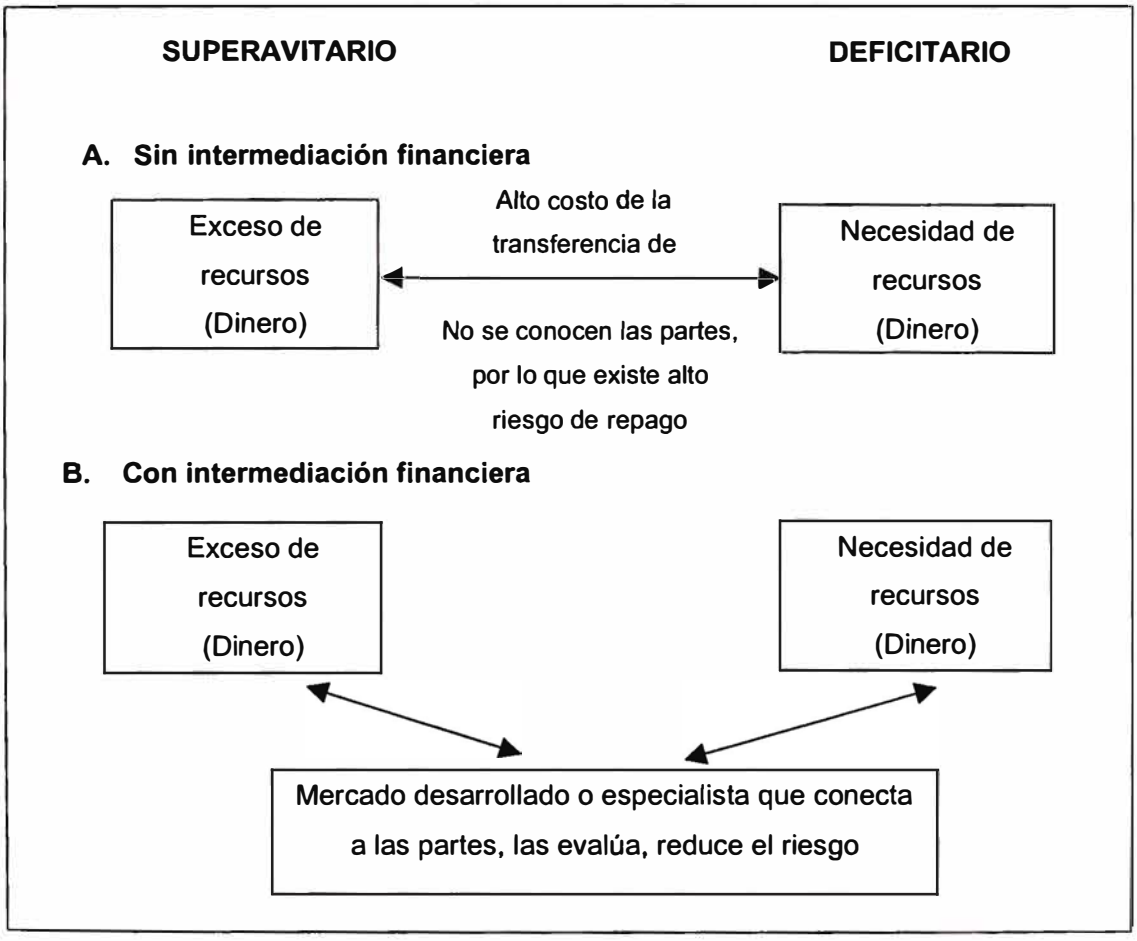
2.1. Introducción

En el presente capítulo se describen las principales características del negocio bancario, incluyendo los riesgos a los que se encuentra expuesto. Las empresas bancarias cumplen un rol importante en la economía del país, dado que permiten financiar al sector real de la economía nacional (encargado de la producción de bienes y servicios), a través de la captación de recursos financieros de agentes superavitarios de estos recursos (inversionistas y depositantes). Asimismo, la inestabilidad del sistema bancario puede ocasionar graves perjuicios para la economía del país, por lo que resulta necesario que su solidez y solvencia sean supervisadas por el Estado.

2.2. El sector real, el sector financiero y el rol de la intermediación financiera.

Todos los bienes y servicios de las personas, así como los medios para producirlos, conforman el sector real de la economía, el cual finalmente materializa la riqueza de una sociedad. Sin embargo, para que los recursos del sector real se movilicen con mayor agilidad, se requiere del dinero o medios de pago en general. Al conjunto de medios de pagos se le denomina sector financiero y viene a ser un sector paralelo al sector real y tiene por objetivo facilitar el funcionamiento de este último. Ambos sectores se interrelacionan a través de muchas formas: los mercados donde se conforman los precios, la intermediación financiera, el mercado de créditos, entre otras.

La intermediación financiera está conformada por aquellos mecanismos e instituciones que permiten canalizar los recursos financieros de aquellos agentes económicos que poseen estos recursos en exceso, denominados normalmente ahorristas o inversionistas, hacia aquellos agentes que lo requieren (agentes deficitarios), a cambio de una retribución. La intermediación financiera permite que aquellos recursos financieros excedentes ahorrados por las personas o empresas intervengan en la producción de más riqueza. Por lo tanto, la primera utilidad para la sociedad es poner una mayor cantidad de recursos en acción para la generación de mayor riqueza. Esta riqueza adicional representará el pago al conjunto de la sociedad por dejar de consumir en el presente para hacerlo en el futuro. Una parte del beneficio obtenido por la sociedad se destina a cubrir los costos de la intermediación, incluidas las utilidades. En la figura siguiente (tomada de *'Introducción a la Banca'* de David Ambrosini) pueden apreciarse esquemáticamente las bases de la intermediación financiera.



La canalización de recursos financieros a través de los intermediarios financieros es posible porque estas instituciones pueden resolver mejor los problemas que enfrentan aquellos inversionistas que eligen invertir directamente en instrumentos financieros corporativos (bonos, acciones, etc.). El principal de estos problemas es el *alto costo de obtener la información* necesaria para monitorear adecuadamente el desempeño de las empresas emisoras de instrumentos financieros corporativos. En tal sentido un intermediario financiero que agrupa los fondos de varios inversionistas tiene menores costos y mayores incentivos para monitorear el desempeño de las empresas emisoras. Por ello se dice que los intermediarios financieros cumplen la función de ***monitoreo delegado*** para actuar en representación de los inversionistas.

Las principales instituciones de intermediación financiera son las empresas bancarias o bancos, las financieras y las empresas de arrendamiento financiero. Al 15 de octubre de 1999, las empresas de intermediación financiera en el Perú mantenían un total de activos por más de 78 mil millones de soles, distribuidos de la siguiente manera:

ACTIVOS DEL SISTEMA FINANCIERO PERUANO

(Al 15 de octubre de 1999)

Tipo de empresa	Cant.	Total de activos (en miles de nuevos soles)	Total de activos (eq. en miles de US$)
Bancos comerciales	24	73.393.938	21.090.212
Financieras	6	1.045.782	300.512
Empresas de arrendamiento financiero*	9	4.498.998	1.292.815
Total	**41**	**78.938.718**	**22.683.539**

Fuente: Superintendencia de Banca y Seguros. Elaboración propia (T.C.:S/.3,48 por US$).

** Estimado*

2.3. La empresa bancaria

La principal institución de intermediación financiera es la empresa bancaria, definida como aquella empresa cuyo negocio principal consiste en recibir dinero del público en depósito o bajo cualquier otra modalidad contractual, y en utilizar ese dinero, su propio capital y el que obtenga de otras fuentes de financiación en conceder créditos en las diversas modalidades, o a aplicarlos a operaciones sujetas a riesgos de mercado.

Las principales operaciones que realizan las empresas bancarias pueden ser agrupadas de la siguiente manera:

A. Captaciones:
   a. Recepción de depósitos a la vista, depósitos a plazo y de ahorros, así como depósitos en custodia.
   b. Emisión de certificados bancarios en moneda extranjera.
   c. Emisión y colocación de bonos, en moneda nacional o extranjera, incluidos los ordinarios, los convertibles, los de arrendamiento financiero, y los subordinados de diversos tipos y en diversas monedas, así como pagarés, certificados de depósito negociables o no negociables, y demás instrumentos representativos de obligaciones emitidas por la empresa.

B. Colocaciones:
   a. Otorgamiento de sobregiros o avances en cuentas corrientes.
   b. Otorgamiento de créditos directos, con o sin garantía.
   c. Descuento y concesión de adelantos sobre letras de cambio, pagarés y otros documentos comprobatorios de deuda.
   d. Aceptación de letras de cambio a plazo, originadas en transacciones comerciales

e. Concesión de préstamos hipotecarios y prendarios; y, en relación con ellos, emitir títulos-valores, instrumentos hipotecarios y prendarios, tanto en moneda nacional como extranjera.
f. Operaciones de factoring.
g. Operaciones de arrendamiento financiero.

C. Operaciones Interbancarias:
a. Operaciones de crédito con bancos y financieras del exterior, así como efectuar depósitos en unos y otros.

D. Operaciones sujetas a Riesgos de Mercado
a. Operaciones en moneda extranjera.
b. Tomar o brindar cobertura de "commodities", futuros y productos financieros derivados.
c. Adquirir, conservar y vender instrumentos representativos de deuda privada (bonos) e instrumentos representativos de capital para la cartera negociable (acciones), que sean materia de algún mecanismo centralizado de negociación (Bolsa de Valores).
d. Adquirir, conservar y vender, en condición de partícipes, certificados de participación en los fondos mutuos y fondos de inversión.

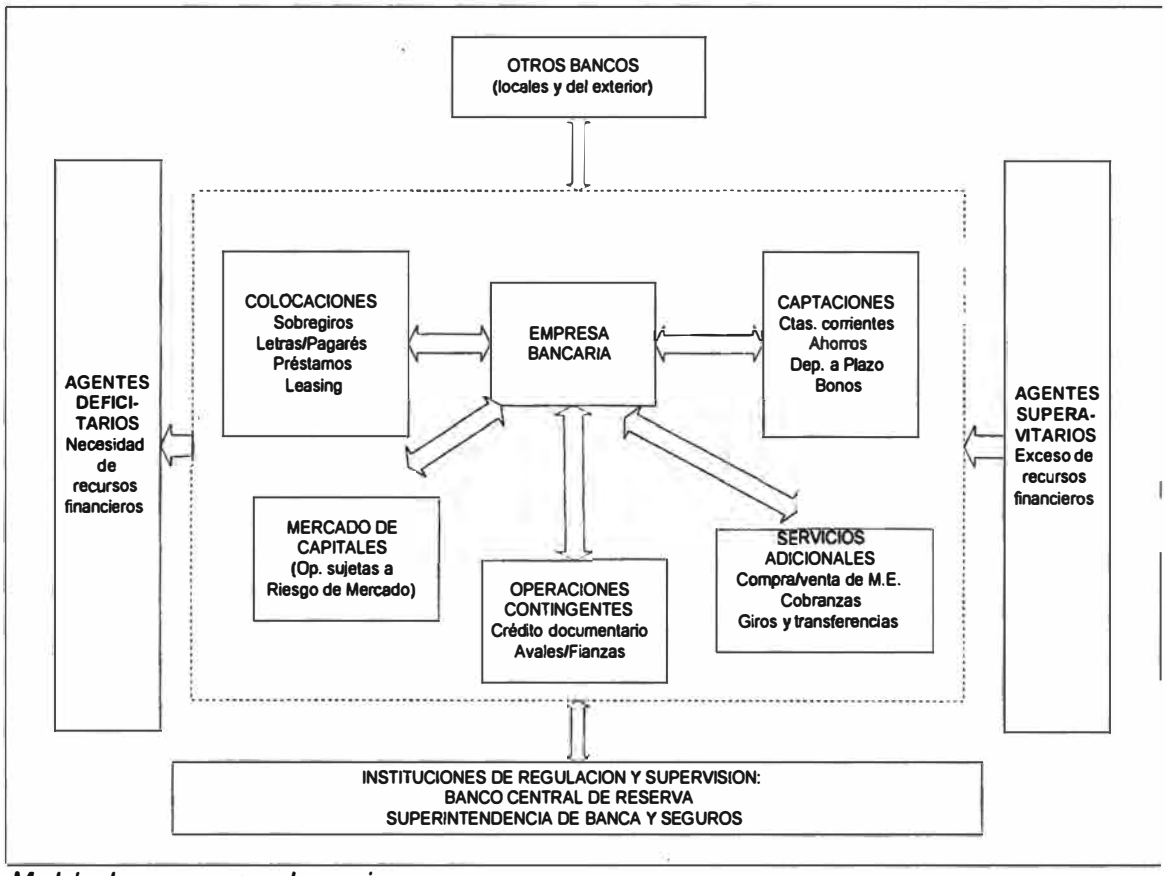
E. Operaciones Contingentes:
a. Otorgamiento de avales, fianzas y otras garantías, inclusive en favor de otras empresas del sistema financiero.
b. Emisión, confirmación y negociación de cartas de crédito, a la vista o a plazo, de acuerdo con los usos internacionales y en general operaciones de comercio exterior.

F. Servicios adicionales
a. Compra/Venta de moneda extranjera
b. Cobranzas

c. Giros y transferencias

Estos son sólo algunos de los numerosos instrumentos financieros tanto pasivos (captación de fondos) como activos (colocaciones) que ofrecen los bancos al público en general en su rol de intermediario financiero. De acuerdo a los cambios en las preferencias de los clientes, cambios tecnológicos o cambios en el entorno legal en el que operan pueden crearse diversos productos financieros basados en estos instrumentos.

En la figura sigiuiente se muestra un esquema con las principales operaciones y procesos de las empresas bancarias descritas en los párrafos anteriores.



Modelo de una empresa bancaria.

La interrelación entre todas aquellas empresas bancarias que brindan servicios de intermediación financiera alrededor de una región determinada (a nivel nacional o global) forman el denominado ***sistema bancario***. Las interrelaciones entre las empresas bancarias se dan principalmente a través de las operaciones interbancarias y la competencia existente tanto en el mercado de captaciones (depósitos) como en el de colocaciones (préstamos).

2.4. Los riesgos en el negocio bancario

La naturaleza de las operaciones que se realizan en el negocio bancario, expone a las empresas bancarias a un conjunto de riesgos. En realidad, la administración de una empresa bancaria está basada principalmente en la administración de los riesgos a los que se encuentra expuesta la empresa. A continuación se describen brevemente los cinco principales riesgos existentes en el negocio bancario:

Riesgo crediticio.- El riesgo crediticio aparece cuando las cuotas prometidas en los préstamos concedidos por las empresas bancarias no son pagadas por completo. Esto puede ocurrir porque las empresas que obtienen los préstamos experimentan problemas financieros (flujo de caja) que les impide efectuar a tiempo el pago de dichos préstamos en los plazos acordados. Esto ocurre igualmente cuando la empresa bancaria invierte en instrumentos financieros de renta fija (p.ej. bonos corporativos), los cuales presentan una naturaleza similar a las concesiones de préstamos.

Riesgo de tasa de interés.- Las empresas bancarias captan fondos a determinados plazos, acordando el pago de una tasa de interés (pasiva), y posteriormente colocan dichos fondos a otros plazos, cobrando una tasa de interés mayor (activa). La diferencia (o descalce) de plazos entre los activos y pasivos de una empresa bancaria, la expone a un riesgo de tasa de interés. Así por ejemplo, si una empresa bancaria capta fondos a 1 año a una tasa de interés de 9% anual, y coloca estos fondos a 2 años a una tasa de interés del 10% anual, obtendría durante el primer año

una ganancia debida a un 'spread' positivo del 1%. Sin embargo, si al término del primer año, las condiciones del mercado de captaciones le permiten a la empresa captar fondos a una tasa no menor del 11% anual, la empresa obtendría una pérdida debida a un 'spread' negativo (-1%). Un caso similar puede ocurrir en el caso inverso en que el plazo de los fondos captados (pasivos) sea mayor que los préstamos concedidos (activos).

Riesgo de mercado.- El riesgo de mercado aparece en la cartera de inversiones negociables de la empresa bancaria. La cotización de estas inversiones, que incluyen instrumentos de renta fija y renta variable, así como instrumentos derivados, está sujeta a las variaciones de precios en el mercado de capitales. El riesgo de mercado puede definirse como la incertidumbre en los ingresos de la institución financiera provenientes de los cambios en las condiciones de mercado que incluyen el precio de activos, las tasas de interés, y la volatilidad y liquidez del mercado.

Riesgo de liquidez.- El riesgo de liquidez aparece cuando los acreedores de la empresa bancaria, tales como los depositantes, demandan efectivo para satisfacer sus requerimientos financieros. A pesar que los intermediarios financieros minimizan la cantidad de efectivo disponible, dado que dicho efectivo no gana interés, los requerimientos regulares de efectivo de los acreedores normalmente son predecibles y pueden ser atendidos. Sin embargo, puede ocurrir una crisis de liquidez en caso exista una falta de confianza en la empresa bancaria o se produzca una necesidad imprevista de efectivo, ante lo cual los acreedores demandarán retiros de efectivo mayores a los normales. Cuando muchas empresas bancarias o financieras experimentan estos problemas el costo de fondos adicionales se incrementa y su provisión se restringe. Como consecuencia de ello, las empresas bancarias pueden verse obligadas a vender algunos de sus activos menos líquidos, normalmente a precios más bajos de los esperados, lo cual puede amenazar seriamente la solvencia de la empresa.

Riesgo tecnológico o informático.- El riesgo informático, o riesgo asociado al uso de los sistemas de información, se define como la probabilidad de sufrir pérdidas en el patrimonio de la empresa o disminución de sus utilidades, debido a un funcionamiento inapropiado de sus sistemas de información. Este funcionamiento inapropiado puede traducirse en fraudes informáticos, paralización de operaciones debido a fallas en los sistemas, accesos no autorizados a los sistemas de la empresa, falta de integridad y consistencia en la información generada por los sistemas, etc. La naturaleza de este riesgo y el diseño de una metodología sistemática para su análisis es el tema central del presente estudio, y será detallado en los capítulos siguientes.

2.5. La necesidad de regulación y supervisión del sistema bancario

Al igual que otras instituciones de intermediación financiera las empresas bancarias requieren ser reguladas y supervisadas. Esto se debe a que las fallas y problemas que puedan existir en el sistema bancario pueden generar efectos adversos en el resto de la economía (externalidades negativas). Por ejemplo, la quiebra de un banco perjudica a los ahorristas (depositantes) y al mismo tiempo restringe el acceso al crédito de algunas empresas. Más aún, la quiebra de varios bancos individuales puede crear dudas en los ahorristas acerca de la estabilidad y solvencia del sistema bancario en general y causar eventuales corridas bancarias, generando problemas en la economía de un país.

En tal sentido, con el fin de proteger a los depositantes y prestatarios contra el riesgo de la quiebra de una institución financiera, la regulación debe considerar diferentes niveles de protección:

a. *Un primer nivel* consiste en requerir que la institución financiera diversifique sus activos a través de la definición de límites para el otorgamiento de créditos a una sola empresa o a grupos vinculados (límites individuales).

b. *Un segundo nivel* consiste en definir niveles mínimos de patrimonio efectivo necesario (aporte de accionistas) para contribuir al financiamiento de las operaciones de la empresa.
c. *Un tercer nivel* es el aporte hacia un fondo de garantía que permita proteger los depósitos de los ahorristas en caso de quiebra de una institución financiera (en el Perú, se denomina Fondo de Seguro de Depósitos).
d. *Un cuarto nivel* es la supervisión y monitoreo en sí mismas, a través del envío de información periódica de las instituciones financieras a los organismos de supervisión, o la supervisión in-situ realizada por dichos organismos.

2.6. El sistema bancario peruano

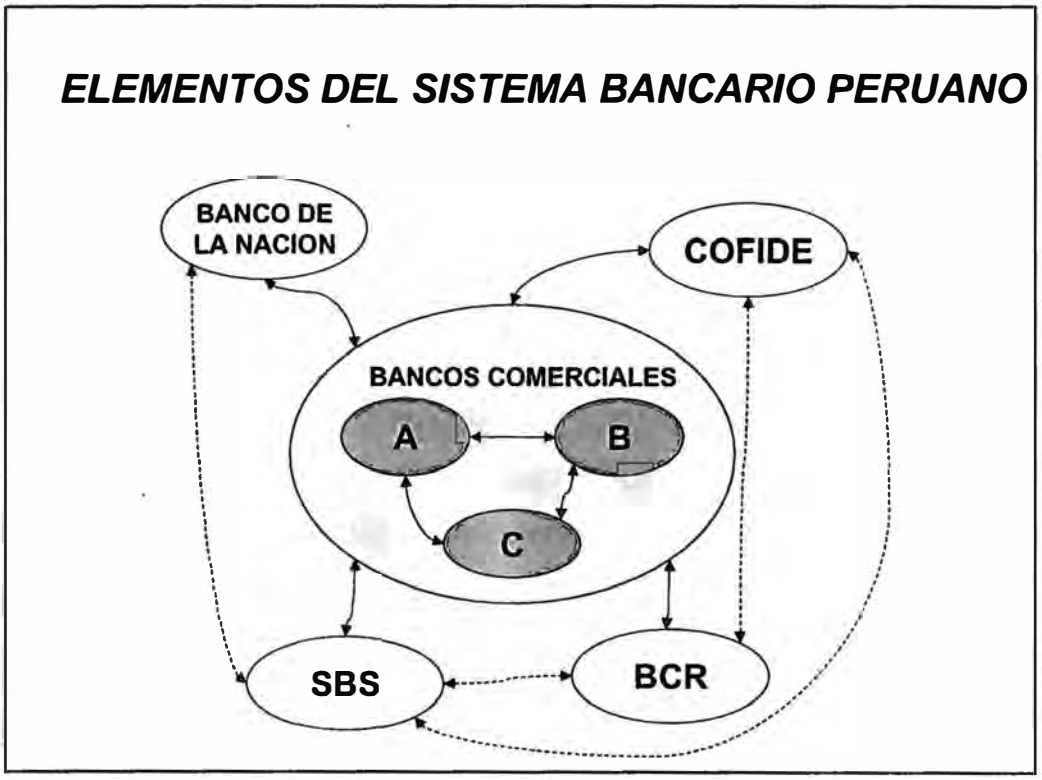
El sistema bancario peruano ha cambiado sustancialmente desde la implementación de las reformas liberales aprobadas en los primeros años de la década del 90. Las nuevas regulaciones bancarias y la virtual liberalización del sector de servicios financieros han incrementado la competencia y han contribuido notablemente a la modernización del sector.

El factor más importante que ha determinado el cambio en la configuración del sistema bancario peruano ha sido la entrada de la competencia extranjera. En tal sentido, pueden mencionarse los casos del Banco Bilbao Viscaya, el Banco Santander y el Banco Central Hispano de España; el Banque Sudameris de Francia, el Standard Chartered Bank de Inglaterra, el Citibank y el BankBoston de Estados Unidos, entre otros.

La entrada de los bancos extranjeros y el consiguiente aumento de la competencia han determinado una modernización de la industria de los servicios financieros en el Perú.

Elementos del sistema bancario peruano

Al mes de octubre de 1999, el sistema bancario peruano se encuentra conformado por 24 bancos comerciales. Adicionalmente, existen otras instituciones que interactúan directamente con las empresas del sistema bancario peruano: el Banco de la Nación, la Corporación Financiera de Desarrollo - COFIDE, el Banco Central de Reserva y el organismo de supervisión y control, la Superintendencia de Banca y Seguros. En el gráfico siguiente se muestra la interrelación entre estas instituciones y las empresas del sistema bancario.



El Banco de la Nación es un banco de propiedad estatal, y tiene como principales funciones: la recaudación de los ingresos fiscales (pago de impuestos e imposiciones judiciales) y el pago a los empleados del sector público (activos y pensionistas).

La Corporación Financiera de Desarrollo - COFIDE es una empresa que cuenta con participación del Estado y de bancos comerciales. Su principal función es la de actuar como un banco de desarrollo de "segundo piso", lo cual significa que canaliza los recursos del Estado hacia el sistema financiero a través de préstamos o líneas de crédito. Este financiamiento incluye tanto a los bancos, como a entidades financieras más pequeñas como las Cajas Rurales de Ahorro y Crédito y las EDPYMEs, dirigidas al financiamiento de actividades del sector agrario (rural) y de las pequeñas y micro empresas respectivamente.

Las instituciones de regulación y supervisión

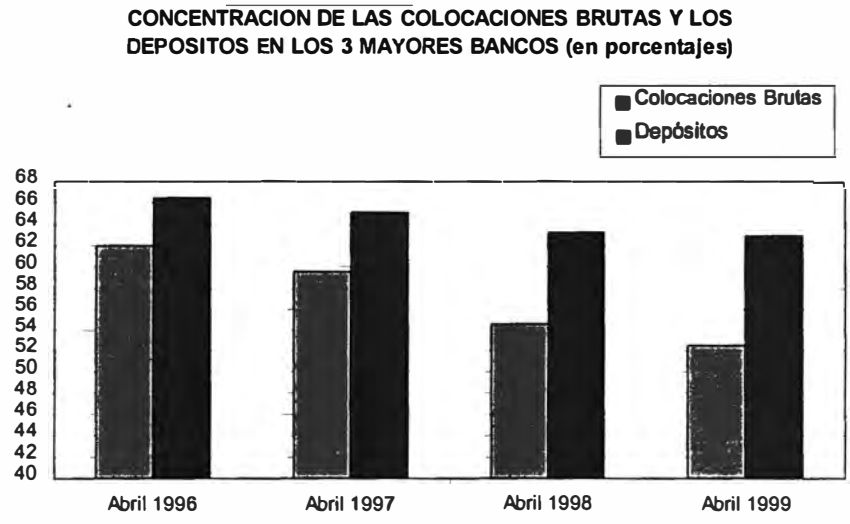
El Banco Central de Reserva (BCR) establece la política monetaria, la cual incluye la regulación de la oferta monetaria, la administración de las reservas internacionales, la determinación de la Balanza de Pagos y otras cuentas monetarias y la revelación de la situación financiera del país. La estabilidad monetaria es la principal función del BCR.

La Superintendencia de Banca y Seguros (SBS) es una institución autónoma gubernamental encargada de la regulación y supervisión del sistema financiero y de seguros, autorizando las nuevas licencias de funcionamiento y supervisando las actividades de todas las entidades financieras. Su principal rol es la protección del público asegurando la estabilidad financiera de las entidades bajo su supervisión. La SBS puede interpretar la ley, emitir normas de regulación financiera e imponer sanciones que incluyen la clausura y disolución de las empresas financieras bajo su supervisión.

Características del sistema bancario peruano

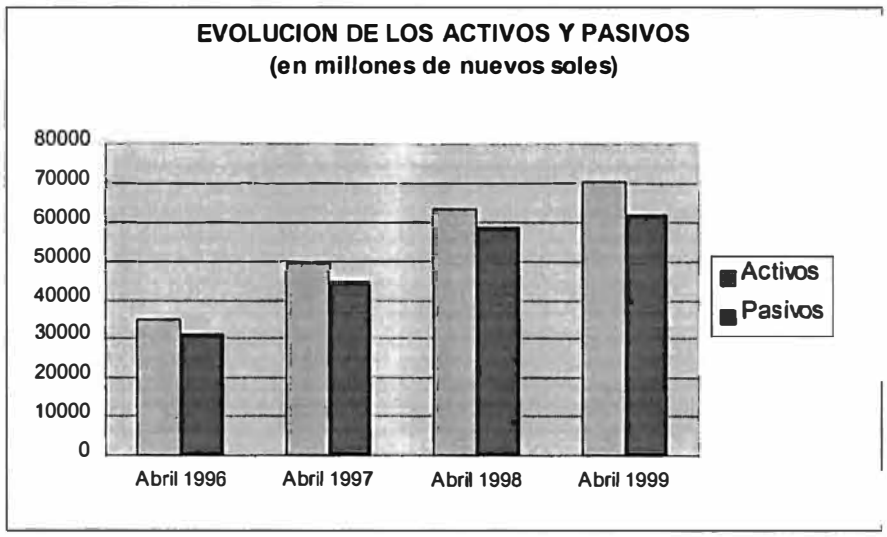
Una de las características del sistema bancario peruano es su alta concentración: al mes de abril de 1999, los tres mayores bancos comerciales: Crédito, Wiese y Continental captaban el 62,97% de los depósitos totales y concentraban el 52,60%

de las colocaciones brutas, aún cuando dicha concentración ha mostrado una ligera tendencia a la baja según puede apreciarse en el cuadro adjunto.



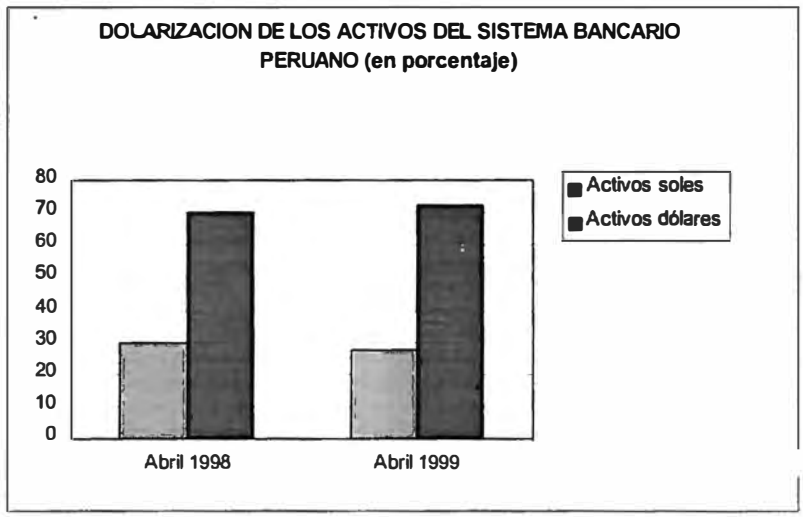
Fuente: Superintendencia de Banca y Seguros. Elaboración propia.

Asimismo, el sistema bancario peruano se encuentra en una fase de crecimiento, según se puede apreciar en el cuadro adjunto, en el que se señalan los totales en activos y pasivos durante los últimos 4 años. Sin embargo, debe señalarse que existe una tendencia decreciente en las tasas de crecimiento anual de las colocaciones y depósitos en los últimos tres años.



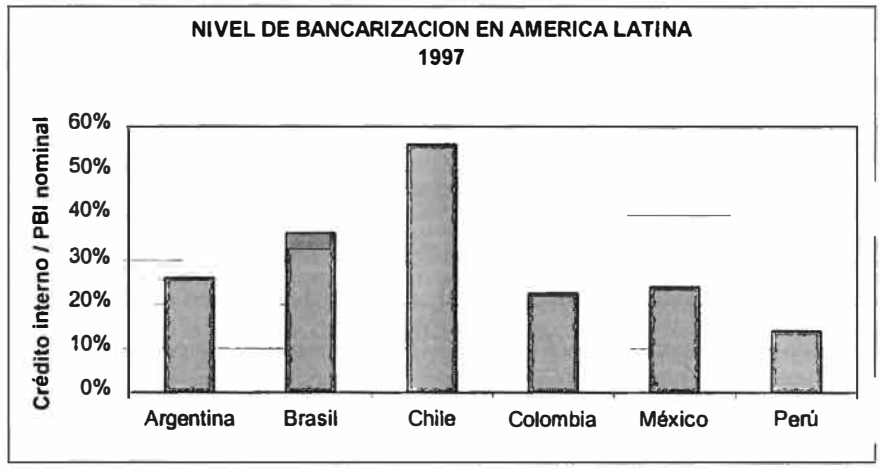
Fuente: Superintendencia de Banca y Seguros. Elaboración propia.

En cuanto a la dolarización de las operaciones bancarias, se observa una mayor participación de las operaciones en moneda extranjera, las cuales pasaron de representar el 70,33% del total de activos en abril de 1998, a representar el 72,43% a fines de abril de 1999.



Fuente: Superintendencia de Banca y Seguros. Elaboración propia.

Finalmente, debe señalarse que a pesar de encontrarse en una fase de crecimiento, el sistema bancario peruano aún es pequeño en comparación con otros países de la región. Esto puede apreciarse mejor en el cuadro adjunto, en el cual se muestra el nivel de bancarización en el Perú, medido a partir de la proporción que representa el crédito interno del país con respecto al PBI nominal.



Fuente: Banco Interamericano de Desarrollo. Unidad de Estadística y Análisis Cuantitativo. Elaboración propia.

Perspectivas del sistema bancario peruano

Los altos niveles de inversión realizados en el Perú en los últimos años, unido con una baja penetración de los servicios bancarios, proporcionaban un entorno positivo para el crecimiento sostenido en préstamos corporativos al igual que una expansión del mercado de préstamos para empresas medianas y de los préstamos de consumo. Sin embargo, en 1998 el efecto de la crisis asiática y los impactos del fenómeno del Niño, entre otras causas, originaron una restricción de la liquidez en el sistema bancario peruano, así como un deterioro del sector productivo. Esto determinó un aumento en la morosidad de la cartera crediticia y una reducción significativa en las utilidades de los bancos peruanos durante ese año.

Como consecuencia de lo anterior, dos bancos dedicados a los préstamos de consumo (Banco Solventa y Serbanco) se vieron obligados a reorientar su estrategia de negocios y dedicarse a otros segmentos de mercado. Asimismo, hacia finales de ese año dos bancos experimentaron problemas (aunque de naturaleza diferente). El Banco República, del grupo chileno Errazuriz, fue intervenido y posteriormente entró en proceso de liquidación, mientras que el Banco Latino, sufrió una reestructuración patrimonial que llevó a COFIDE a convertirse en su principal accionista. En el primer caso, se puso a prueba el funcionamiento del seguro de depósitos, lográndose devolver los depósitos de la gran mayoría de los ahorristas del Banco, coberturados por el Fondo de Seguro de Depósitos, de acuerdo a ley.

Durante 1999 se han dispuesto un conjunto de medidas destinadas a aumentar la demanda interna, y a apoyar la reestructuración de los préstamos concedidos a empresas productivas aún viables, pero que experimentaron problemas durante 1998. En tal sentido, el Ministerio de Economía y Finanzas ha dispuesto la canalización de fondos a través de COFIDE hacia los bancos comerciales, con el fin de reestructurar dichos préstamos. Asimismo, ha creado un programa de canje de bonos del Tesoro Público por cartera pesada, y finalmente ha dispuesto que los

bancos puedan capitalizar sus acreencias en empresas que no cotizan en la Bolsa de Valores de Lima.

El panorama existente ha determinado la necesidad de fusiones entre las empresas del sistema bancario. Así por ejemplo, a mediados de 1999, se oficializó el acuerdo entre el Banco Wiese Ltdo. (2° en el ranking de depósitos) y el Banco de Lima Sudameris (5°) para la formación del Banco Wiese Sudameris, y se espera que en los siguientes meses se oficialice la fusión entre el Banco Santander Perú y Bancosur, cuyas casas matrices (Banco Santander de España y Banco Central Hispano, respectivamente) ya formalizaron su fusión. Estas fusiones permitirán dar mayor solidez al sistema bancario peruano, y transmitirán mayor confianza a los ahorristas.

En resumen, el sistema bancario peruano actualmente es un sistema sólido y en crecimiento. El nivel de bancarización existente en el Perú se encuentra aún por debajo del promedio de América Latina, lo cual ofrece perspectivas interesantes de crecimiento. Sin embargo, es necesaria la recuperación del sector productivo a través del aumento de la demanda interna. Asimismo, elevar el nivel de cultura bancaria entre el público, y particularmente entre los pequeños y medianos empresarios, es una tarea pendiente para las empresas del sistema bancario.

CAPITULO III

EL USO DE LA TECNOLOGIA DE INFORMACION EN LAS EMPRESAS BANCARIAS

3.1. Introducción

Uno de los aspectos más importantes para el funcionamiento de las empresas bancarias, lo constituye, sin lugar a dudas, el uso adecuado de la tecnología de información. Las aplicaciones de la tecnología de información en el sector bancario son cada vez más variadas y de mayor impacto. Inicialmente el uso de la tecnología de información estuvo limitado a la automatización de transacciones rutinarias y la preparación de reportes financieros, pero en la actualidad se utiliza, entre otros aspectos, en la automatización de las operaciones y procesos administrativos de una empresa bancaria, como soporte a la toma de decisiones de nivel táctico y estratégico, y para desarrollar complejos productos financieros utilizando sofisticados modelos de valorización. Asimismo los avances tecnológicos en el área de comunicaciones y conectividad han permitido minimizar los límites geográficos dentro del sector, y desarrollar nuevos canales de distribución de los servicios bancarios.

En las siguientes secciones, se describen las principales aplicaciones de la tecnología de información en el sector bancario, agrupadas en cuatro áreas:

a) Automatización de las operaciones bancarias.
b) Soporte a la toma de decisiones
c) Banca electrónica y el uso de Internet
d) Comercio electrónico

3.2. Automatización de las operaciones bancarias

La tecnología de información ha permitido automatizar las operaciones de todas las áreas de negocio y las áreas administrativas de una empresa bancaria. Actualmente existen soluciones informáticas que han permitido automatizar un conjunto amplio de operaciones bancarias, como por ejemplo:

a. Captaciones

Permiten la administración integral de las operaciones de depósito y retiro de fondos de las cuentas de ahorros o cuentas corrientes de los clientes. De igual manera, administran las cuentas de depósitos a plazo y el manejo de cheques, cuya conciliación se realiza a través de cámaras de compensación.

Estas operaciones se realizan en línea y tiempo real, buscando un manejo eficiente de altos volúmenes de transacciones con adecuados tiempos de respuesta. Los cálculos de intereses, las operaciones contables y los costos asociados a cargos por comisiones o mantenimientos de cuenta se realizan automáticamente.

b. Líneas pasivas de crédito

Permiten la administración de las líneas de crédito de la entidad financiera, otorgadas por fuentes externas para el financiamiento de proyectos y recursos propios de la entidad. Esta administración incluye el control de las características de cada fuente de recursos, el manejo de las asignaciones, los desembolsos, los reembolsos y la disponibilidad.

c. Colocaciones

Permiten la automatización de las diferentes operaciones de crédito propias de una institución financiera, incluyendo la administración, organización y el control de los

documentos, garantías, eventos y etapas involucradas para el procedimiento de aprobación o rechazo de una operación de crédito definidos por la organización, de acuerdo con la calificación del cliente, logrando obtener un servicio eficiente.

Asimismo, existen soluciones para la administración de líneas de crédito, las cuales contribuyen a una adecuada utilización de los fondos, según las necesidades del cliente, fijando parámetros de disponibilidad para las diferentes modalidades de crédito en función de las políticas y procedimientos definidos por la institución. Estas modalidades incluyen: préstamos, sobregiros en cuentas corrientes, descuentos de letras, entre otros.

Además de ello, los sistemas de información permiten manejar refinanciamientos, renovaciones, reestructuras, fondeo de capitales, cálculos y revisiones automáticas de provisiones, cargos, saldos y tasas diarias o mensuales; así como también amortizaciones anticipadas, vencidas, retroactivas de capital e intereses, y orígenes de fondos por cada operación. Todo ello, con el fin de llevar un adecuado control de los préstamos concedidos.

En relación a los créditos de consumo, existen los modelos de "credit scoring", que permiten evaluar de manera automatizada a clientes potenciales, y de acuerdo a ello otorgar diversos tipos de créditos de consumo, incluyendo tarjetas de crédito y créditos para pequeños negocios.

d. Administración de garantías

Permiten la administración eficiente de las garantías presentadas, como: fianzas, avales y aceptaciones, entre otras, las cuales respaldan las operaciones de crédito, disminuyendo el riesgo de dichas operaciones.

e. Gestión de tesorería

Permiten administrar, controlar y hacer seguimiento a las operaciones de inversión realizadas por la entidad financiera para la colocación de fondos (inversiones en títulos-valores) o la captación de fondos a través de la emisión de valores propios (bonos ordinarios o de arrendamiento financieros).

Asimismo, permite administrar todas las operaciones relacionadas con la compra y venta de moneda extranjera y 'commodities' que se realizan en la institución de manera diaria o futura.

De otro lado, existen actualmente aplicaciones informáticas que permiten el uso de la denominada "ingeniería financiera", para la creación y valorización de complejos productos financieros derivados (opciones, swaps, etc.).

f. Operaciones de comercio exterior

Permiten la administración de instrumentos de comercio exterior, como: cartas de crédito de importación, exportación, avales y fianzas, cobranzas documentarias y aceptaciones de cartas de crédito y de cobranzas, entre otros.

g. Administración de agencias

Permiten la administración de las operaciones que se realizan en las agencias, a través de las ventanillas de atención a los clientes. Esta administración incluye el control de los montos máximos y mínimos en caja, la administración del efectivo, los pagos mediante cheques, incluyendo aquellos recibidos en depósitos, y definiendo la relación contable de todas las operaciones realizadas en ventanilla.

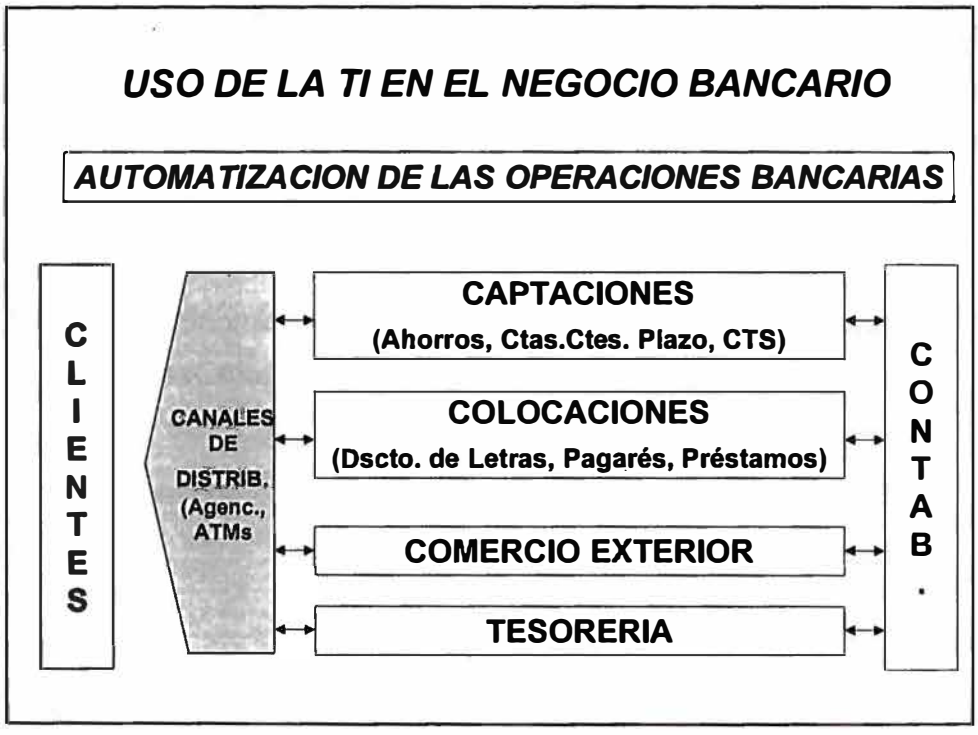
h. Operaciones con bancos del exterior

Las operaciones con instituciones financieras del exterior se realizan normalmente a través de la red internacional S.W.I.F.T., la cual proporciona el servicio de mensajería electrónica alrededor del mundo. Actualmente, cerca de 6500 instituciones financieras en 178 países se encuentran conectados a esta red, la cual cuenta con mecanismos de confidencialidad, autenticación y encriptación de la información enviada.

i. Contabilidad bancaria

Permiten registrar las diferentes transacciones realizadas durante el día y afectar las cuentas contables respectivas, a través de procesos de cierre diarios, los cuales permiten generar además estados financieros actualizados, según los requerimientos de la Gerencia respectiva y de los organismos de control.

En el gráfico siguiente se muestra un esquema simplificado de lo expresado en los párrafos anteriores:



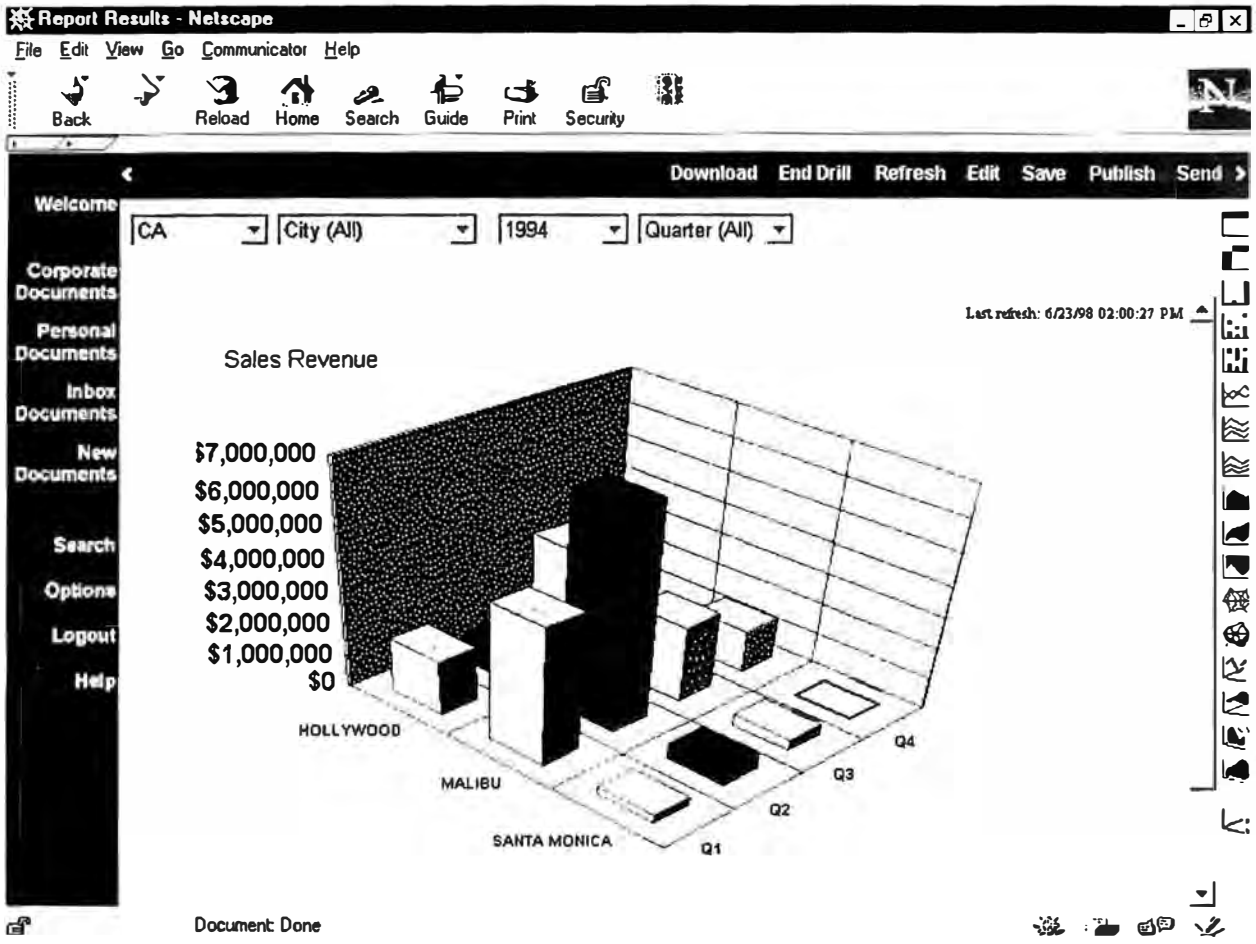
3.3. Soporte a la toma de decisiones

Las aplicaciones informáticas de soporte a la toma de decisiones tienen como objetivo transformar los datos procesados por los sistemas transaccionales que soportan las operaciones diarias de la empresa, en información que facilite la toma de decisiones a nivel táctico y estratégico. Asimismo, estas aplicaciones brindan a las áreas gerenciales y administrativas herramientas que permiten la ejecución de consultas reutilizables y análisis comparativo de sus resultados. Existen diversas técnicas utilizadas para estos aplicaciones, entre las que destacan:

a. Procesamiento Analítico en Línea u OLAP (On-Line Analytical Processing)

Los sistemas OLAP permiten analizar los datos de la empresa proporcionando un acceso rápido, consistente e interactivo a una amplia variedad de posibles vistas de la información, y considerando las dimensiones existentes en dicha información. Así por ejemplo, una empresa bancaria podría analizar la información de las transacciones realizadas durante el mes anterior por día, por hora, por agencia, por producto, por tipo de cliente, por tipo de transacción, etc. Estas diferentes vistas de la información permiten una mayor riqueza en el análisis y facilitan la toma de decisiones. De otro lado, estas aplicaciones permiten realizar análisis de sensibilidad del tipo "Qué pasaría si...", lo cual es sumamente útil para la toma de decisiones entre políticas alternativas.

En la pagina siguiente se muestra un ejemplo de este tipo de sistema, la herramienta se denomina *WebIntelligence* y ha sido desarrollada por la compañía francesa *BusinessObjects*.



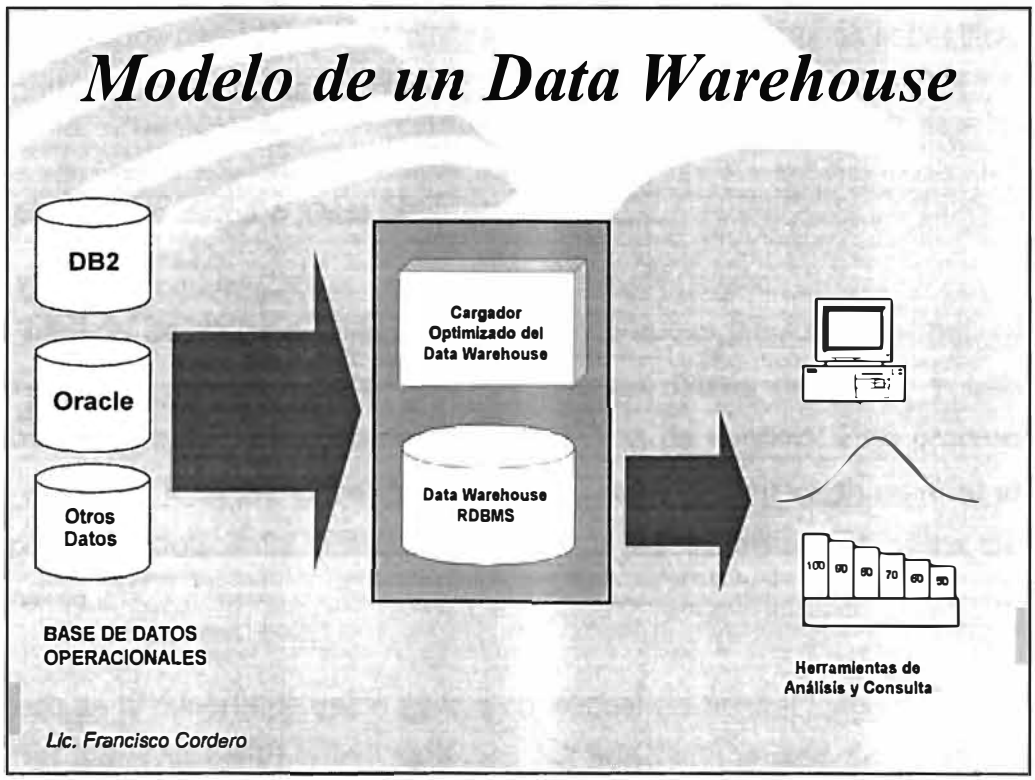
b. Construcción de un almacén centralizado de datos o 'data warehouse'

Un almacén centralizado de datos o 'data warehouse' es un repositorio central de datos sumarizados a partir de diferentes sistemas operacionales internos y de fuentes externas. Los datos son extraídos, integrados y sumarizados en el almacén de datos, y a partir de él pueden ser accesados por los usuarios finales en formatos consistentes y orientados a temas específicos, generalmente relacionados con entidades del negocio como cliente, producto o región geográfica.

Un almacén de datos tiene una estructura muy diferente a la de un sistema operacional. Los datos en un data warehouse deben ser:

- Archivados y sumarizados
- Organizados por temas específicos y no por aplicación
- Estáticos hasta su actualización periódica, en lugar de dinámicos.
- Simplificados para el análisis
- No estructurados para un procesamiento repetitivo.

En el gráfico siguiente se muestra un modelo para la construcción de un data warehouse.



Un data warehouse proporciona muchas ventajas para el soporte a la toma de decisiones:

- Es posible ejecutar rápidamente consultas complejas, dado que todos los datos se encuentran almacenados en un formato consistente y centralizado.

- Las consultas no interfieren con las operaciones diarias, dado que el almacén de datos está dedicado exclusivamente a la extracción de reportes o consultas.
- Los datos pueden ser organizados por categorías útiles, como clientes o productos dado que previamente ha sido consolidada a partir de diferentes fuentes.

El data warehouse proporciona una visión global de los datos de la empresa. A partir de este almacén centralizado es posible generar pequeños almacenes de datos de nivel departamental, conocidos como 'Data Marts', los cuales normalmente son utilizados para generar consultas orientadas a las funciones específicas de cada departamento o área de negocio.

c. Minería de datos o 'Data Mining'

La minería de datos o 'data mining' es un proceso dirigido a extraer información previamente desconocida a partir de grandes bases de datos, y utilizar dicha información para tomar decisiones estratégicas de negocio. Este proceso se basa en el uso de técnicas estadísticas que normalmente demandan un nivel elevado de soporte computacional, incluyendo el uso de procesamiento de bases de datos en paralelo.

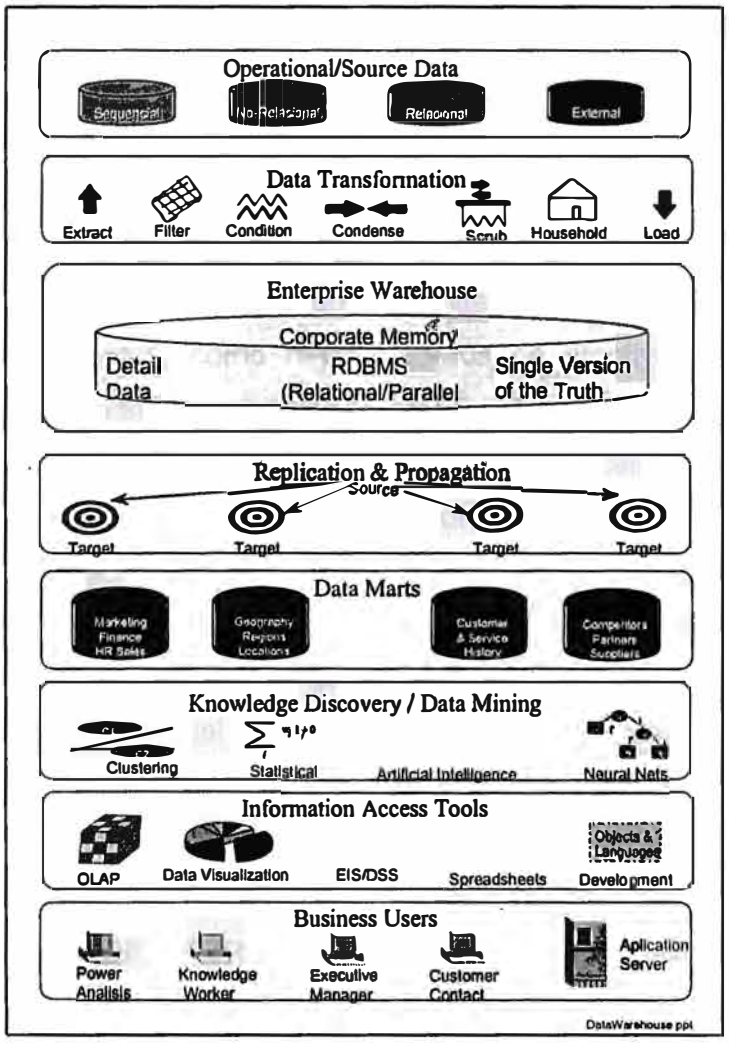
El uso de la minería de datos es una consecuencia natural luego de la construcción de un almacén centralizado de datos. Un adecuado diseño de dicho almacén de datos (o 'data warehouse') proporciona una fuente de datos apropiada para transformar los datos en información útil y confiable, que permite soportar el proceso de toma de decisiones.

Algunas de las aplicaciones existentes de la minería de datos en el sector bancario, incluyen:

- Detectar patrones de uso fraudulento de tarjetas de crédito.

- Identificar a los clientes más leales.
- Agrupar a los clientes de tarjeta de crédito de acuerdo a sus patrones de gasto.
- Encontrar correlaciones escondidas entre diferentes indicadores financieros.
- Identificar patrones en las transacciones de valores (acciones, bonos) a partir de los datos históricos del mercado.

En el esquema siguiente, se grafican las diferentes etapas y técnicas existentes para transformar los datos provenientes de los sistemas operacionales que soportan las operaciones diarias de la empresa en información estratéfica útil para la toma de decisiones.



3.4. Banca Electrónica y el uso de Internet

La banca electrónica consiste en la distribución de información, productos y servicios entre un cliente y una institución financiera usando dispositivos electrónicos como teléfonos, cajeros automáticos, redes de puntos de venta, cámaras de compensación automatizadas y computadores personales. Normalmente, estos dispositivos se encuentran conectados a través de redes de comunicación, como líneas telefónicas, redes privadas o Internet. La banca electrónica constituye en la actualidad uno de los principales canales de distribución de servicios bancarios utilizados por las entidades financieras. En particular, debe destacarse que el uso de la red mundial Internet para dichas operaciones se ha incrementado notablemente en los últimos años.

A. Cajeros automáticos

Los cajeros automáticos (o ATMs: Automated Teller Machines) son terminales de computador conectados en red, que permiten proporcionar diversos servicios bancarios a los clientes, como realizar retiros de efectivo, transferencias entre cuentas, consultas de saldos, pagos a terceros, entre otros. Los cajeros automáticos operan durante las 24 horas del día y se encuentran localizados dentro o fuera de las agencias bancarias. Los retiros diarios normalmente se encuentran limitados a pequeñas cantidades.

Los cajeros automáticos se activan generalmente a través de una tarjeta de plástico con banda magnética, la cual es introducida por el cliente en el momento de iniciar una transacción. Además de ello, el cliente debe ingresar un número personal de identificación (o 'clave secreta'). Los cajeros automáticos operan ya sea en modo fuera de línea, como en línea. Las transacciones realizadas fuera de línea son registradas en una cinta y transportadas físicamente a la institución financiera para su procesamiento diario.

Normalmente, las redes de cajeros automáticos son compartidas entre dos o más instituciones financieras con el fin de compartir los costos de funcionamiento y aprovechar las economías de escala. En tal sentido, existen redes de cajeros compartidas por un grupo de instituciones financieras y administradas por una empresa externa (P.ej. Unibanca en Perú), así como redes de cajeros que simplemente se interconectan entre sí, permitiendo a un cliente de una empresa bancaria hacer uso de los cajeros de otra red. Igualmente, existen redes propietarias de cajeros automáticos, las cuales permiten que solamente los clientes de una determinada empresa bancaria puedan hacer uso de dicha red.

B. Puntos de Venta

Los terminales de Punto de Venta permiten a los clientes, realizar consumos en establecimientos comerciales afiliados sin necesidad de disponer de efectivo, sino a través del uso de tarjetas de crédito o débito. En el caso de tarjetas de crédito, el establecimiento obtiene un código de autorización y genera un comprobante de pago (voucher), el mismo que debe ser firmado por el cliente. Este comprobante es presentado posteriormente al Banco, el cual procede a abonar el monto consumido en la cuenta del establecimiento, y a cargar dicho monto en la cuenta corriente del cliente. En el caso de las tarjetas de débito, el cliente autoriza la transacción, ingresando su número personal de identificación (clave secreta). Esto da como

resultado un débito automático a la cuenta del cliente, y el correspondiente crédito en la cuenta del establecimiento comercial donde se realiza la transacción.

C. Banca Telefónica

La Banca Telefónica permite al cliente realizar diversas operaciones bancarias desde su hogar o cualquier otro lugar, a través de la línea telefónica. Esto se realiza a través de un sistema automatizado que define un conjunto de menúes con diversas opciones que debe elegir el cliente para efectuar sus transacciones a través de la línea telefónica. Este esquema se puede complementar con personal de apoyo que asista a los clientes en aquellas transacciones no estructuradas que deseen realizar.

Las operaciones que pueden ser realizadas a través de la Banca Telefónica incluyen la consulta de saldos, pagos de tarjeta de crédito, pago de servicios, transferencia entre cuentras propias, entre otras. Una de las ventajas de la Banca Telefónica es que amplía el horario de atención de los Bancos, con respecto a las agencias, poniendo a disposición del cliente la posibilidad de efectuar sus operaciones en el momento que desee, sin tener que trasladarse hasta la agencia o cajero automático más cercano.

D. Banca por Internet

La Banca por Internet constituye un medio a través del cual los clientes de una empresa bancaria pueden realizar determinadas operaciones desde sus hogares u oficinas, utilizando para ello un computador personal conectado a Internet. Solamente es necesario conectarse al sitio web del banco y elegir el tipo de operación a realizar, ahorrando de este modo tiempo y dinero invertidos al acudir a una agencia bancaria.

Entre las operaciones bancarias que pueden realizarse a través de Internet se incluyen:

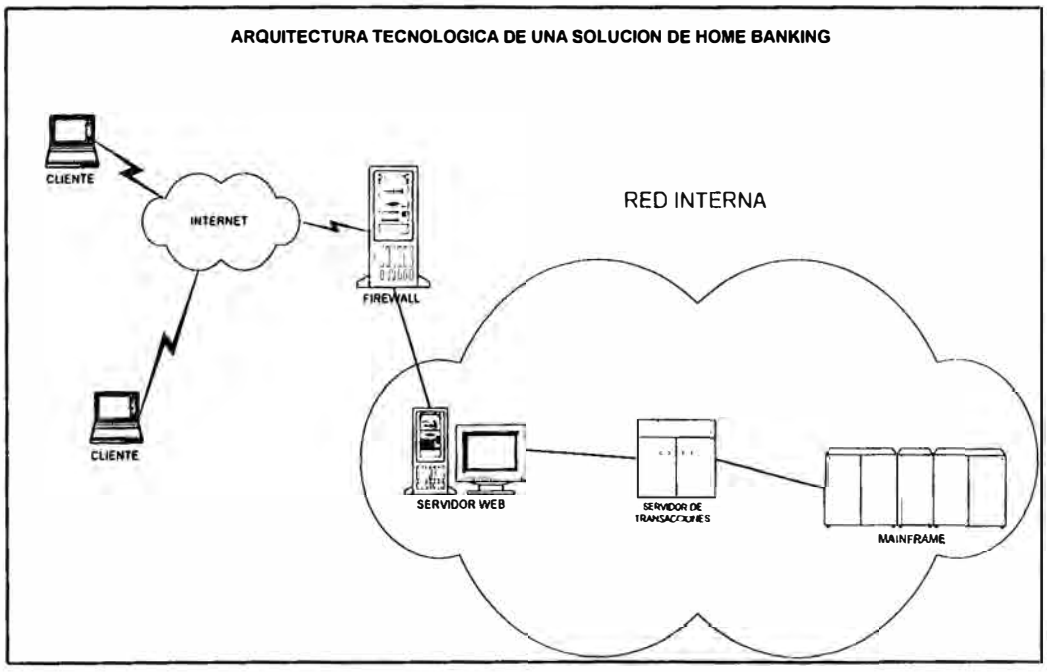
- Consultas de Saldos de Cuentas de Ahorros, Cuentas Corrientes, etc.
- Consultas de Movimientos de Cuentas de Ahorros, Cuentas Corrientes, etc.
- Pagos de servicios públicos: teléfono, agua, luz, etc.
- Pagos de tarjetas de créditos personales y empresariales
- Transferencias de fondos entre cuentas propias.
- Solicitud de chequeras para empresas
- Cancelación de solicitud de chequeras, etc.

Una de las ventajas de la distribución de servicios bancarios a través de Internet es su bajo costo, tanto para el cliente, como para la empresa bancaria. Así por ejemplo, se ha estimado que una transacción de pago en Internet le cuesta a la empresa bancaria - en promedio - 13 centavos de dólar o menos, cifra que resulta ser casi diez veces menor al compararla con el costo de esa misma operación en una agencia bancaria, aproximadamente unos 1,28 dólares.

La puesta en operación de un sitio web para la atención bancaria a través de Internet puede tener variadas formas de implementación, dependiendo básicamente de los siguientes factores:

- Servicios que la institución desee brindar a través de Internet
- Arquitectura tecnológica con la cual opera la entidad bancaria
- Niveles de seguridad que desee implementar

Dado que la gran mayoría de entidades financieras brindan, aproximadamente, los servicios especificados anteriormente es posible establecer un esquema general de arquitectura tecnológica para la implementación de la Banca por Internet, el cual se muestra en la figura siguiente



A continuación se explicará brevemente los elementos presentes en esta arquitectura tecnológica típica y su función dentro del conjunto:

Cliente: Persona o empresa que, a través de una PC conectada a Internet, realiza operaciones bancarias accediendo a la pagina web de un banco

Firewall: Una computadora, con software asociado, usada para impedir el acceso no autorizado, desde redes públicas (Internet), hacia redes privadas de computación (en este caso la red interna de la entidad bancaria). Es el encargado de realizar la autenticación a nivel de cliente (es decir, verifica que solo accedan a los datos de la empresa aquellas personas que están autorizadas para ello)

Servidor Web: Computador que procesa los pedidos de información de los clientes (browser) en Internet. Contiene la información que será mostrada en la página web de la empresa. El servidor y los datos son direccionados usando el URL. Para poder realizar operaciones comerciales seguras en Internet, este servidor debe tener una calificación de "servidor seguro" otorgada por empresas especializadas y que se visualiza con la expresión *https* en la dirección de la página web del site de la empresa. Incluye los protocolos SSL y SHTTP de encriptación de datos y autenticación a nivel de servidor, respectivamente.

Servidor de Transacciones: Computador que, ante una solicitud de datos, sirve de enlace entre el Servidor Web y los datos y/o aplicaciones existentes en el computador central de la organización. Al recibir un pedido de información genera una transacción (solicitud de información) hacia el computador central.

Host: Computador central de la organización donde residen los datos y se procesan las aplicaciones de la entidad bancaria.

3.5. El comercio electrónico

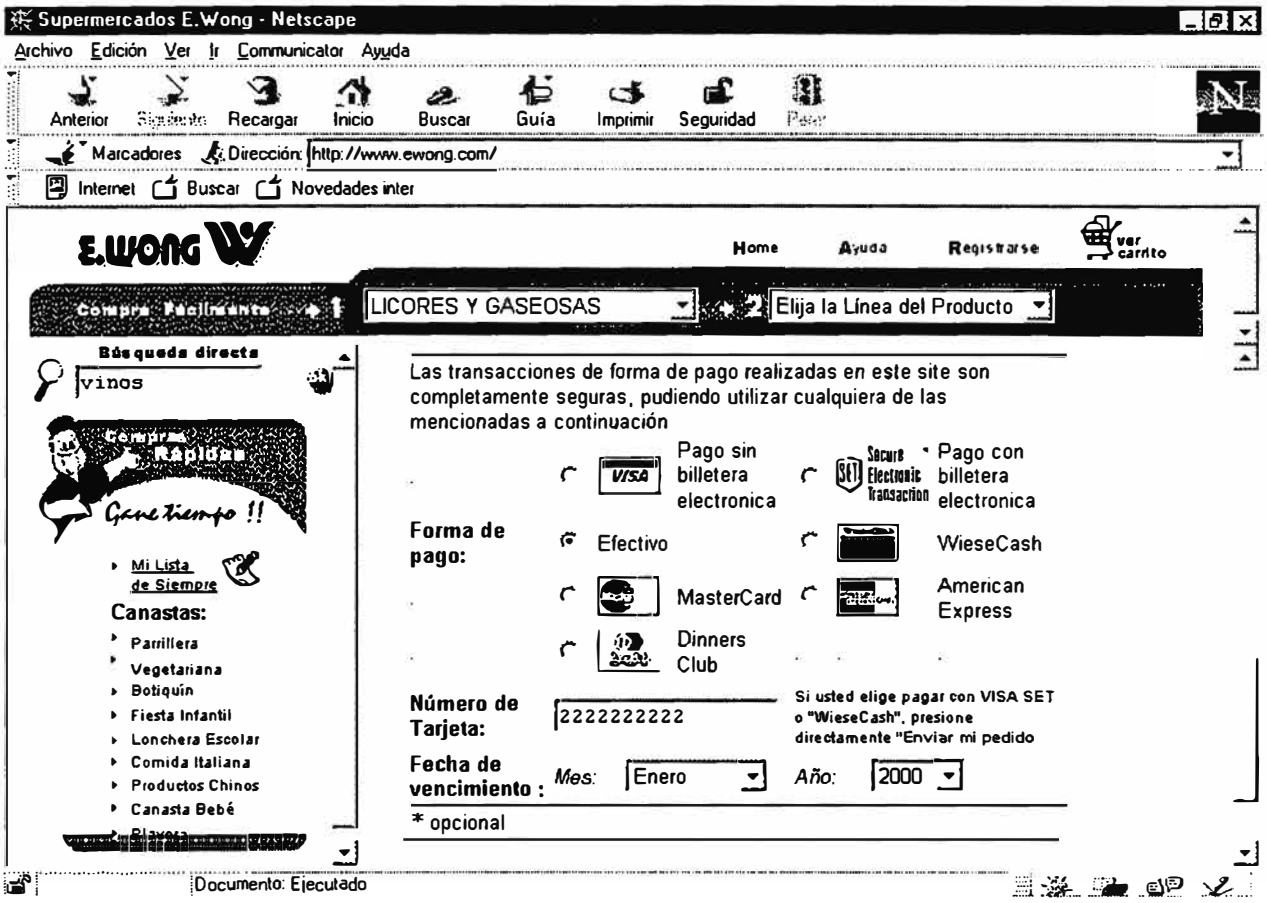
La rápida evolución en el uso de Internet ha permitido el desarrollo del comercio electrónico. El comercio electrónico permite que los consumidores puedan comprar desde sus casas una gran variedad de productos de diferentes productores y comerciantes de distintas partes del mundo. A través del uso de Internet, los consumidores pueden ver estos productos en sus computadores o televisores, acceder a información acerca de estos productos, ordenar sus pedidos y realizar el pago correspondiente, todo ello desde la comodidad de sus hogares.

El desarrollo del comercio electrónico ofrece una oportunidad para las empresas bancarias de brindar nuevos servicios a sus clientes. Así por ejemplo, los mecanismos de pago de los productos y servicios comercializados a través del Internet, incluyen enlaces con los sistemas de banca electrónica y con las redes de tarjetas de crédito y de débito existentes. Para ello se vienen desarrollando protocolos estándares que permiten brindar seguridad a las transacciones comerciales realizadas a través del Internet. El más importante de ellos es SET (Secure Electronic Transaction), promovido por los dos administradores de tarjetas de crédito más importantes del mundo: Visa y Mastercard.

El protocolo SET utiliza técnicas de certificación digital, basadas en una criptografía de clave pública RSA. El objetivo primordial de SET es mantener el carácter estrictamente confidencial de la información, garantizar la integridad del mensaje y autenticar la legitimidad de las entidades o personas que participan en una transacción comercial a través del Internet.

En el Perú el comercio electrónico se encuentra aún en una fase inicial de desarrollo. A partir de 1997 se desarrollaron las primeras 'tiendas virtuales', aunque no se brindaba todavía el enlace con la banca electrónica. En 1999 se lanzó la primera experiencia piloto entre la cadena de supermercados E.Wong S.A. y el Banco Wiese Ltdo, que permite realizar compras en la 'tienda virtual' de E.Wong en

Internet (http://www.ewong.com) y efectuar los pagos en línea mediante la tarjeta de débito WieseCash. Posteriormente, se han desarrollaron las funcionalidades para el enlace directo con las tarjetas de crédito como Visa, Mastercard, American Express y Diners Club. En la página siguiente se muestran las facilidades de pago existentes en esta 'tienda virtual' a través de la pantalla que se muestra al cliente en Internet.



3.6. Tendencias en el uso de la tecnología de información en el sector bancario

Además del desarrollo del comercio electrónico, el cual tendrá un gran impacto en la distribución de nuevos servicios bancarios adaptados a las características de esta nueva modalidad de comercio, existen otros temas que se encuentran actualmente en desarrollo, y que próximamente constituirán aplicaciones normales de la

tecnología de información en el sector bancario. A continuación describimos brevemente algunos de estos temas:

Dinero electrónico o 'e-cash'

Se trata de unidades con valor monetario, sin necesidad de estar vinculadas a una cuenta bancaria. Están destinados a transacciones de valor más bajo en principio que las tarjetas normales de crédito o débito, y permitirán, por ejemplo, el intercambio de dinero entre dos particulares. En algunos casos se ha puesto bastante énfasis en que permitan el anonimato (al menos del que paga) sin que pierdan seguridad. Siguiendo este esquema, el usuario se conecta en línea a su banco y retira una cantidad de monedas electrónicas a cargo de su cuenta que guarda en el disco duro de su "monedero digital". Este dinero electrónico puede utilizarlo a su gusto para realizar pagos a vendedores o individuos que acepten este tipo de transacción. El dinero electrónico normalmente se carga o descarga en tarjetas especiales, que cuentan con alguna circuitería electrónica inteligente, las cuales son descritas a continuación.

Tarjetas inteligentes o 'smart cards'

Se trata de tarjetas de plástico, a las cuales se les ha insertado una circuitería inteligente, incluyendo un microprocesador, que le permite cargar o descargar información asociada a cierta cantidad de dinero (dinero electrónico). El microprocesador de la tarjeta inteligente o 'smart card' cuenta con claves y algoritmos de encriptación desarrollados para codificar y decodifcar los datos grabados en la tarjeta. Una solución basada en el uso de tarjetas inteligentes debe incluir la implementación de lectoras de tarjetas, terminales, redes y sistemas de procesamiento de la información contenida en las tarjetas.

El uso de las tarjetas de 'pre-pago' utilizadas en la telefonía pública y celular constituyen un ejemplo inicial de la aplicación de estas tarjetas. Estas tarjetas tienen almacenadas cierta cantidad de dinero, la cual se va descontando conforme el consumidor va haciendo uso de la tarjeta en llamadas telefónicas. Se espera que el uso de estas tarjetas se generalice en otro tipo de transacciones, lo cual abriría una oportunidad a las empresas bancarias de brindar nuevos servicios a sus clientes.

Así por ejemplo, un caso que combina las facilidades del dinero electrónico y las tarjetas inteligentes lo constituye el sistema de pagos electrónicos Mondex desarrollado por el National Westminister Bank en el Reino Unido. Este sistema implementa un mecanismo de transferencia de tarjeta a tarjeta. Por ejemplo, una transacción comprador-vendedor procedería de la siguiente manera: El vendedor instala una lectora de tarjetas compatible con Mondex, en la cual coloca su tarjeta Mondex. El comprador pasa su tarjeta Mondex por la lectora y transfiere el valor del dinero en efectivo de su tarjeta a la tarjeta del vendedor. La lectora registra dicha transacción, de tal manera que puede servir para los procesos de cierre y de conciliación de las cuentas. De otro lado, el banco emisor de las tarjetas puede transferir valor de dinero en efectivo a la tarjeta cuando ésta sea recargada, e igualmente transferir valor de dinero en efectivo de la tarjeta del vendedor a su correspondiente cuenta bancaria.

Otro caso es el lanzamiento de las tarjetas VISA Cash que permiten guardar un determinado valor de dinero en efectivo. Cada vez que se utiliza esta tarjeta para abonar una compra, el total de la compra se deduce automáticamente del saldo almacenado en la tarjeta. Estas tarjetas pueden ser recargadas en terminales situados en sucursales bancarias o en cajeros automáticos. Actualmente estas tarjetas se encuentran disponibles en países como Argentina, Australia, Brasil, Canadá, Colombia, España, Estados Unidos, Inglaterra y Japón.

CAPITULO IV

LOS RIESGOS EN LOS SISTEMAS DE INFORMACION

4.1. Introducción

En el capítulo anterior se describieron las principales aplicaciones de la tecnología de información en las empresas bancarias. Como se ha podido apreciar el uso de la tecnología de información se ha extendido hacia todos los niveles de la organización bancaria, desde la automatización de las operaciones, hasta el soporte a las decisiones tácticas y estratégicas del negocio, así como el uso de canales de distribución electrónicos de los servicios bancarios. Sin embargo, conforme las empresas bancarias adquieren un mayor grado de dependencia hacia el uso de la tecnología de información se encuentran expuestas en mayor medida a los riesgos derivados de posibles fallas en su planeamiento, desarrollo, adquisición, operación, mantenimiento o control. Estas fallas pueden traducirse en una degradación de los tiempos de procesamiento, errores de integridad en la información procesada, fraudes informáticos, entre otros, que finalmente pueden representar pérdidas importantes para la empresa bancaria. En este capítulo describiremos la naturaleza de estos riesgos, y para ello utilizaremos el concepto de sistema de información y las técnicas del análisis de riesgos.

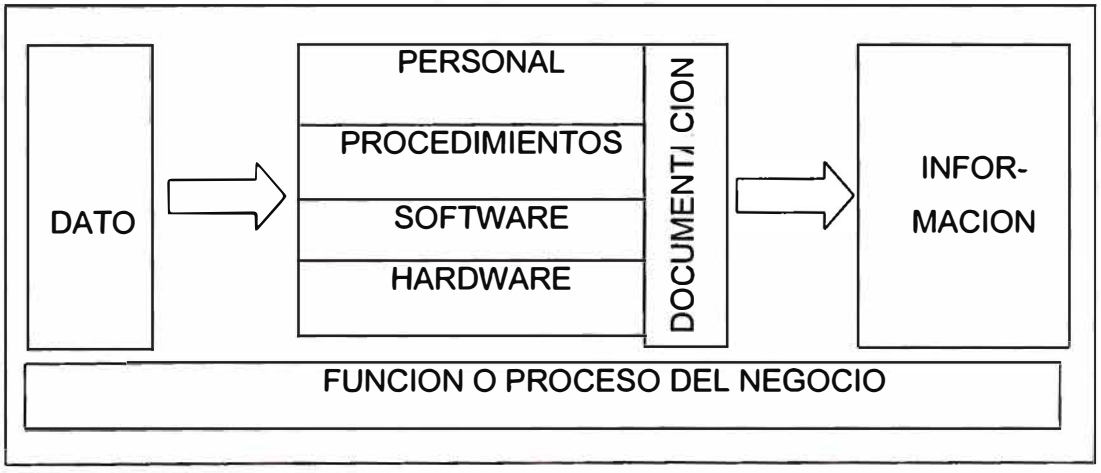
4.2. Los sistemas de información

Un sistema de información está formado por aquellos elementos interrelacionados entre sí, cuyo objetivo es el procesamiento automatizado de la información, como

soporte a alguna función o proceso del sistema organizacional del cual forma parte. En general, un sistema de información estará compuesto por cinco elementos:

a) *Hardware.*- Componente físico del sistema. Está constituido por los equipos de cómputo, equipos de comunicaciones, dispositivos de almacenamiento, entre otros.
b) *Software.*- Componente lógico del sistema. Está constituido por las aplicaciones o programas que implementan los procedimientos y procesos del negocio. Asimismo por los sistemas operativos y utilitarios que permiten administrar eficientemente el hardware.
c) *Procedimientos.*- Los procesos de negocio se implementan a través de sub-procesos y de procedimientos detallados. Estos últimos son codificados en las aplicaciones y programas que forman parte del software.
d) *Personal.*- Constituido por los usuarios responsables tanto de la operación de los sistemas, como de la explotación de la información generada por ellos.
e) *Documentación.*- Constituido por todos aquellos registros documentarios que permiten un adecuado mantenimiento y operación de los sistemas, como por ejemplo: Manual de Usuario, Manual Técnico del Sistema, etc.

Un sistema de información normalmente recibirá datos de entrada, los procesará de acuerdo a los procedimientos definidos y codificados en el software y generará como resultado información a ser utilizada por los usuarios. El esquema siguiente muestra los componentes de un sistema de información:



Las diversas aplicaciones de la tecnología de información, descritas en el capítulo anterior, no se encuentran presentes en las empresas bancarias de manera aislada, sino que forman parte de la arquitectura de sistemas de información de la empresa. De esta manera:

a. *La automatización de las operaciones bancarias* se realiza a través de sistemas de información denominados operacionales o transaccionales, dado que están orientados al procesamiento de las transacciones diarias de la empresa, tanto en tiempo real (en línea) como en lotes (procesos batch).

b. *El soporte a la toma de decisiones* se realiza a través de sistemas de información denominados Sistemas de Soporte a las Decisiones (SSD), que incluyen a los Sistemas de Información Gerencial (SIG).

c. *Las operaciones en Banca Electrónica, el uso de Internet y el comercio electrónico* se realizan a través de sistemas operacionales especializados para procesar las transacciones realizadas a través de los canales de distribución electrónicos.

Considerando lo anterior, y siguiendo una perspectiva sistémica, el análisis de los riesgos asociados al uso de la tecnología de información no debe ser realizado sobre los componentes informáticos de manera aislada, sino que debe orientarse hacia los sistemas de información implementados en la empresa.

4.3. Naturaleza del riesgo en los sistemas de información

Como se vio en el Capítulo I, el riesgo puede ser definido como el potencial que eventos, ya sea esperados o no anticipados, puedan ocasionar un impacto adverso en las utilidades o el patrimonio de la empresa. En particular, el riesgo en los sistemas de información se define como la probabilidad de sufrir pérdidas en el

patrimonio de la empresa o disminución en sus utilidades, como consecuencia del funcionamiento inapropiado de sus sistemas de información.

En tal sentido, se han identificado diez áreas de riesgo que aparecen durante el ciclo de vida de los sistemas de información, y que pueden determinar un funcionamiento inapropiado de dichos sistemas, en caso no se tomen las medidas adecuadas para administrar dichos riesgos. Estas áreas de riesgo han sido agrupadas en cuatro dominios, de la siguiente manera:

Dominio I : Planeamiento y Organización
Areas de Riesgo

a. Planeamiento estratégico de sistemas de información
b. Organización del departamento de sistemas de información

Dominio II : Adquisición, Desarrollo y Mantenimiento
Areas de Riesgo

a. Adquisición e implementación de sistemas de información
b. Desarrollo y mantenimiento de sistemas de información
c. Implementación de un sistema de información integral

Dominio III: Operaciones
Areas de Riesgo

a. Seguridad de información
b. Continuidad operacional
c. Banca electrónica y el uso de Internet

Dominio IV: Monitoreo y control interno
Areas de Riesgo

a. Control de Gerencia
b. Revisiones de Auditoría Interna y Externa

En las siguientes secciones se describirán en detalle cada una de las áreas de riesgo identificadas, agrupadas en los cuatro dominios señalados.

4.4. Riesgos en el planeamiento y la organización

4.4.1. Planeamiento estratégico de sistemas de información

El planeamiento estratégico empresarial es un proceso dirigido hacia la definición de los objetivos y metas de la organización, su visión y misión, así como la estrategia adecuada para alcanzar dichos objetivos y metas organizacionales, en un horizonte de tiempo determinado. Dado que los sistemas de información constituyen un componente importante para el normal desarrollo de las operaciones de una institución financiera, es necesario que los planes de desarrollo de los sistemas de información se encuentren alineados al plan estratégico de la empresa.

Un proceso efectivo de planeamiento estratégico de sistemas de información se encuentra integrado en el proceso de planeamiento estratégico empresarial y se dirige hacia el desarrollo de sistemas de información que permitan alcanzar los objetivos y metas de la organización en un horizonte de mediano y largo plazo. Esto incluye además un análisis de las oportunidades que brindan los desarrollos recientes en tecnología de información, a fin de lograr mejoras en la eficiencia y efectividad de las operaciones bancarias, así como nuevas maneras de llegar a los clientes.

En caso una empresa bancaria no cuente con un proceso efectivo para el planeamiento estratégico de sus sistemas de información, esto puede significar que los sistemas de información desarrollados no soporten el logro de los objetivos y metas de la organización, así como la pérdida de oportunidades de negocio brindadas por los desarrollos recientes en tecnología de información.

4.4.2. Organización del departamento de sistemas de información

El departamento de sistemas de información de una institución financiera, debe ser organizado de acuerdo a la naturaleza de los objetivos y metas de la empresa, así como al diseño organizacional de la institución en su conjunto. Esta organización puede seguir un esquema de dispersión, centralización o descentralización de recursos, o finalmente a través de un "outsourcing", o contrato de servicios de un proveedor externo.

En general, es conveniente que el jefe del departamento (Gerente de Sistemas) reporte directamente a la Alta Gerencia de la empresa. Asimismo, es recomendable la existencia de un Comité Ejecutivo de Sistemas (u otro órgano similar), formado por los gerentes de las áreas usuarias y de sistemas, encargado de establecer las coordinaciones necesarias entre las áreas y determinar las prioridades en los requerimientos para el desarrollo y mantenimiento de los sistemas de información de la empresa.

El Directorio debe ser responsable de aprobar los planes y políticas del departamento de sistemas, así como los gastos importantes relacionados a la infraestructura tecnológica de la empresa. Asimismo debe ser responsable de realizar el seguimiento correspondiente al desarrollo y cumplimiento del Plan Anual de Sistemas.

Los roles y responsabilidades del personal del departamento deben ser adecuadamente documentados y difundidos (p.ej. a través de un Manual de Organización y Funciones), de tal manera que la comunicación al interior del departamento sea más fluida, y la asignación de tareas sea más eficiente.

Asimismo, la organización debe considerar una adecuada separación de funciones en ciertas áreas clave del departamento, como: desarrollo, aseguramiento de calidad, implementación, operaciones y seguridad de información. En particular,

deben asignarse recursos adecuados para las funciones de aseguramiento de calidad y de seguridad de información.

En caso la institución financiera mantenga una inadecuada organización del departamento de sistemas de información, pueden originarse las siguientes consecuencias:

a. Ineficiente desempeño de las funciones del departamento de sistemas de información.
b. Conflictos internos permanentes entre el departamento de sistemas y las áreas usuarias.
c. Redundancias en el desarrollo de sistemas, generando costos innecesarios.

4.5. Riesgos en la adquisición, desarrollo y mantenimiento

4.5.1. Adquisición e implementación de sistemas de información

Cada año las empresas bancarias gastan importantes cantidades de dinero en la adquisición de equipos de cómputo, servicios de desarrollo de sistemas de información a medida, software de aplicación, telecomunicaciones, entre otros rubros relacionados a la tecnología de información. El éxito o fracaso en estas adquisiciones influye directamente sobre los tiempos de respuesta en el procesamiento informático de las transacciones bancarias y finalmente en la calidad de servicio que se ofrece a los clientes.

La Oficina General de Contabilidad de Estados Unidos (*United States General Accounting Office*) propone un modelo basado en 3 fases y 14 actividades generales para la adquisición de sistemas de información, las cuales se mencionan a continuación:

FASE	***ACTIVIDAD EN CADA FASE***
I. Pre - solicitud	1.1. Inicio del Proyecto 1.2. Análisis de Requerimientos 1.3. Identificar alternativas 1.4. Preparar plan de adquisición 1.5. Preparar especificaciones
II. Solicitud y Adjudicación	2.1. Mantener la estructura del proyecto 2.2. Preparar solicitud 2.3. Publicar solicitud 2.4. Evaluar propuestas 2.5. Negociar con proveedores 2.6. Seleccionar al proveedor
III. Post - Adjudicación	3.1. Establecer la administración del contrato 3.2.Monitorear el rendimiento y desempeño en la ejecución del contrato 3.3. Probar y aceptar el sistema

Fuente: GAO - Information Technology: An Audit Guide for Assessing Acquisition Risks (Diciembre 1992)

Un adecuado proceso de adquisición de sistemas de información cuenta con las siguientes características:

- Apoyo de la Alta Gerencia.
- Involucramiento y apoyo de los usuarios durante todo el proceso, a fin de asegurar que sus requerimientos han sido correctamente entendidos y que el sistema resultante sea aceptado y usado.
- Designación de un gerente de proyecto y un equipo de trabajo para el proyecto de adquisición con suficiente autoridad, experiencia y habilidad para manejar exitosamente el proyecto.
- La adquisición debe satisfacer claramente los requerimientos de la empresa y ajustarse a sus políticas y estándares.

- Establecimiento de una administración del contrato que asegure que la empresa reciba los productos y servicios dentro de los plazos y costos previamente establecidos.
- Establecimiento de planes de pruebas y criterios de aceptación de los sistemas adquiridos.

Un inadecuado proceso de adquisición de sistemas de información (o de alguno de sus elementos) tiene como consecuencias: la insatisfacción de las necesidades de los usuarios, excesos sobre los costos y tiempos inicialmente estimados, incompatibilidades entre los sistemas adquiridos y la arquitectura de sistemas de información de la empresa, selección de alternativas innecesariamente complejas o costosas, entre otras.

4.5.2 Desarrollo y mantenimiento de sistemas de información

Los proyectos de desarrollo de sistemas de información se encuentran expuestos a un conjunto de riesgos cuya ocurrencia puede determinar que el resultado de dichos proyectos sea excesivamente costoso, entregado fuera del plazo inicialmente establecido, o inaceptable para el usuario final.

Siguiendo el modelo propuesto por el *Software Engineering Institute* de Estados Unidos, los riesgos en los proyectos de desarrollo de software pueden existir en las siguientes áreas:

A. Ingeniería del producto	**B. Entorno de desarrollo**	**C. Restricciones**
1. Requerimientos	1. Proceso de desarrollo	1. Recursos
2. Diseño	2. Sistema de desarrollo	2. Contratos
3. Codificación y pruebas unitarias	3. Proceso administrativo	3. Interfases

4. Integración y Pruebas	4. Métodos de gerencia	
5. Especialidades de Ingeniería	5. Entorno de trabajo	

Fuente: Software Engineering Institute - Software Risk Evaluation Method version 1.0 (Diciembre 1994)

El área de *Ingeniería del Producto* se refiere a aquellas actividades de ingeniería de software realizadas con la finalidad de crear un sistema de información que satisfaga los requerimientos especificados y también las expectativas del cliente. Estas actividades incluyen el análisis y especificación de requerimientos, diseño y codificación del software, integración de los componentes de hardware y software, y las pruebas unitarias y de integración del sistema de información. Estas actividades se refieren a factores técnicos asociados con el producto entregable en sí mismo, independiente de los procesos o herramientas utilizadas para producirlo, o las restricciones impuestas por recursos finitos o factores externos no controlables por el proyecto.

Los riesgos en esta área generalmente están asociados con requerimientos técnicamente difíciles o imposibles de implementar, en combinación con dificultades para negociar dichos requerimientos o revisar los presupuestos o cronogramas inicialmente aprobados. Asimismo, están asociados con inadecuados análisis de requerimientos o especificaciones de diseño, o especificaciones de código de baja calidad.

El área de *Entorno de Desarrollo* se refiere al entorno del proyecto y el proceso utilizado para el desarrollo del sistema de información. Los riesgos en esta área están asociados principalmente al uso de herramientas de hardware y software inadecuados para el desarrollo del sistema de información, así como una inadecuada administración del proyecto en términos de planeamiento, organización, gestión del personal asignado al proyecto, directivas de monitoreo y control, aseguramiento de calidad, entre otros aspectos. Asimismo, está relacionado con las características del entorno de trabajo en el que se desarrolla el proyecto, lo cual

incluye la cultura de calidad, la comunicación, la cooperación y la moral existente en dicho entorno.

El área de *Restricciones* incluye principalmente factores externos al proyecto, pero que pueden afectar su desarrollo. Así por ejemplo, en lo relativo a recursos, se refiere a la estabilidad del cronograma inicialmente aprobado o de la asignación inicial de presupuesto o de personal, frente a eventos internos o externos que afecten a la empresa. Asimismo, se refiere a factores como el soporte de la Alta Gerencia, contratos con proveedores externos, nivel de comunicación con los usuarios finales, entre otros aspectos.

Documentación de los sistemas de información

Un aspecto adicional que debe resaltarse consiste en la documentación de los sistemas de información. La documentación consiste en un registro de los

procedimientos necesarios para operar el sistema, y constituye la fuente básica de información para todas aquellas personas que auditan, corrigen, mejoran, administran, operan o usan el sistema. El valor de la documentación se deriva de su exactitud y amplitud. Los sistemas adecuadamente documentados son más sencillos de mantener, y además permite la continuidad de operaciones en caso de rotación de personal clave.

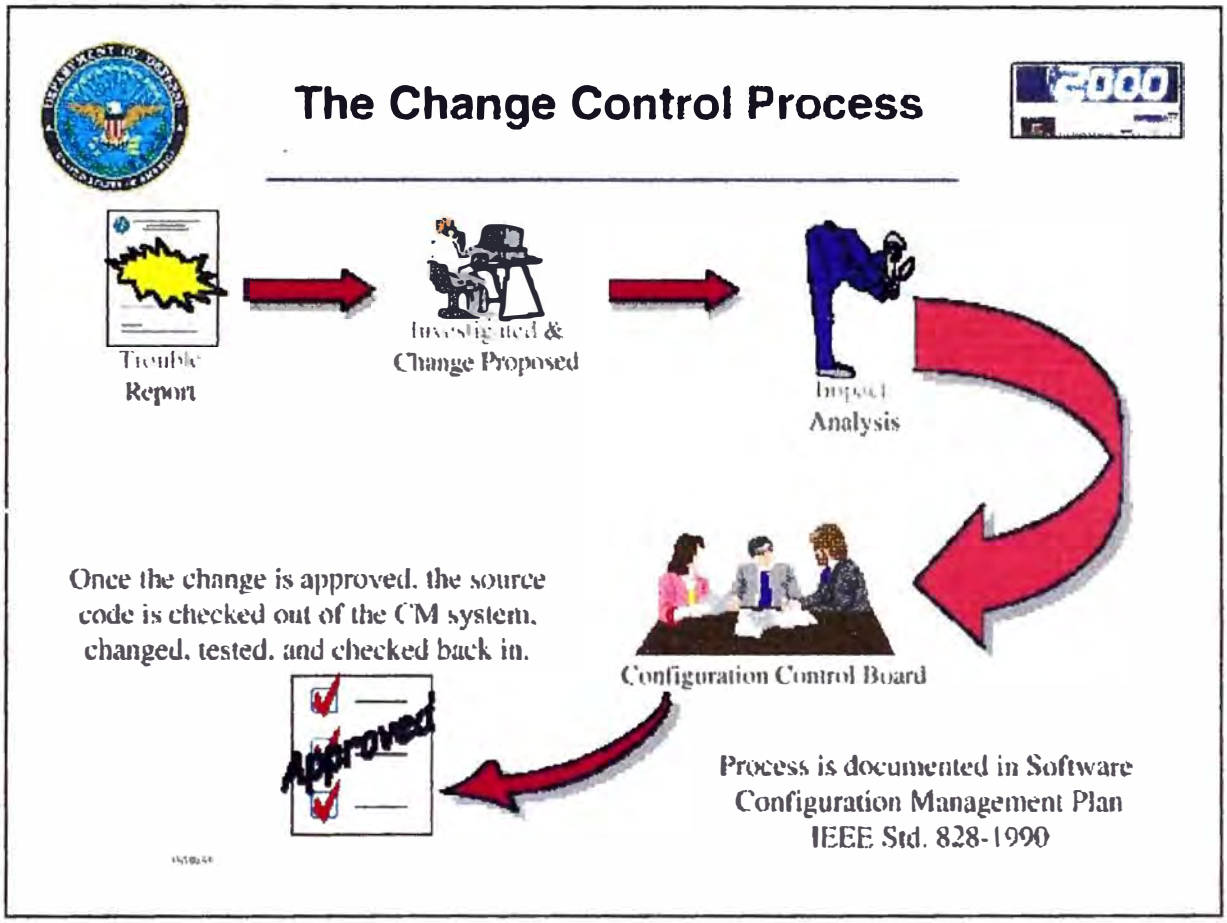
Control de cambios

Durante el ciclo de vida de los sistemas de información será necesario efectuar algunos cambios a los programas desarrollados inicialmente. Estos cambios pueden estar asociados a requerimientos de mejora en la funcionalidad del sistema, variaciones en las operaciones y procedimientos internos de la empresa, o a exigencias derivadas de normas emitidas por los organismos regulatorios, entre otras razones. La empresa debe establecer un procedimiento documentado para el control de cambios que establezca los canales formales para la aprobación de los requerimientos de cambios, y que permita llevar un control estricto de las modificaciones realizadas en los sistemas de información de la empresa.

El control de cambios está directamente relacionado con la administración de configuraciones (*configuration management: CM*) que permite controlar las diferentes versiones de un software simultáneamente y reproducir una versión requerida en particular en un instante. Para ello, existen diversas herramientas que permiten realizar esta tarea de manera automatizada.

La inexistencia de adecuados procedimientos de control de cambios puede originar modificaciones no autorizadas o fraudulentas en los sistemas de información, o la pérdida de funcionalidades alcanzadas al no poder restaurar las versiones anteriores del software desarrollado.

En la gráfica siguiente se muestra el proceso de control de cambios (*Change Control Process*) propuesto por el Departamento de Defensa de los Estados Unidos.



4.5.3. Implementación de un sistema de información integral

Emprender la implementación de un sistema de información integral que abarque todos los procesos críticos de una empresa bancaria, constituye un proyecto de gran envergadura que puede tomar desde varios meses, hasta algunos años. Estos proyectos son similares a aquellos emprendidos por empresas industriales, comerciales y de servicios con el fin de implementar sistemas ERPs (enterprise

resource planning), los cuales les permiten administrar los procesos productivos y administrativos de la empresa a través de un sistema de información integrado.

Las ventajas de contar con un sistema de información integral, ha determinado que varias empresas bancarias hayan decidido iniciar este tipo de proyectos, a través de la adquisición de sistemas de información integrales elaborados por importantes proveedores de software. En tal sentido, las principales ventajas de contar con un sistema de información integral para una empresa bancaria son las siguientes:

a. Incrementa la eficiencia y reduce costos a través de la incorporación de las 'mejores prácticas' en los procesos de negocio de la empresa, las cuales se encuentran incorporadas en el sistema de información.
b. Elimina la redundancia en los archivos de datos.
c. Proporciona herramientas para mejorar la administración de los productos y las relaciones con los clientes.
d. Mejora la distribución oportuna de información a través de la institución.
e. Permite mejorar la calidad de la información brindada a la Alta Gerencia.

Sin embargo, la implementación de un sistema de información integral (o un sistema ERP) representa cambios en los procesos y procedimientos de la organización, lo cual genera, en la mayoría de los casos, resistencia al cambio por parte del personal involucrado. Asimismo, debe evaluarse adecuadamente al proveedor del sistema de información con el fin de asegurar que pueda brindar el soporte técnico necesario durante la ejecución del proyecto.

Este tipo de proyectos requiere una adecuada administración del cambio en los procedimientos y en la cultura de la organización, así como el liderazgo y compromiso de la Alta Gerencia y la construcción de una visión compartida con el personal involucrado en el cambio, con el fin de asegurar la culminación exitosa del proyecto.

4.6. Riesgos en las operaciones

4.6.1. Seguridad de información

Uno de los activos más importantes de una organización es la información. Por tal motivo, proteger o asegurar la información y los dispositivos que la procesan y mantienen es vital para un adecuado desempeño de las operaciones bancarias. Las deficiencias en seguridad de la información pueden traer como consecuencia: negocios perdidos, reputaciones dañadas, pérdidas financieras, activos perdidos, y posiblemente secretos comerciales perdidos.

Es necesario establecer controles de seguridad para salvaguardar la información de alguna modificación, destrucción o revelación no autorizadas o accidentales, y para asegurar la puntualidad, disponibilidad y uso de dicha información. Las posibles amenazas a la seguridad de la información incluyen la ignorancia y negligencia de los operadores y usuarios, daños por fuego o agua, empleados con actitudes no éticas, agentes externos, hackers, y virus.

La organización requiere desarrollar un plan y definir procedimientos de seguridad para minimizar la exposición a todas las amenazas y riesgos descritos en el párrafo anterior. Este programa debe enfatizar la necesidad de protección de activos, y el establecimiento de controles. El grado de control debe estar basado en una evaluación previa del riesgo en relación con el valor del activo.

Además del plan, la empresa debe contar con una organización establecida que asegure el cumplimiento de dicho plan.

Organización para la seguridad de información

La empresa debe asignar personal para desempeñar las funciones asociadas con la seguridad de la información. Estas funciones incluyen la definición del plan de seguridad, así como el monitoreo de la ejecución de dicho plan. El personal asignado no debería estar involucrado en funciones operativas en el centro de cómputo, programación, o conciliación de datos de salida.

El plan de seguridad de información debe ser desarrollado con la aprobación y el compromiso de la Alta Gerencia y debe incluir aspectos de seguridad física y de datos, que alcancen a todos los sistemas de información implementados en la empresa.

Seguridad Física

La seguridad física se refiere a las medidas de protección que deben ser tomadas para prevenir y detectar las posibles pérdidas de información causadas por daños o usos no autorizados en los equipos de cómputo y otros dispositivos de procesamiento de datos.

Un plan de seguridad física debe ser diseñado para obtener máxima protección a un costo razonable. Para ello debe realizarse un análisis de riesgo que incluya los siguientes aspectos:

a. Determinar qué activos necesitan tener seguridad (información, equipos, personal, servicios de red, aplicaciones, etc.)
b. Determinar las fuentes de riesgo: ambiente (fuego, inundaciones, explosiones, etc.) o personas (hackers, empleados con actitudes antiéticas, delincuencia, vandalismo, etc.)
c. Determinar la probabilidad de ocurrencia de dichos riesgos
d. Determinar los costos asociados a dicha ocurrencia.

e. Evaluar las alternativas disponibles para minimizar la exposición a dichos riesgos. Así por ejemplo, frente a las amenazas originadas por personas, pueden establecerse medidas de restricción de acceso para los centros de cómputo a través de personal de seguridad, equipos de vigilancia, seguridad en puertas y ventanas, entre otras.

El plan de seguridad física debe incluir medidas de prevención y detección en las siguientes áreas:

a. Centros de cómputo
b. Computadores personales y redes de área local distribuidos en diferentes áreas de la empresa.
c. Dispositivos y medios de almacenamiento

Seguridad de datos

Así como los equipos de cómputo deben ser protegidos, el acceso al software y los datos también debe ser restringido. El software y los datos son activos valiosos, y pueden producirse pérdidas financieras, si éstos son perdidos, robados o comprometidos. Los controles en seguridad de datos permiten proteger los datos, el software o cualquier información que es transmitida o almacenada, de posibles modificaciones, destrucciones o revelaciones no autorizadas, ya sean éstas accidentales o intencionales.

A fin de asegurar que los datos se encuentran seguros y que las operaciones permanecerán ininterrumpidas, deben considerarse los siguientes elementos en un esquema de seguridad de datos que incluya todas las plataformas computacionales de la empresa (computadores centrales, redes de área local y computadores personales):

a. Controles de acceso lógico
b. Integridad de datos

c. Separación de funciones
d. Seguridad en Telecomunicaciones
e. Virus informáticos

Controles de acceso lógico.- Evita que usuarios no autorizados se conecten u obtengan acceso a aplicaciones o recursos de los sistemas antes y después de haber logrado una conexión física a los computadores personales, redes de área local o equipos de cómputo central. Esto incluye tanto el control de acceso a las aplicaciones a través de identificaciones, autorizaciones y contraseñas de los usuarios, como el control de acceso al software base o software de sistema.

Integridad de datos.- Consisten en controles de ingreso y de procesamiento que incluyen verificaciones de valor, rango, consistencia y razonabilidad de los datos, con el fin de asegurar su integridad. Estos mecanismos de control permiten asegurar que solamente sean ingresados datos válidos al sistema y notifican al usuario y al personal correspondiente cuando se ingresan datos erróneos. En entornos distribuidos, la integridad de datos se encuentra expuesta a mayores riesgos, dado que existen más oportunidades de transformar los datos a medida que éstos son trasladados a través de los sistemas. En particular, la integridad de la información generada por los sistemas de información, que será utilizada por los gerentes, el Directorio y los organismos supervisores, debe recibir un nivel suficiente de revisión. Si la integridad de la información no se encuentra auditada, es posible generar reportes con datos incompletos, inexactos o erróneos, lo cual trae como consecuencia que la toma de decisiones resultante a partir de la información generada por los sistemas de información de la empresa pueda llevar a la organización a seguir prácticas inadecuadas e inseguras.

Separación de funciones.- El objetivo de la separación de funciones es evitar que un individuo tenga acceso a una combinación de recursos o a recursos clave que creen un riesgo potencial a los activos de la empresa, ya sea por error o fraude (error intencional). Si las funciones se encuentran adecuadamente separadas, el

fraude solamente puede ser cometido a través de la colusión. Algunos ejemplos de separación de funciones son los siguientes:

a. El responsable de revisar la exactitud de las transacciones de entrada debe ser una persona que no haya estado involucrada en su preparación.
b. El responsable de revisar y aprobar los ajustes y correcciones a los registros maestros debe ser una persona diferente a aquella que aprueba las transacciones de rutina.
c. El personal de procesamiento informático debe estar prohibido de iniciar o autorizar cualquier cambio a las aplicaciones, software del sistema, registros maestros u otro tipo de información almacenada en los sistemas de la empresa, con excepción de aquellos requeridos para efectuar una recuperación en caso de fallas de procesamiento.

En general, es recomendable separar las funciones operativas y las funciones de control, de tal manera que las tareas que realiza una persona sean verificadas por otra, de manera independiente.

Seguridad en Telecomunicaciones.- Se refiere al acceso que se obtiene al sistema de información de la empresa, a partir de una locación remota o desde un punto no conectado directamente a la red, utilizando satélite, microondas de radio o líneas telefónicas. El acceso no autorizado a través de las redes de comunicación a los sistemas de cómputo central, minicomputadores o redes de área local de una empresa bancaria es una seria amenaza para la seguridad de sus sistemas de información. Es necesario establecer mecanismos de control que permitan entre otros aspectos: identificar y autenticar a los usuarios remotos, y definir los niveles autorizados de acceso y de uso de recursos, según el tipo de usuario.

Asimismo, deben establecerse medidas de control que permitan proteger la confidencialidad y exactitud de los datos transmitidos a través de las redes de comunicación. La confiabilidad de los datos transmitidos puede ser mejorada

utilizando técnicas de verificación de paridad, autenticación de mensajes y encriptación de datos.

Virus informáticos.- Los virus informáticos constituyen otra amenaza a la seguridad de los sistemas de información de la empresa, especialmente aquellos virus destructivos que pueden eliminar total o parcialmente la información almacenada en los discos duros de los computadores personales de la empresa. Las políticas de seguridad de la empresa deben incluir prohibiciones del uso de software proveniente de fuentes no confiables, así como del uso de software personal en los computadores personales de la empresa. Asimismo, deben implementarse controles detectivos con el fin de detectar la presencia de un virus, lo cual puede realizarse mediante la adquisición y uso de software antivirus.

En relación a la seguridad de datos y el nivel de seguridad de los sistemas de información, el Departamento de Defensa de los Estados Unidos ha editado un conjunto de guías, entre las que destaca el Libro Naranja (*Orange Book*) conocido formalmente como TCSEC (*Trusted Computer System Evaluation Criteria*). En esta Guía, ampliamente usada en las agencias gubernamentales de los Estados Unidos, se definen cuatro clases de seguridad:

Clase D - Seguridad mínima
Clase C - Protección discrecional (incluye niveles C1 y C2)
Clase B - Protección mandatoria (incluye niveles B1, B2 y B3)
Clase A - Protección verificatoria

Muchos de los contratos de las agencias gubernamentales de los Estados Unidos consideran en sus políticas de adquisición de sistemas de información un nivel de seguridad mínimo equivalente a C2, el cual establece diversos requerimientos de seguridad como por ejemplo:

- Un individuo dueño de un recurso o archivo debe tener la capacidad de controlar el acceso a ese recurso.
- El sistema operativo debe ser capaz de evitar que los recursos sean reusados aleatoriamente por otros procesos.
- Los usuarios deben ingresar una única identificación y contraseña antes de acceder al sistema. Adicionalmente, el sistema debe ser capaz de usar esta información para rastrear las actividades del usuario.
- Los usuarios administrativos deben tener acceso a los datos de auditoría, que le permita auditar los eventos relacionados con la seguridad de información.
- El sistema debe ser capaz de protegerse de modificaciones no autorizadas y otros tipos de interferencias.

El nivel C2 es alcanzado por sistemas operativos como Microsoft WindowsNT, Novell Intranetware e IBM OS/400.

4.6.2 Continuidad operacional

El objetivo de asegurar un *servicio continuo* de los sistemas de información de la empresa, es soportado mediante un proceso estructurado de planeamiento de contingencias. El plan de contingencias de la empresa debe estar dirigido hacia los procesos críticos del negocio con el objetivo de minimizar interrupciones de servicio al interior de la empresa, así como en la relación con los clientes, minimizando de esta manera posibles pérdidas financieras, y asegurando un tiempo razonable para la reanudación de las operaciones en el caso de un desastre. Los desastres pueden ser tanto físicos (incendios, inundaciones, etc.), como ambientales (fallas de energía o de telecomunicaciones) o de otro tipo (asaltos o acceso restringido a las instalaciones del centro de cómputo principal).

Una adecuado planeamiento de contingencias debería considerar, entre otros aspectos:

a. Análisis de las posibles amenazas a la continuidad operacional de la empresa: desastres naturales (incendios, inundaciones, sismos), fallas técnicas (fallas de hardware/software, interrupción de energía, interferencia en las comunicaciones, etc.) o acciones humanas (huelgas, sabotaje).
b. Evaluación del impacto de la pérdida de información y de servicios de fuentes internas y externas en: la condición financiera de la empresa, su posición competitiva, la confianza del cliente, etc.
c. Evaluación de las necesidades críticas: Procesos críticos que no pueden ser interrumpidos, personal clave, información crítica, registros vitales, etc.
d. Definición de las prioridades para la recuperación de operaciones, basada en la evaluación de las necesidades críticas.
e. Definición de las estrategias de recuperación para cada amenaza analizada.
f. Organización y documentación de un plan escrito que incluya todos los puntos anteriores, en el cual se describan de manera detallada los procedimientos de recuperación y los responsables de su activación y ejecución.
g. Definir criterios para la prueba y mantenimiento del plan.
h. Definir procedimientos para el entrenamiento del personal involucrado en la ejecución del plan.
i. Aprobación del plan por la Alta Gerencia.
j. Guardar una copia del Plan fuera del local principal, junto con otras provisiones de reserva.

Asimismo, las políticas y procedimientos de respaldo son importantes para asegurar la continuidad de las operaciones, y deben incluir consideraciones a nivel de hardware, software de sistema, archivos de datos, aplicaciones y redes de comunicación.

La habilidad para reanudar las operaciones de una manera eficiente y efectiva en caso de una contingencia, reduce el riesgo de pérdidas financieras para la organización y minimiza el nivel de interrupción en el servicio al cliente.

4.6.3 Banca electrónica y el uso de Internet

En general, el fraude, el asalto y el mal funcionamiento constituyen los principales riesgos en un entorno de cajeros automáticos, y en redes de puntos de venta. A pesar que el uso de tarjetas de plástico y de las claves secretas asociadas actúan como una barrera inicial, existe el riesgo que un individuo no autorizado (incluyendo personal de la empresa) pueda obtenerlas y hacer uso indebido de ellas.

Asimismo, existe un riesgo de imagen en caso los sistemas de banca electrónica no funcionen adecuadamente, causando una reacción negativa por parte de los clientes. Este riesgo también puede aparecer en caso los clientes experimenten problemas con alguno de los servicios proporcionados, y no se les proporcione adecuada información acerca del uso del producto y los procedimientos para resolver problemas.

De otro lado, existen riesgos en las transferencias electrónicas de fondos realizadas a través de los cajeros automáticos, redes de puntos de venta, tarjetas de débito, tarjetas inteligentes o la red mundial Internet. El riesgo en estas transferencias es bajo en la medida que las transacciones individuales generalmente involucran montos bajos de dinero. Sin embargo, la existencia de debilidades en los controles que puedan llevar a un uso incorrecto o impropio de muchas cuentas, puede originar pérdidas significativas para una institución financiera.

Banca por Internet

La red mundial Internet, es insegura básicamente porque los mensajes enviados a través de ella son ruteados a través de muchos computadores, en diferentes partes del mundo, antes que finalmente alcancen a sus respectivos destinatarios. Existe entonces la posibilidad que el mensaje pueda ser interceptado en algún lugar a lo largo de la transmisión. Incluso aquellas computadoras que no se encuentran

directamente involucradas en la transmisión del mensaje pueden interceptarlo. El envío de datos a través de Internet está expuesto a tres grandes riesgos:

a. Personas no autorizadas puedan acceder a información privada transmitida a través de Internet.
b. Personas no autorizadas puedan modificar la información trasmitida en una comunicación privada a través de Internet.
c. Una persona puede enviar o recibir información de la empresa utilizando una identificación falsa.

Considerando la existencia de estos riesgos asociados a la transmisión de datos por Internet, es importante que los bancos se aseguren que los mensajes enviados desde sus clientes sean autenticados y asimismo que los mensajes enviados hacia sus clientes no sean interceptados y dirigidos hacia otras computadoras. Para lograr esto se requieren implementar determinados niveles de seguridad al diseñar una solución tecnológica para ofrecer servicios bancarios a través de la Red, entre los cuales deben considerarse:

A. Seguridad de la información del cliente enviada a través de Internet, para lo cual se utilizan técnicas de encriptación de datos.
B. Seguridad en el entorno del servidor de transacciones en Internet y del servidor de base de datos donde reside la información de los clientes.
C. Prevención de accesos no autorizados al servidor de transacciones en Internet, mediante el uso de firewalls y pasarelas (gateways).

La *encriptación de datos* consiste en la transformación de un archivo de datos, a través del uso de un algoritmo especial, en un conjunto ilegible de letras y caracteres. La encriptación está basada en una contraseña o clave, sin la cual el archivo encriptado es completamente ilegible. La encriptación no sólo mantiene la información privada sino que además proporciona un mecanismo de autenticación, mediante el cual el receptor de un mensaje puede estar seguro de la identidad del

emisor y de la integridad del mensaje. Los protocolos de autenticación están basados ya sea en claves privadas (como DES) o en claves públicas (como RSA). Los sistemas de claves públicas utilizan firmas digitales para la autenticación.

4.7. Riesgos en el monitoreo y control interno

4.7.1. Control y monitoreo de Gerencia

La gerencia debe definir indicadores de rendimiento y asegurarse de recoger datos para la elaboración de reportes de gerencia acerca del desempeño de las diferentes funciones del departamento de sistemas de información, de tal manera que puedan identificarse posibles desviaciones con respecto a los niveles esperados de desempeño, y puedan tomarse las acciones correctivas necesarias en el momento oportuno.

4.7.2. Revisiones de Auditoría Interna y Externa

Para cada uno de los riesgos mencionados en las secciones anteriores, deben diseñarse e implementarse **actividades de control** que permitan administrar adecuadamente dichos riesgos. La función de las revisiones de auditoría interna relacionadas al entorno de sistemas informáticas debe consistir en identificar posibles deficiencias de control existentes en dicho entorno. Una deficiencia de control se produce cuando una actividad de control no se encuentra adecuadamente diseñada, no se ejecuta apropiadamente, o no es efectiva para reducir los riesgos a un nivel aceptable. El programa de auditoría externa complementa esta función proporcionando una visión externa objetiva acerca del mismo tema.

Existen dos cualidades fundamentales que debe poseer el personal de auditoría interna para realizar sus funciones adecuadamente: Independencia y Competencia. La Unidad de Auditoría Interna debe depender directamente del Directorio o del

Comité de Auditoría, y sus funciones no deben incluir la participación en actividades que puedan comprometer su independiencia, como por ejemplo la preparación de archivos, desarrollo de procedimientos, entre otras actividades operativas. Asimismo, la competencia requerida para el personal debe encontrarse acorde con el tamaño y complejidad de las operaciones de la empresa.

La inexistencia de un adecuado control a través de las revisiones de auditoría interna y externa, puede significar que la empresa no identifique en el tiempo necesario, posibles deficiencias de control y/o problemas potencialmente serios relacionados con sus sistemas de información.

CAPITULO V

ANALISIS DE RIESGOS EN LOS SISTEMAS DE INFORMACION DE UNA EMPRESA BANCARIA

5.1. Introducción

En los capítulos anteriores se han descrito las principales aplicaciones de la tecnología de información en el negocio bancario, así como los riesgos asociados al uso cada vez más extendido de esta tecnología. En base a estos aspectos, y tomando como referencia fuentes metodológicas internacionales (descritas en detalle en el capítulo VI), se ha elaborado una metodología de análisis de riesgos en los sistemas de información de una empresa bancaria. En el presente capítulo se describe dicha metodología, señalando las seis fases de ejecución propuestas, así como las actividades comprendidas en cada fase.

5.2. Descripción general de la metodología

Nombre:

Metodología de Análisis de Riesgos en los Sistemas de información de una Empresa Bancaria

Objetivos:

El objetivo de la metodología propuesta consiste en brindar un marco general de actividades para el análisis de riesgos en los sistemas de información de una empresa bancaria, el cual incluya por lo menos:

a. Identificación de los riesgos existentes en el planeamiento, organización, adquisición, desarrollo, mantenimiento, operación y monitoreo de los sistemas de información de una empresa bancaria.

b. Identificación y evaluación de las actividades de control implementadas por la empresa para administrar adecuadamente estos riesgos.
c. Propuesta de medidas correctivas para superar posibles deficiencias en las actividades de control implementadas por la empresa.

Dirigido a:

Gerentes de Sistemas, Auditores de Sistemas, Consultores independientes

Fases:

La metodología considera seis fases:

a. *Fase I: Inicio.* Esta fase incluye la obtención de información básica de la empresa, tanto a nivel de su estrategia de negocio, como de su infraestructura tecnológica y la arquitectura de sistemas de información empleada.
b. *Fase II: Identificación de riesgos.* Se identifican los riesgos en los sistemas de información de la empresa en base a diez áreas de riesgo agrupadas en cuatro dominios, y se evalúa su impacto en la situación particular de la empresa analizada.
c. *Fase III: Evaluación de actividades de control.* Se evalúan las actividades de control implementadas por la empresa para administrar los riesgos en los sistemas de información, considerando la adecuación y el cumplimiento de las actividades de control implementadas.
d. *Fase IV: Medidas correctivas.* Se proponen medidas correctivas para la adecuada administración de los riesgos, de acuerdo a las deficiencias de control identificadas.
e. *Fase V: Calificación.* Se califican las áreas de riesgo analizadas y se propone una calificación global de la empresa, de acuerdo a los resultados de la evaluación realizada.
f. *Fase VI: Reporte Final.* Se emite un Reporte Final de Evaluación con los resultados de la evaluación realizada.

Actividades a ser desarrolladas

FASE I : INICIO

Actividades:

1.1. Obtener y analizar información general de la empresa

1.2. Obtener y analizar información de la infraestructura tecnológica y de los sistemas de información de la empresa.

FASE II : IDENTIFICACION DE RIESGOS

Actividades:

2.1. Identificar riesgos en sistemas de información.

2.2. Evaluar los riesgos identificados, de acuerdo a la situación particular de la empresa.

FASE III: EVALUACION DE ACTIVIDADES DE CONTROL

Actividades por cada área de riesgo a ser analizada:

3.1. Obtener un entendimiento de las actividades de control implementadas

3.2. Evaluar la adecuación de las actividades de control implementadas.

3.3. Evaluar el cumplimiento consistente y continuo de las actividades de control implementadas

FASE IV: MEDIDAS CORRECTIVAS

Actividades:

4.1. Proponer medidas correctivas

FASE V : CALIFICACION

Actividades:

5.1. Proponer calificación por área de riesgo analizada

5.2. Proponer calificación global de la empresa

FASE VI : REPORTE FINAL

Actividades:

6.1. Emitir reporte final de evaluación

Cuadro de actividades de la Metodología propuesta

En las secciones siguientes se describen en detalle cada una de las actividades señaladas en el cuadro anterior.

5.3. FASE I : INICIO

Desde una perspectiva sistémica, el estudio de análisis de riesgos que se propone no debe restringirse a la evaluación de los aspectos tecnológicos, considerándolos de manera aislada, sino que debe considerar la interrelación entre los sistemas de información de la empresa, los riesgos asociados, y los principales componentes de la estrategia empresarial. En tal sentido, el analista debe obtener información general relacionada con la estrategia de negocio de la empresa, así como información relativa a su infraestructura tecnológica y su arquitectura de sistemas de información.

En el cuadro siguiente se resumen las actividades que se desarrollan durante esta fase, y la información a ser obtenida.

FASE I - INICIO

Actividad 1.1. Obtener y analizar información general de la empresa

Se deberá obtener y analizar la siguiente información:

A. *Principales líneas de negocio de la empresa (Banca empresarial, banca de consumo, banca de inversión, etc.).*
B. *Procesos críticos de negocio*
C. *Puesto en el ranking del sistema bancario por colocaciones, depósitos y patrimonio.*
D. *Número de agencias y distribución de las mismas.*
E. *Hechos de importancia ocurridos en la empresa durante los últimos 6 meses (cambios en la estrategia de negocio, desarrollo de nuevos productos*

financieros, cambios en el directorio y/o en gerencias, posibles fusiones o adquisiciones por ser realizadas, etc.)

Actividad 1.2. Obtener y analizar información de la infraestructura tecnológica de la empresa y sus sistemas de información

Se deberá obtener y analizar la siguiente información:

A. *Infraestructura tecnológica de la empresa (hardware, sistemas operativos, manejadores de bases de datos, lenguajes de programación utilizados).*
B. *Interfases críticas con entidades externas para el intercambio de información y para la transferencia electrónica de fondos.*
C. *Dispositivos de banca electrónica utilizados y arquitectura tecnológica que lo soporta.*
D. *Arquitectura de sistemas de información que soporta los procesos de negocio de la empresa.*
E. *Organización del departamento de sistemas de información de la empresa y su ubicación dentro del organigrama general de la empresa.*

El análisis de esta información, como etapa inicial del estudio, permitirá orientar adecuadamente el estudio a ser realizado, y alinearlo con los requerimientos estratégicos de la empresa.

5.4. FASE II : IDENTIFICACION DE RIESGOS

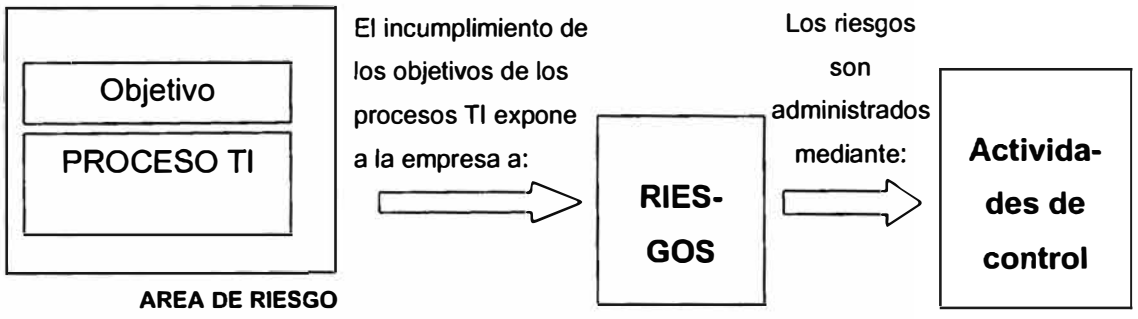
Actividad 2.1. Identificar riesgos en sistemas de información

En el capítulo anterior se describió un Modelo de Análisis, en el cual se identificaron diez áreas de riesgo en sistemas de información a las que se encuentran expuestas las empresas bancarias. Dichas áreas de riesgo fueron agrupadas en cuatro dominios, de la siguiente manera:

Dominio I: Planeamiento y Organización	**Dominio II: Adquisición, Desarrollo e Implementación**	**Dominio III: Operaciones**	**Dominio IV: Monitoreo y control interno**
• Planeamiento estratégico • Organización del dpto. de SI	• Adquisición e implementación • Desarrollo y mantenimiento • Implementación de un SI integral	• Seguridad de información • Continuidad operacional • Banca electrónica y el uso de Internet	• Control de Gerencia • Revisiones de Auditoría Interna y Externa

Cada una de estas áreas de riesgo se encuentra asociada a un proceso genérico de tecnología de información (TI). El incumplimiento de los objetivos de estos procesos expone a la organización a ciertos riesgos (riesgos informáticos o riesgos asociados a los sistemas de información). Frente a ello, deben implementarse actividades de control que permitan asegurar el cumplimiento de estos objetivos y administrar adecuadamente estos riesgos.

El esquema siguiente describe este modelo de análisis:



Actividad 2.2. Evaluar los riesgos identificados, de acuerdo a la situación particular de la empresa

Si bien las diez áreas de riesgo señaladas anteriormente se encuentran presentes en la mayoría de las empresas bancarias, su importancia e impacto puede ser muy variado entre las diferentes empresas. En tal sentido, en esta fase el analista deberá evaluar los riesgos identificados de acuerdo a la situación particular de la empresa. Como consecuencia de dicho análisis, deberá definir qué areas de riesgo serán evaluadas, de acuerdo a la naturaleza y características particulares de la empresa, así como el tiempo y los recursos que serán necesarios para llevar a cabo dicha evaluación. Asimismo debe considerar en brindar un mayor tiempo de análisis en aquellas áreas que representen un mayor riesgo para la empresa. Para ello debe considerar la información obtenida en la Fase I y los resultados de estudios anteriores (en caso éstos se hayan realizado).

5.5. FASE III: EVALUACION DE ACTIVIDADES DE CONTROL POR AREA DE RIESGO

Luego de definir las áreas de riesgos que serán incluidas en el estudio de análisis de riesgos, el analista debe evaluar las actividades de control implementadas por la empresa en cada una de las áreas de riesgo identificadas. El procedimiento general de evaluación para cada una de las áreas de riesgo analizadas, consiste en las siguientes actividades :

Actividad 3.1. Obtener un entendimiento de las actividades de control implementadas

El analista deberá obtener un entendimiento de las actividades de control implementadas por la empresa para cada una de las áreas de riesgo evaluadas.

Esto se logra a través de la revisión de la documentación relacionada al área analizada, y de entrevistas con funcionarios de la empresa.

Actividad 3.2. Evaluar la adecuación de las actividades de control implementadas

La adecuación de las actividades de control implementadas por la empresa, es evaluada siguiendo un conjunto de guías que forman parte integral de la metodología propuesta u que señalan qué aspectos deben ser revisados durante la evaluación. Estas guías se detallan en la sección 5.10 del presente capítulo, junto con formatos para el registro de los hallazgos encontrados durante la evaluación.

Actividad 3.3. Evaluar el cumplimiento consistente y continuo de las actividades de control implementadas.

El analista deberá obtener sustentos (documentación física o electrónica) que demuestren el cumplimiento consistente y continuo de las actividades de control implementadas por la empresa.

5.6. FASE IV : MEDIDAS CORRECTIVAS

Actividad 4.1. Proponer medidas correctivas

Como consecuencia de la evaluación realizada, el analista debe proponer las medidas correctivas que sean necesarias con el fin que la empresa logre corregir las deficiencias de control identificadas en la evaluación. Normalmente, estas medidas correctivas estarán asociadas a la implementación y/o cumplimiento consistente de aquellas actividades de control sugeridas en la guía de evaluación que no hayan

sido implementadas por la empresa (o cuyo cumplimiento no se realice de una manera continua), y que el analista considere crítico para la empresa.

5.7. FASE V: CALIFICACIÓN

Actividad 5.1. Proponer calificación por área de riesgo analizada

Luego de realizada la evaluación de las actividades de control implementadas por la empresa, siguiendo las guías de evaluación propuestas, el analista debe proponer una calificación para cada una de las áreas de riesgo analizada. Para ello deberá tomar en cuenta el grado de adecuación y cumplimiento de las actividades de control evaluadas, y seguir el siguiente esquema propuesto:

Calificación	Descripción
A	La empresa ha implementado las actividades de control adecuadas para mitigar los riesgos en sistemas de información, a los que se encuentra expuesta en esta área. Estas actividades de control se vienen cumpliendo de manera continua y consistente.
B	La empresa ha implementado las actividades de control adecuadas para mitigar los riesgos en sistemas de información, a los que se encuentra expuesta en esta área. Sin embargo, estas actividades de control no se cumplen de manera continua, o sobre una base consistente.
C	La empresa ha implementado parcialmente actividades de control para mitigar los riesgos en sistemas de información, a los que se encuentra expuesta en esta área. Estas actividades de control se vienen cumpliendo parcialmente.
D	La empresa ha implementado mínimamente algunas actividades de control para mitigar los riesgos en sistemas de información, a

	los que se encuentra expuesta en esta área. Estas actividades de control se vienen cumpliendo de manera continua y consistente.
E	La empresa no ha implementado actividades de control para mitigar los riesgos en sistemas de información, a los que se encuentra expuesta en esta área, o aquellas implementadas no se cumplen de manera continua o sobre una base consistente.

Actividad 5.2. Proponer calificación global de la empresa

De acuerdo a la calificación otorgada a cada una de las áreas de riesgo evaluadas, y siguiendo el criterio del analista, debe proponerse una calificación global del riesgo en sistemas de información de la empresa analizada, para lo cual se propone el siguiente esquema:

Calificación	Descripción
A	La empresa viene tomando las medidas necesarias para administrar adecuadamente los riesgos en los sistemas de información a los que se encuentra expuesta.
B	La empresa viene tomando medidas para administrar adecuadamente los riesgos en los sistemas de información a los que se encuentra expuesta. Se han identificado debilidades menores, pero éstas pueden ser corregidas siguiendo los procedimientos normales de la empresa.
C	La empresa ha tomado medidas parciales para administrar los riesgos en los sistemas de información a los que se encuentra expuesta. Se han identificado deficiencias de control, cuya corrección requiere acción por parte de la Gerencia responsable y un monitoreo posterior. Sin embargo, la empresa cuenta con el personal y las habilidades requeridas para corregir los

	problemas identificados
D	La empresa ha tomado medidas mínimas para administrar los riesgos en los sistemas de información a los que se encuentra expuesta. En tal sentido, es posible que la empresa experimente pérdidas financieras o reducción en sus utilidades, como consecuencia de dicha situación. Se requiere una acción correctiva inmediata por parte de la Gerencia, con el fin de mitigar estos riesgos.
E	La empresa no ha tomado medidas para administrar los riesgos en los sistemas de información a los que se encuentra expuesta, o aquellas tomadas no se vienen cumpliendo de manera consistente. En tal sentido, la ocurrencia de estos riesgos tendría un impacto muy significativo en las operaciones de la empresa, incluyendo la posible paralización de operaciones, o corrupción en la integridad de datos, lo cual puede determinar que la empresa experimente pérdidas financieras o reducción de sus utilidades. Se requiere una acción correctiva inmediata por parte de la Gerencia, y un monitoreo permanente, con el fin de mitigar estos riesgos.

5.8. FASE VI: REPORTE FINAL

Actividad 6.1. Emitir reporte final de evaluación

El reporte final que se realizará al finalizar la evaluación debe contener las siguientes secciones:

REPORTE FINAL DE EVALUACION

ANALISIS DE RIESGOS EN LOS SISTEMAS DE INFORMACION

I. ASPECTOS GENERALES

1.1. Nombre de la empresa.
1.2. Analistas responsables.
1.3. Período de evaluación.
1.4. Areas de riesgo evaluadas.

II. RESUMEN DE LA EVALUACION

2.1. Calificación de la empresa.

A	B	C	D	E

2.2. Calificación de las áreas de riesgo evaluadas:

Area de riesgo	**Calificación**				
Area 1	A	B	C	D	E
Area 2	A	B	C	D	E
.....					
.....					

2.3. Comentarios generales

III. RESULTADOS DE LA EVALUACION POR AREA DE RIESGO

A. Area de riesgo 1
a. Calificación

A	B	C	D	E

b. Resultados de la evaluación

Principales actividades de control implementadas	Comentarios sobre la adecuación y el cumplimiento	Documentación de sustento
.....	.....	.....
.....	.....	.....

c. Medidas correctivas propuestas.

d. Comentarios adicionales.

B. Area de riesgo 2

.....

IV. ANEXOS

A. Diagrama con la infraestructura tecnológica de la empresa

B. Organigrama del departamento de sistemas de información de la empresa

C. Guías de evaluación de las áreas de riesgo llenadas (de acuerdo a los formatos propuestos en la sección 5.10).

5.9. Aplicaciones de la metodología

La metodología propuesta puede ser utilizada por los Gerentes de Sistemas de empresas bancarias, por auditores internos, auditores externos, consultores independientes, supervisores bancarios, entre otros.

Los Gerentes de Sistemas pueden utilizar la metodología como una guía para realizar una auto-evaluación (Self-assessment) de las actividades de control

implementadas por su empresa, y determinar las medidas correctivas que sean necesarias.

Los Auditores Internos y Externos pueden utilizar la metodología como referencia para los estudios de auditoría que realicen. En particular, las guías de evaluación que se detallan en la siguiente sección pueden ser fácilmente adaptadas y utilizadas como guías de auditoría.

Los consultores independientes pueden utilizar la metodología en la ejecución de estudios de análisis de riesgos en los sistemas de información para empresas bancarias. Para ello, deberán estimar el tiempo y recursos necesarios para llevar a cabo este tipo de estudios, de acuerdo al tamaño y complejidad de la empresa evaluada. Asimismo deben asegurarse que los analistas responsables del estudio cuenten con las habilidades necesarias y se encuentren adecuadamente capacitados para realizar un estudio de esta naturaleza. Normalmente se requerirá conocimientos de auditoría y/o experiencia previa en empresas del sector bancario.

Se estima que un estudio de análisis de riesgos en sistemas de información (como el que se propone), realizado en un Banco grande requerirá de 2 analistas a tiempo completo durante un mes, lo cual es equivalente a 368 horas-hombre (23 días útiles x 8 horas-hombre/día útil x 2).

Los supervisores bancarios generalmente incluyen entre sus labores de supervisión de la administración de riesgos en las empresas bancarias, los riesgos en los sistemas de información. Esto se realiza considerando la importancia de los sistemas de información en la operatividad normal de las empresas bancarias y la prestación de servicios al público. En tal sentido, la metodología propuesta puede ser usada por los supervisores bancarios en dicha labor, puesto que se encuentra orientada precisamente al análisis de riesgos en sistemas de información, la identificación de deficiencias de control y la formulación de las recomendaciones o medidas correctivas que sean necesarias.

5.10. Guías de evaluación de las actividades de control implementadas por la empresa en cada área de riesgo

En esta sección se presentan un conjunto de guías de evaluación, las cuales permiten analizar y evaluar las actividades de control implementadas por la empresa en cada una de las áreas de riesgo en sistemas de información identificadas. Estas guías se presentan junto con formatos de llenado, los cuales serán utilizados para registrar los hallazgos obtenidos durante la evaluación.

En tal sentido, por cada área de riesgo identificada se describe lo siguiente:

a. Proceso de tecnología de información asociado
b. Objetivo del proceso
c. Riesgos asociados
d. Aspectos a considerar en la evaluación de las actividades de control implementadas por la empresa

Se presentan guías de evaluación para las diez áreas de riesgo identificadas en el Modelo de Análisis propuesto:

a. Planeamiento estratégio de sistemas de información
b. Organización del departamento de sistemas de información
c. Adquisición e implementación de sistemas de información
d. Desarrollo y mantenimiento de sistemas de información
e. Implementación de un sistema de información integral
f. Seguridad de información
g. Continuidad operacional
h. Banca electrónica y el uso de Internet
i. Control de Gerencia
j. Revisiones de Auditoría Interna y Externa

La evaluación se orienta principalmente hacia la adecuación de las actividades de control implementadas por la empresa. La evaluación del cumplimiento se realiza a través de la obtención de documentación de sustento que acredite el cumplimiento consistente y continuo de las actividades de control identificadas.

El esquema planteado permite al analista, luego de evaluar la adecuación y el cumplimiento de las actividades de control implementadas por la empresa, proponer una calificación de las áreas de riesgo evaluadas, identificar posibles deficiencias existentes y proponer las medidas correctivas que sean necesarias.

5.10.1. Planeamiento estratégico de sistemas de información

Proceso de tecnología de información asociado:

- Definición de un plan estratégico de sistemas de información.

Objetivo del proceso:

- Elaboración de un plan estratégico de sistemas de información alineado al plan estratégico corporativo que considere las oportunidades que brinda el uso de la tecnología de información para el logro de los objetivos y metas de la organización.

Riesgos asociados:

- Sistemas de información que no soportan el logro de los objetivos y metas de la organización.
- Pérdida de oportunidades de negocio brindadas por los desarrollos recientes de tecnología de información, los cuales pueden ser aprovechados por la competencia.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent.***
• Se cuenta con un proceso de planeamiento estratégico de sistemas de información que considere, entre otros aspectos: a. Los objetivos y metas de la empresa b. La estrategia adoptada por la empresa para el logro de dichos objetivos y metas c. Los procesos de negocio de la empresa d. La arquitectura de sistemas de información necesaria para soportar la estrategia de la empresa. e. La infraestructura tecnológica existente y aquella necesaria para soportar la arquitectura de sistemas objetivo de la empresa.			

• Se ha realizado un análisis de impacto de las oportunidades y amenazas competitivas generadas por los desarrollos recientes de la tecnología de información. • Se han considerado los requerimientos de los organismos reguladores. • Los planes a largo plazo de sistemas de información son traducidos regularmente en planes de corto plazo (semestral, anual). • El plan estratégico de sistemas de información considera: a. Objetivos y metas cuantificables b. Cronograma de actividades, indicando fechas de inicio y término c. Asignación de responsables d. Mecanismos de control y reportes de avance del Plan e. Presupuesto necesario • El plan estratégico de sistemas de información cuenta con la aprobación del Directorio.			

5.10.2. Organización del departamento de sistemas de información

Proceso de tecnología de información asociado:

- Definición de la organización del departamento de sistemas de información.

Objetivo del proceso:

- Establecer la organización del departamento de sistemas de información, con roles y responsabilidades definidas y comunicadas, que defina de manera apropiada el número y las habilidades requeridas del personal del departamento.

Riesgos asociados:

- Ineficiencia en el desempeño de las funciones del departamento de sistemas de información.
- Organización inapropiada del departamento, personal insuficiente o sin las habilidades requeridas, deficiente asignación de roles y responsabilidades, inadecuada separación de funciones, entre otros aspectos.
- Conflictos internos permanentes entre el departamento de sistemas de información y las áreas usuarias.
- Redundancias en el desarrollo de sistemas de información, generando costos innecesarios.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent***
• Se ha definido una estructura organizativa y de reporte en la empresa, que asegura la independencia del departamento de sistemas de información, la cual puede incluir que el jefe del departamento (Gerente de Sistemas) reporte directamente a la Alta Gerencia. • Se cuenta con un Comité Gerencial (Comité Tecnológico o de Sistemas) conformado por el Gerente de Sistemas y los Gerentes de las áreas			

usuarias, con el objetivo de monitorear la ejecución de los planes de desarrollo de sistemas de información, y la priorización de los requerimientos de sistemas, de acuerdo al Plan Estratégico de Sistemas de Información de la empresa. • La composición, funciones y responsabilidades de dicho Comité Gerencial se encuentran documentadas. • Se han definido y se utilizan indicadores de rendimiento para medir: a. La efectividad y aceptación en el desempeño de las funciones del departamento con respectos a las áreas usuarias (clientes internos). b. Los resultados de las funciones del departamento en el logro de los objetivos de la organización. • Se han definido, documentado y difundido los roles y responsabilidades del personal del departamento, así como la definición de las habilidades técnicas necesarias para cada puesto asignado (P.ej. a través de un Manual de Organización y Funciones). • Existen políticas dirigidas hacia la evaluación y modificación de la estructura organizacional del departamento, de tal manera que se encuentre alineada apropiadamente a los cambios en los objetivos y en el entorno de la organización. • Existe una función y políticas de aseguramiento de calidad. • La función de aseguramiento de calidad cuenta con independencia suficiente con respecto al personal de desarrollo de sistemas, y cuenta con personal con las habilidades adecuadas para desempeñar sus responsabilidades. • Existe un proceso definido para asignar recursos y			

asegurar la ejecución de las pruebas de aseguramiento de calidad y la aprobación de esta área antes que los nuevos sistemas de información o los cambios en los sistemas existentes sean implementados. • Se ha designadò a un responsable, a nivel de la organización, para la formulación de las políticas y procedimientos relacionados con la seguridad de la información (física y lógica). • Existe separación de funciones en las siguientes áreas: a. Desarrollo y operación de sistemas. b. Desarrollo/mantenimiento de sistemas y seguridad de información. c. Desarrollo y aseguramiento de calidad d. Operaciones y control de datos. e. Operaciones y usuarios. f. Operaciones y seguridad de información. • Existen roles y responsabilidades apropiados para los procesos clave, incluyendo las actividades del ciclo de vida del desarrollo de sistemas (requerimientos, diseño, desarrollo, pruebas, implantación), seguridad de información, adquisiciones y planeamiento de la capacidad. • Se han definido y puesto en práctica una política de capacitación permanente al personal del departamento, de acuerdo a sus responsabilidades. • Se han definido y puesto en práctica políticas de motivación y retención del personal del dpto. • Existen políticas y procedimientos para controlar y monitorear las actividades del personal contratado por out-sourcing u otro mecanismo de contratación similar.			

5.10.3. Adquisición e implementación de sistemas de información

(La evaluación debe enfocarse hacia aquellos proyectos de adquisición e implementación de sistemas de información que resulten críticos para la empresa. La criticidad puede medirse en función al costo del proyecto en comparación con otros, o en función al impacto del proyecto en los procesos críticos de la empresa)

Proceso de tecnología de información asociado:

- Adquisición e implementación de sistemas de información, incluyendo equipos de cómputo, sistemas de información desarrollados a medida, software de aplicación, equipos de telecomunicaciones, entre otros rubros.

Objetivo del proceso:

- Adquirir e implementar sistemas de información que satisfagan los requerimientos de la empresa y se ajusten a sus políticas y estándares.

Riesgos asociados:

- Insatisfacción de las necesidades de los usuarios finales.
- Excesos sobre los costos y tiempos inicialmente estimados.
- Incompatibilidad entre los sistemas adquiridos y la arquitectura de sistemas de la empresa.
- Selección de alternativas excesivamente complejas o costosas.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent***
• Los proyectos de adquisición e implementación de sistemas de información se encuentran enmarcados en el Plan Estratégico de Sistemas de Información de la empresa. • La Alta Gerencia participa en los proyectos de adquisición de sistemas de información de la siguiente manera: a. Ha aprobado los objetivos y metas de la adquisición.			

b. Ha designado a un líder de proyecto, responsable del proyecto de adquisición. c. Ha aprobado el presupuesto del proyecto de adquisición. d. Participa en revisiones periódicas del proyecto. • Los usuarios finales participan a lo largo de todo el proceso de adquisición de sistemas de información, de tal manera que se asegure que sus requerimientos han sido correctamente entendidos y que el sistema resultante sea aceptado y usado. • En tal sentido, los usuarios finales: a. Participan en las revisiones periódicas del proyecto b. Han aprobado la determinación de requerimientos del proyecto c. Han validado las alternativas planteadas con respecto a los requerimientos originales. d. Han aprobado la alternativa seleccionada. e. Han definido un criterio de aceptación. f. Han participado durante las pruebas, implementación y aceptación final del sistema adquirido. • Se ha asignado a un equipo de trabajo responsable del proyecto de adquisición con las habilidades y autoridad necesarias para la ejecución del proyecto. • Se han definido adecuadamente las especificaciones del sistema a ser adquirido, de tal manera que se satisfagan los requerimientos de los usuarios finales. Estas especificaciones incluyen por lo menos: a. Un resumen de los requerimientos funcionales que serán satisfechos por el sistema.			

b. Cargas de trabajo presente y proyectadas, y un análisis de la capacidad requerida. c. Requerimientos de seguridad de información d. Requerimientos de controles operacionales. e. Requerimientos de contingencia para aquellos recursos cuya pérdida origine la paralización de los procesos críticos de la empresa f. Factores de espacio y de entorno, como fuentes de energía, disipación de calor generado, etc. g. Requerimientos de capacitación h. Interfases con otros sistemas i. Requerimientos de interfases de usuario • Se han analizado los riesgos, costos y beneficios de las alternativas consideradas, y se ha seleccionado una alternativa en base a los resultados de dicho análisis. En tal sentido, se ha considerado por lo menos: a. Costos de implementación, operación y mantenimiento de la alternativa evaluada. b. Beneficios de la alternativa evaluada en términos de reducción de costos, uso de recursos y menores tiempos para el procesamiento de la información. c. Riesgos financieros, técnicos y aquellos asociados al cumplimiento del cronograma planteado para la ejecución del proyecto. • Se realiza una adecuada administración del proyecto en su fase de implementación, a través de las siguientes actividades: a. Monitoreo del desempeño del proveedor a través de la revisión de los entregables y reportes de avance. b. Verificar que los requerimientos del contrato			

sigan reflejando de manera exacta las necesidades de los usuarios. c. Evaluación del proceso de control de calidad del proveedor. • Se han definido y ejecutado pruebas de aceptación de los entregables finales del proyecto, de tal manera de asegurar que los requerimientos funcionales hayan sido satisfechos.			

5.10.4. Desarrollo y mantenimiento de sistemas de información

Proceso de tecnología de información asociado:

- Desarrollo y mantenimiento de los sistemas de información de la empresa.

Objetivo del proceso:

- Desarrollar y mantener los sistemas de información de la empresa, de tal manera que satisfagan los requerimientos de los usuarios y soporten adecuadamente los procesos de negocio.

Riesgos asociados:

- Sistemas de información que no satisfacen los requerimientos de las áreas usuarias.
- Documentación inadecuada de los sistemas, lo cual genera ineficiencia y dependencia excesiva hacia cierto personal del área de sistemas.
- Proyectos de desarrollo de sistemas que se exceden en los tiempos, o que resultan excesivamente costosos en términos del uso de recursos humanos y financieros.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent***
Ingeniería del Producto • Se han definido, documentado y difundido estándares para cada una de las etapas de los proyectos de desarrollo de sistemas de información: determinación de requerimientos, diseño, codificación, pruebas, implementación. • Los procedimientos utilizados para la determinación de requerimientos incluyen: a. La aprobación final del usuario a fin de verificar su alcance, claridad y validez. b. Una revisión de la factibilidad y complejidad de los requerimientos.			

• Existen procedimientos para el registro y documentación de los requerimientos de datos de entrada, lógica de procesamiento y datos de salida para cada nuevo proyecto de desarrollo y/o modificación de sistemas. • Los estándares de diseño de sistemas señalan la participación del usuario en la verificación de las especificaciones de diseño en comparación con sus requerimientos iniciales. • Las especificaciones de diseño son firmadas por los departamentos usuarios para cada nuevo proyecto de desarrollo de sistemas y para proyectos de modificación de sistemas. • Existen estándares para la ejecución de pruebas unitarias previas a las pruebas de aceptación de usuario. • Las pruebas de aceptación de usuario incluyen criterios de aceptación para todos los requerimientos especificados. • Existen procedimientos para el registro de los requerimientos de control interno y de seguridad (control de acceso) en los proyectos de desarrollo de sistemas. *Entorno de Desarrollo* • Se cuenta con herramientas de desarrollo (lenguajes de programación, compiladores, herramientas CASE) con el soporte adecuado que facilite el entrenamiento del personal y el mantenimiento de los sistemas desarrollados. • Se utiliza un equipamiento de hardware adecuado para la ejecución de las pruebas de integración y de aceptación de usuario , de tal manera que permita simular el ambiente de producción.			

• Se define un cronograma de actividades con la asignación de responsables para los proyectos de desarrollo de sistemas • Se definen, documentan y comunican los roles y responsabilidades de los integrantes de los equipos de desarrollo de sistemas. • Existen procedimientos de monitoreo y de reporte del avance para los proyectos de desarrollo de sistemas • Se cuenta con la participación del área de aseguramiento de calidad en los proyectos de desarrollo de sistemas. *Restricciones* • La Alta Gerencia aprueba los proyectos de desarrollo de sistemas, así como los cronogramas, personal y presupuestos del proyecto. *Documentación* • Se preparan manuales de usuario y manuales técnicos del sistema desarrollado para cada proyecto de desarrollo de sistemas. • Se tienen procedimientos de modificación de los manuales, en caso sea necesario para cada modificación de los sistemas existentes en la empresa. *Control de cambios* • Existe un procedimiento documentado y en uso para el control de cambios que incluye la participación de las áreas usuarias y del equipo de desarrollo. • Se cuenta con herramientas automatizadas que			

permiten llevar una adecuada administración de la configuración, y un control apropiado de las versiones de los aplicativos existentes en la empresa.			

5.10.5. Implementación de sistemas de información integrales

Proceso de tecnología de información asociado:

- Implementación de un sistema de información integral (o un sistema ERP) que soporte los procesos críticos de la empresa bancaria.

Objetivo del proceso:

- Implementar un sistema de información integral bancario que permita incrementar la eficiencia en el uso de recursos de la empresa, así como la incorporación de las 'mejores prácticas' en los procesos de negocio de la empresa, de acuerdo a las reglas de negocio incorporadas en el sistema.

Riesgos asociados:

- Resistencia al cambio por parte del personal de la empresa.
- El proveedor del sistema de información no cuenta con el soporte técnico adecuado a lo largo del desarrollo del proyecto de implementación.
- No se cuenta con el apoyo y compromiso de la Alta Gerencia
- La empresa no cuenta con los recursos humanos y financieros adecuados durante el desarrollo del proyecto de implementación.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent***
Evaluación del sistema de información integral • La empresa ha evaluado el sistema de información integral a ser implementado considerando entre otros aspectos: a. Funcionalidades del sistema b. Alcance del sistema con respecto a los procesos críticos de negocio de la empresa c. Flexibilidad en relación a nuevos requerimientos funcionales de la empresa			

d. Características técnicas de rendimiento y tiempos de respuesta e. Infraestructura tecnológica necesaria para la implementación del sistema f. Generación de información consolidada para la Gerencia, así como posibilidad de explotar dicha información con herramientas adicionales. g. Tiempos estimados de implementación h. Costos y facilidades de financiamiento. *Evaluación del proveedor* • La empresa ha evaluado el soporte técnico brindado por el proveedor del sistema de información integral a ser implementado considerando entre otros aspectos: a. Número de implementaciones realizadas b. Recursos humanos asignados c. Características del servicio de soporte brindado por el proveedor • Se ha firmado un contrato de soporte técnico, el mismo que se encuentra vigente, con el proveedor del sistema de información o con otra empresa especializada en el sistema de información implementado. *Compromiso de la Alta Gerencia, administración del cambio y organización del proyecto* • La Alta Gerencia se encuentra comprometida con el proyecto de implementación de la siguiente manera: a. Ha establecido un plan de comunicaciones con			

el personal involucrado, con el fin de reforzar la concientización del personal en los objetivos del proyecto y minimizar la resistencia al cambio. b. Ha definido un programa de entrenamiento y capacitación al personal en los nuevos procedimientos de trabajo y en el uso del nuevo sistema de información. c. Ha designado a un jefe de proyecto a dedicación exclusiva, con la capacidad suficiente para administrar este tipo de proyectos. d. Ha definido mecanismos de reporte periódicos sobre el avance del proyecto de implementación. • Se ha definido un cronograma de actividades del proyecto con asignación de responsables, e hitos de control. • Se ha formado un equipo idóneo para la implementación del sistema de información integral • Se han definido políticas y procedimientos para la documentación de los cambios realizados durante la etapa de 'personalización' del sistema de información integral. • Se han definido políticas y procedimientos para la 'convivencia' transitoria entre módulos del sistema de información antiguo con los módulos implementados del sistema de información nuevo.			

5.6.6. Seguridad de información

Proceso de tecnología de información asociado:

- Seguridad física y lógica de los sistemas de información de la empresa.

Objetivo del proceso:

- Proteger la información de la empresa contra posibles usos, revelaciones o modificaciones no autorizadas, así como los dispositivos y las instalaciones en las cuales se procesa la información de la empresa.

Riesgos asociados:

- Acceso y revelación no autorizada de información crítica y confidencial de la empresa.
- Modificaciones no autorizadas de información crítica y confidencial de la empresa.
- Daños en los dispositivos e instalaciones que procesan la información de la empresa.
- Robos de los equipos de hardware y comunicaciones de la empresa.
- Proporcionar información inexacta a la Gerencia lo cual expone a la empresa a una inadecuada toma de decisiones tácticas y estratégicas.
- Proporcionar información inexacta a los órganos de regulación y supervisión, lo cual expone a la empresa a posibles sanciones y multas.
- Pérdida de información crítica debido a sabotaje, virus informáticos, accesos no autorizados, etc.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent***
Organización de la Seguridad de Información • Se cuenta con personal responsable de la seguridad de información, cuyas funciones incluyen: a. Desarrollo del plan de seguridad de información de la empresa, el cual incluye la definición de normas y procedimientos de			

detección de amenazas, y de protección de activos de información. b. Control de la ejecución y aplicación de dichas normas y procedimientos. • El personal responsable de la seguridad de información cuenta con las habilidades técnicas necesarias y se encuentra adecuadamente capacitado para cumplir sus funciones. *Seguridad Física* • Se cuenta con un plan de seguridad física que considera entre otros aspectos: a. Evaluación de aquellos equipos informáticos (hardware y dispositivos de comunicación) que requieren tener seguridad. b. Evaluación de las fuentes de riesgo que amenazan a dichos equipos. c. Evaluación de la probabilidad de ocurrencia de dichos riesgos. d. Determinación de los costos asociados a dicha ocurrencia. e. Evaluación de las alternativas disponibles para minimizar la exposición de dichos riesgos. f. Implementación de las alternativas seleccionadas. • Existe un proceso para actualizar periódicamente el inventario de hardware (computadores centrales, terminales, servidores, PCs, periféricos, etc.) y equipos de comunicación de la empresa, el cual registra por lo menos: a. Marca, tipo y modelo b. Número de serie c. Costo d. Fecha y lugar de compra			

e. Localización actual f. Nombre del usuario o grupo de usuarios responsable de su uso • El inventario de hardware incluye a los equipos no utilizados por la empresa, los mismos que son almacenados en un lugar seguro. • Se ha identificado y definido las responsabilidades del personal autorizado para el ingreso y operación del centro de cómputo. • El centro de cómputo cuenta con las medidas de seguridad necesarias para impedir y detectar el ingreso de personal no autorizado, lo cual puede incluir el uso de dispositivos de identificación (badges), personal de seguridad, cámaras de video, detectores láser, alarmas, etc. • El centro de cómputo cuenta con medidas de seguridad para mitigar los riesgos ambientales: equipos anti-incendios, detectores de calor o detectores de humo, etc. • El personal del centro de cómputo se encuentra entrenado para utilizar el equipo de emergencia en caso de un incendio u otro tipo de desastre. • Se han definido y difundido medidas preventivas hacia el personal del centro de cómputo que incluyen posibles prohibiciones para comer, beber o fumar en las instalaciones del centro de cómputo, así como la necesidad de mantener libre el acceso a los equipos de emergencia en caso de desastre. • Se ha definido y difundido procedimientos de seguridad hacia los usuarios de computadores personales, que incluyen: a. Medidas preventivas con el fin de evitar posibles daños debidos a excesos de humo,			

calor, polvo, agua, partículas de comida, entre otros aspectos. b. Medidas preventivas para el manejo de diskettes, discos compactos (CDs), cintas de respaldo, entre otros dispositivos. c. Estándares para el rotulado de diskettes, cintas de respaldo y otros. • Se utilizan mecanismos de protección contra la electricidad estática (descarga a tierra), y contra las fluctuaciones bruscas de la energía (estabilizadores, supresores de picos). *Seguridad de Datos - Controles de acceso lógico* • Se han definido e implementado los niveles de acceso del personal a los sistemas de información de la empresa, de acuerdo a sus funciones y responsabilidades. • Se utilizan apropiadamente las facilidades proporcionadas por el software base para la implementación de dichos niveles de acceso (sistema operativo del computador central, sistemas operativos de red, administrador de bases de datos, etc.). • La identificación de usuario ('user-id') es única para cada uno de los usuarios, de tal manera que pueda asignarse el nivel de acceso que le corresponda y para registrar las transacciones realizadas por dicho usuario. • Se utilizan contraseñas para cada usuario, las mismas que sirven para autentificar el acceso del usuario. • Las contraseñas: a. Son cambiadas periódicamente			

b. Se mantienen de manera confidencial. c. Al ser ingresados en el computador, su valor no puede ser leído por terceros (formato encriptado, no aparece en la pantalla o su valor es sobre-escrito por otros caracteres: ****, ####, XXXX, etc.) d. Están asociadas a un número limitado de intentos de acceso, luego del cual se niega el acceso definitivamente. • Los identificadores de usuario y sus respectivas contraseñas son eliminadas cuando un usuario se encuentra ausente por tiempo prolongado, o se ha retirado de la empresa. • Se mantienen y analizan registros de transacciones o 'logs' que contienen la siguiente información: a. Intentos no autorizados para acceder a los sistemas de información de la empresa. b. Intentos para obtener información por encima del nivel de acceso asignado al usuario. c. Archivos de transacciones detalladas por cada aplicación. Como mínimo, estos archivos deberían contener información acerca de la transacción y la identificación del terminal y operador que inició la transacción. • Se utilizan procedimientos especiales de seguridad para restringir el acceso a los programas y librerías de los sistemas operativos, con el fin de evitar posibles modificaciones no autorizadas a dichos programas. *Seguridad de datos - Integridad de datos* • Se utilizan procedimientos de verificación de la información crítica generada por los sistemas de			

información de la empresa. • Se utilizan procedimientos especiales de revisión de la información proporcionada a la Alta Gerencia y al Directorio (sistemas de información información gerencial), y aquella que es proporcionada a los organismos de regulación y supervisión (Superintendencia, Banco Central). • Se han definido y puesto en práctica procedimientos de seguridad para la impresión de reportes con información confidencial, con el fin de impedir el acceso no autorizado a dicha información. • Se han definido y puesto en práctica procedimientos de seguridad relacionados con el uso de información confidencial en los escritorios del personal, tanto en medio impreso como electrónico (diskettes, cintas de respaldo), los cuales deberían ser almacenados en sitios cerrados con el fin de evitar posibles robos, revelación no autorizada o modificaciones. • Se han definido y puesto en práctica procedimientos de seguridad en relación al uso de computadores personales que incluyan el uso de contraseñas de encendido y de acceso al disco duro del computador, el uso de protectores de pantalla, entre otros aspectos. *Seguridad de datos - Separación de funciones* • Se utiliza la política de separación de funciones, en particular entre las siguientes actividades: a. La preparación de los datos de entrada a los sistemas y la revisión de la exactitud y legimitidad de dichos datos. b. La revisión de los cambios o correcciones de			

los archivos maestros y la ejecución de las transacciones que realizan dichos cambios. c. En general, las personas responsables de generar la información de entrada deben ser diferentes de aquellas que procesan dicha información. *Seguridad de datos - Seguridad en Redes* • Se han definido y puesto en práctica mecanismos de control que permiten identificar y autentificar a los usuarios remotos que requieren tener acceso a la red interna de la empresa, además de definir sus niveles de acceso de acuerdo a sus funciones y responsabilidades. • Se han establecido mecanismos de control que permiten asegurar la confiabilidad y exactitud de la información transmitida a través de redes de comunicación (telefonía, redes de datos, ondas de radio, satélites, etc.). • Se ha definido, difundido y puesto en práctica procedimientos de seguridad relacionados con el nivel de acceso a los recursos de la red intena de la empresa (incluyendo el acceso a equipos con información de carácter confidencial). *Seguridad de datos - Virus informáticos* • Se han definido, difundido y puesto en práctica procedimientos de seguridad para evitar el uso de archivos de procedencia dudosa, tanto aquellos que puedan ser ingresados a través de diskettes, como aquellos que puedan ser descargados de la red Internet.			

• Se cuenta con software antivirus, el mismo que es actualizado periódicamente. • Se han definido los procedimientos a seguir en caso se detecte la presencia de un virus informático en alguno de los equipos de la red de la empresa.			

5.10.7. Continuidad operacional

Proceso de tecnología de información asociado:

- Elaboración de un plan de continuidad operacional para la empresa

Objetivo del proceso:

- Asegurar el funcionamiento continuo de los sistemas de información de la empresa frente a la ocurrencia de un desastre o una interrupción en sus proveedores de servicios básicos (energía, comunicaciones, etc.).

Riesgos asociados:

- Paralización de operaciones de la empresa y dificultades en la reanudación de operaciones ante la ocurrencia de un desastre.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent.***
Plan de contingencia corporativo • La empresa cuenta con un plan de contingencias corporativo, el mismo que ha sido aprobado por el Directorio y revisado dentro de los últimos doce meses. • Existe un gerente encargado de monitorear el desarrollo, implementación y mantenimiento del plan de contingencias corporativo. • El plan de contingencias corporativo: a. Considera los procesos críticos de negocio de la empresa b. Considera los posibles riesgos que amenazan la continuidad operativa de la empresa: inundaciones, fuego, terremotos, fallo en la energía, fallo del computador central, interferencia en las telecomunicaciones, etc. c. Define claramente el esquema de notificación			

en caso de una contingencia d. Define claramente las responsabilidades y atribuciones de los equipos designados a trabajar durante la contingencia. e. Designa a una persona responsable para la comunicación externa (vocero oficial). f. Define claramente los procedimientos de recuperación de operaciones en caso de una contingencia, lo cual puede incluir el uso de un centro de cómputo alterno. g. Define los procedimientos de restauración al modo normal de operaciones en caso haya finalizado el estado de contingencia. • En caso el plan de contingencia corporativo incluye el uso de un centro de cómputo alterno: a. El centro de cómputo alterno es físicamente compatible con el centro de cómputo principal. Tanto el hardware como el software deben ser físicamente compatibles con el fin de procesar adecuadamente las aplicaciones de la empresa. b. El centro de cómputo alterno se encuentra a una distancia razonable del centro de cómputo principal, de tal manera que se encuentre libre de los efectos de algún posible desastre natural que afecte al centro de cómputo principal. c. El centro de cómputo alterno tiene la suficiente capacidad de procesamiento para procesar el volumen de operaciones promedio de la empresa e inclusive el volumen más alto de operaciones ('peak load'). d. Se han definido: el esquema de notificación al centro de cómputo alterno en caso de una			

contingencia, los procedimientos a seguir en dicho centro de cómputo, y la información física y electrónica que serán llevadas desde el centro de cómputo principal. • Se cuenta con procedimientos documentados y en uso para el entrenamiento del personal que participará durante la contingencia. • Una copia del plan de contingencia corporativo es guardada fuera del centro de cómputo y de la oficina principal de la empresa. • Se cuenta con procedimientos documentados y en uso para el mantenimiento y actualización del plan. • Las pruebas realizadas al plan de contingencia se encuentran documentadas, y consideran lo siguiente: a. Definición de metas y objetivos de la prueba b. Condiciones realistas y volumen de actividad cercano a la realidad c. Participación y revisión por la unidad de auditoría interna d. Un reporte de análisis de los resultados de la prueba, el cual incluye una comparación de los resultados de la prueba con las metas originales e. Desarrollo de un plan de acción correctiva para todos aquellos problemas encontrados *Procedimientos de respaldo* • Se han definido, difundido y puesto en práctica procedimientos de respaldo para que los usuarios de computadores personales respalden información crítica de acuerdo a sus funciones y responsabilidades, en dispositivos de			

almacenamiento adecuados para tal fin (discos duros de la red interna, diskettes, cintas magnéticas, discos ópticos, etc.). • Se cuenta con procedimientos regulares y se asignado responsables para la obtención periódica de respaldos de la información crítica manejada por la empresa en sus computadores centrales, o servidores de red. • Se cuenta con procedimientos regulares para la obtención de copias de respaldo actualizadas de: a. Los sistemas operativos utilizados por la empresa en sus diferentes plataformas. b. Las aplicaciones críticas de la empresa (código fuente y objeto) c. Documentación de sistemas operativos y de aplicaciones críticas • Las copias de respaldo son almacenadas en un lugar seguro y separado del centro de cómputo, y (en la medida de lo posible) en un local diferente al de la oficina principal. • Se han definido procedimientos para probar periódicamente la efectividad de las copias de respaldo en la reanudación de las operaciones normales de la empresa.			

5.10.8. Banca electrónica y el uso de Internet

Proceso de tecnología de información asociado:

- Distribución de servicios bancarios a través de dispositivos electrónicos y redes de comunicación

Objetivo del proceso:

- Brindar el soporte informático adecuado para el correcto funcionamiento de los dispositivos de banca electrónica que permiten brindar servicios bancarios a los clientes de la empresa bancaria y el público en general.

Riesgos asociados:

- Mal funcionamiento de los dispositivos de banca electrónica, lo cual puede causar reacciones negativas por parte de los clientes de la empresa bancaria.
- Fraude electrónico, a través de delincuentes que pueden efectuar robos a través de los dispositivos de banca electrónica.
- Accesos no autorizados a información privada de los clientes, la cual es transferida a través de redes de comunicación públicas (red telefónica, Internet).
- Accesos no autorizados a la red interna del Banco, a través de la red Internet.
- Establecimiento de sitios web falsos en Internet que simulan el sitio web del Banco, obteniendo de esta manera información confidencial brindada por los clientes de la empresa.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent.***
• Las claves secretas o PINs (Personal Identification Numbers) utilizadas para el funcionamiento de los cajeros automáticos se encuentran encriptadas en todos los archivos y bases de datos. • El personal del banco no tiene disponible el valor de las claves secretas de los clientes en sus			

terminales de operación o de atención en ventanilla. • Las claves secretas son ingresadas solamente por el cliente y en un entorno que evite la observación casual de su valor. • El sistema de administración de los cajeros registra el número de intentos no exitosos para el ingreso de la clave secreta, y restringe el acceso a las cuentas del cliente, después de un número pequeño de intentos. • Las aplicaciones que contienen las fórmulas, algoritmos y datos usados para generar las claves secretas estan sujetas al más alto nivel de acceso por propósitos de seguridad. • El sistema de administración de claves secretas permite el cambio de la clave secreta por el cliente, sin que ello requiera el cambio de la tarjeta. • El personal dedicado a la administración y asignación de las tarjetas no se encuentra involucrado de manera alguna en los procesos de asignación de las claves secretas. • Existen procedimientos apropiados para el control del inventario de las tarjetas en blanco y las tarjetas usadas (incluyendo aquellas usadas para pruebas y aquellas desechadas). • (En caso las tarjetas sean producidas por la empresa) Se cuenta con procedimientos de seguridad adecuados para los equipos utilizados en la producción de las tarjetas. • (En caso las tarjetas sean producidas por un tercero) Se cuenta con un contrato escrito con el proveedor de tarjetas en el que se detallan los procedimientos de control utilizados para			

mantener la confidencialidad de la información de los clientes y los procedimientos de contingencia en uso. • Existen procedimientos de control adecuados para las tarjetas retenidas por los cajeros automáticos. • Se mantienen registros de las transacciones diarias realizadas por los cajeros automáticos, los cuales pueden ser utilizados como pistas de auditoría en caso de una revisión. • Se cuenta con mecanismos de monitoreo del funcionamiento de la red de cajeros automáticos. • Se cuenta con procedimientos de contingencia en caso de caídas de la red de cajeros automáticos. • (En caso se utilice una red de cajeros automáticos compartida) Se cuenta con procedimientos de control adecuados en caso la red compartida se vuelva inoperable, con el fin de mantener el nivel de seguridad apropiado y la exactitud de las operaciones. • Se ha comunicado apropiadamente a los clientes los procedimientos de seguridad que deben seguir con el fin de evitar posibles robos o usos fraudulentos de sus tarjetas de débito y crédito. • Se cuenta con mecanismos (automatizados) para reconocer patrones anormales de consumo en tarjetas de débito y crédito, de tal manera que sea posible detectar posibles robos o usos fraudulentos de estas tarjetas. *Banca por Internet* • Se utiliza un protocolo de seguridad para la transmisión de mensajes a través del Internet, el cual considera:			

a. El uso de técnicas de encriptación de datos para asegurar la privacidad de la transmisión. b. La autentificación de la identidad de las partes utilizando criptografía asimétrica o de clave pública (P.ej. RSA, DSS). c. La confiabilidad de la conexión a través de la verificación de la integridad del mensaje usando un código de autenticación de mensajes (MAC) con clave. Pueden utilizarse funciones especiales (P.ej. SHA, MD5, etc.) para los cálculos de las MACs. • Se cuenta con un firewall, el cual permite centralizar el control de acceso a la red interna de la empresa desde el Internet. • Se guarda un registro diario de las transacciones realizadas a través del Internet, con el fin que sea utilizado como pista de auditoría en revisiones posteriores. • Se han definido esquemas especiales de seguridad en caso se permita la transferencia de fondos a cuentas de terceros.			

5.10.9. Control y monitoreo de la Gerencia

Proceso de tecnología de información asociado:

- Monitoreo de los procesos de tecnología de información

Objetivo del proceso:

- Asegurar el logro de los objetivos definidos para los procesos de tecnología de información

Riesgos asociados:

- Un esquema deficiente de monitoreo de los procesos de tecnología de información no permite corregir oportunamente los posibles errores que ocurran durante su ejecución, tanto en el corto como en el largo plazo.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent.***
• La información utilizada para monitorear los procesos de tecnología de información es apropiada. • Se utilizan indicadores de rendimiento para medir el desempeño de los procesos de tecnología de información versus los niveles definidos. • Se han definido procedimientos para el registro de información relacionada con errores de control interno, inconsistencias y excepciones, los mismos que son comunicadas oportunamente a la Gerencia. • La frecuencia de los reportes permite una rápida respuesta para las posibles excepciones encontradas.			

5.10.10 Revisiones de auditoría interna y externa

Proceso de tecnología de información asociado:

- Revisión independiente de los procesos de tecnología de información

Objetivo del proceso:

- Incrementar los niveles de confianza en el desempeño de los procesos de tecnología de información de la empresa, e incorporar las mejores prácticas de dichos procesos en la empresa.

Riesgos asociados:

- Revisiones inadecuadas por parte de la unidad de auditoría interna puede significar que la empresa no identifique en el tiempo necesario, posibles deficiencias de control y/o problemas potencialmente serios relacionados con sus sistemas de información.

Evaluar las actividades de control implementadas por la empresa, considerando si:	***Rev. (S/N)***	***Hallazgos encontrados***	***Doc. sustent.***
• El Directorio: a. Aprueba los planes de auditoría y sus cronogramas respectivos b. Revisa el cumplimiento de los planes c. Aprueba actividades extraordinarias de auditoría no consideradas en los planes d. Revisa los informes de auditoría y el trabajo de los auditores y consultores externos. • El programa de auditoría externa complementa las funciones de la auditoría interna de sistemas. • El orden jerárquico de la función de auditoría de sistemas garantiza la independiente necesaria de esta unidad.			

• El personal de auditoría de sistemas es adecuado en número y tiene competencia técnica para cumplir sus funciones. • Se ha definido y puesto en práctica un manual de procedimientos de auditoría de sistemas, el cual incluye: a. Las políticas y procedimientos de auditoría de sistemas a ser practicados en la empresa. b. El formato, contenido y distribución de los reportes de auditoría c. Los procedimientos para el seguimiento de las recomendaciones de auditoría d. El formato y contenido de las hojas de trabajo e. Las políticas de seguridad sobre los materiales de auditoría. • Los criterios de planeamiento y programación para la selección, alcance y frecuencia de los trabajos de auditoría, incluyen los siguientes aspectos: a. La definición adecuada del universo de auditoría. b. Un análisis de riesgos previo (*risk assessment*) • La programación de los trabajos de auditoría soporta el universo completo de auditoría, el mismo que será revisado al terminar el ciclo de auditoría. • El ciclo de auditoría es razonable. • Determinar la fecha del último trabajo de auditoría realizado a las siguientes áreas: a. Planeamiento y Organización • Planeamiento estratégico de sistemas de información			

• Organización del departamento de sistemas de información b. Adquisición, desarrollo y mantenimiento • Adquisición de sistemas de información • Desarrollo y mantenimiento de sistemas de información • Implementación de sistemas de información integrales c. Operaciones y soporte • Planeamiento de contingencias • Seguridad de información • Banca electrónica y el uso de Internet • Existe una participación adecuada de la función de auditoría interna en: a) El ciclo de vida de desarrollo de sistemas de información b) Los cambios importantes a las aplicaciones o a los sistemas operativos. • Los procedimientos de seguimiento de las observaciones exigen: a. Una respuesta escrita de la gerencia que indique cada deficiencia, incluyendo la acción correctiva tomada. b. Pruebas subsiguientes de auditoría para verificar la solución de las deficiencias. c. Reportes escritos al Directorio o Comité de Auditoría indicando los resultados del seguimiento.			

CAPITULO VI

FUENTES METODOLOGICAS DE REFERENCIA

6.1. Introducción

En el presente capítulo se describen las principales fuentes de referencia utilizadas para el diseño de la metodología descrita en el capítulo anterior. Estas fuentes de referencia incluyen el estándar COBIT de la Asociación ISACA, la Metodología de Análisis de Riesgos en Sistemas de Información del sistema de la Reserva Federal de Estados Unidos, la Metodología MAGERIT del Consejo Superior de Informática de España, entre otras.

6.2. El estándar COBIT de la Asociación ISACA

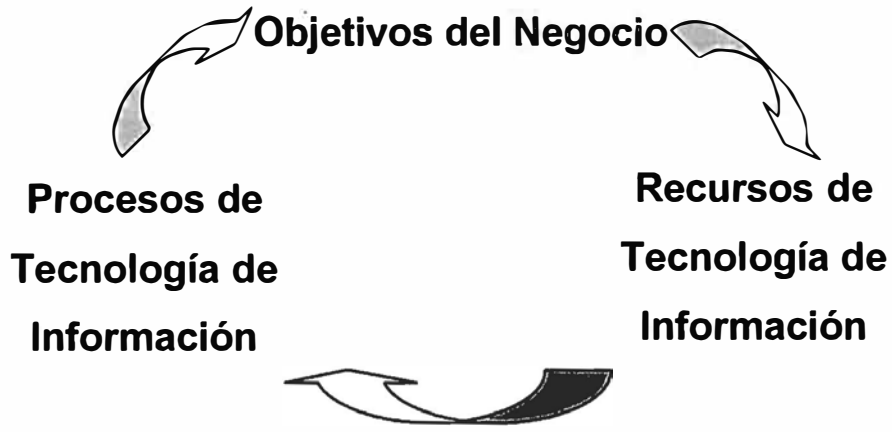
ISACA (Information Systems Audit and Control Asociation) es una asociación internacional de profesionales en auditoría de sistemas de información formada en 1969, y constituye en la actualidad una de las principales fuentes de estándares en prácticas de control de los procesos de tecnología de información. Asimismo esta asociación administra la certificación internacional CISA (Certified Information Systems Auditor), la cual ha sido otorgada a cerca de 12000 profesionales alrededor del mundo.

El proyecto COBIT (Control Objectives for Information and Related Technology) surgió al haberse identificado la necesidad de contar con estándares de referencia para el control en los procesos de tecnología de información. El objetivo del proyecto COBIT consistía en desarrollar un *estándar generalmente aceptado* y aplicable de *buenas prácticas* para el control de los sistemas de información. El

término "generalmente aceptado" se utiliza en el mismo sentido de los "Principios de Contabilidad Generalmente Aceptados" usados en Contabilidad, y las "buenas prácticas" se han definido de acuerdo a un consenso entre los expertos sobre el tema.

La estructura del COBIT se basa en la siguiente premisa:

"Los recursos de tecnología de información necesitan ser administrados mediante un conjunto de **procesos de tecnología de información** agrupados naturalmente, para proporcionar la información que la empresa necesita para alcanzar sus objetivos."[1]



A partir de esta premisa se han identificado 34 procesos de tecnología de información, cada uno de los cuales soporta algún requerimiento del negocio. Estos procesos han sido agrupados en cuatro dominios:

Planeamiento y Organización. Este dominio cubre la estrategia y tácticas de la empresa y se refiere a la manera como la tecnología de información puede

[1] COBIT Framework - 1996.

contribuir de la mejor manera al logro de los objetivos del negocio. Además, la implementación de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, considera el establecimiento de una organización apropiada, así como una adecuada infraestructura tecnológica.

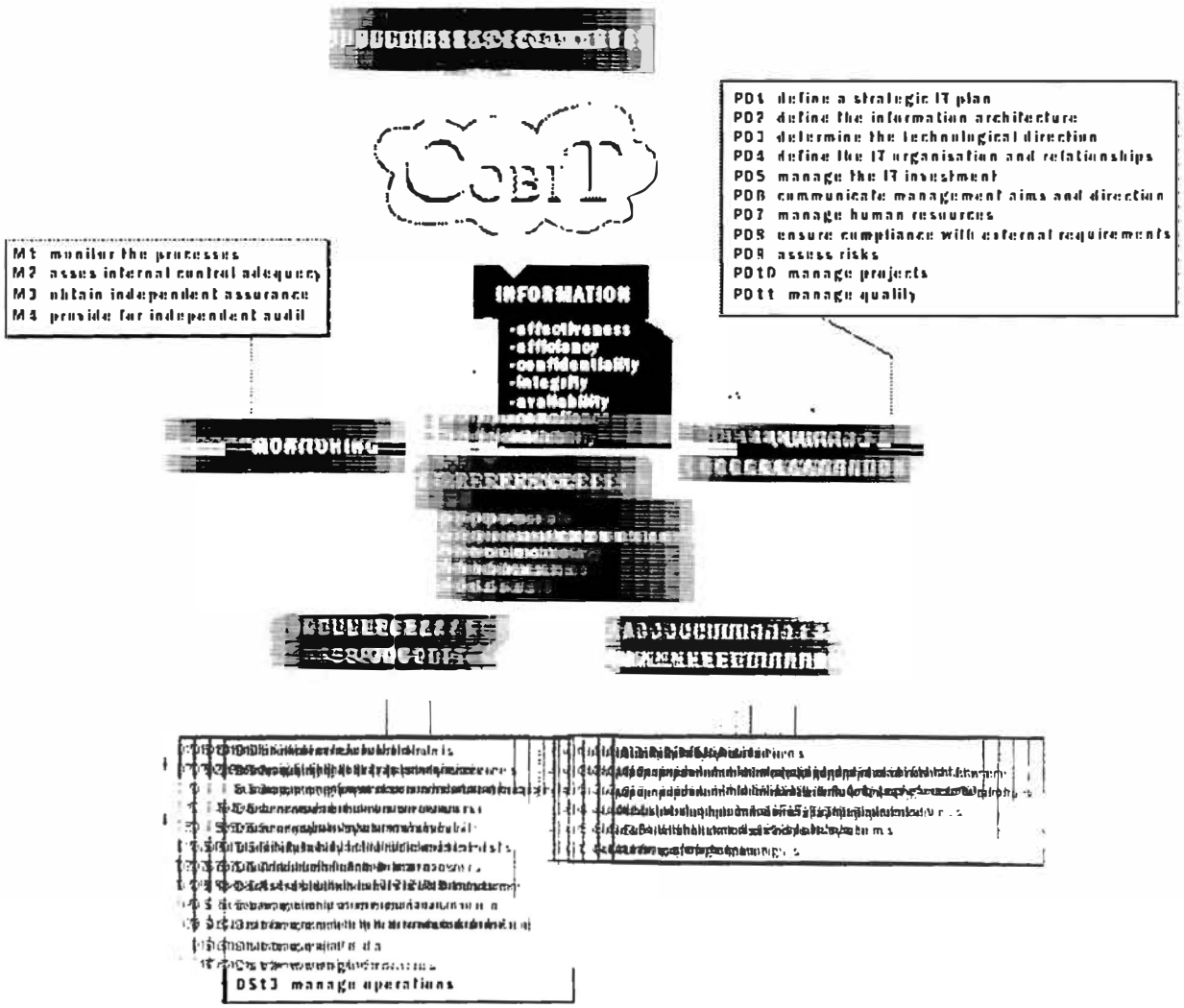
Adquisición e Implementación. La implementación de la estrategia de tecnología de información requiere la identificación, desarrollo o adquisición de soluciones de tecnología de información, y además su integración en los procesos de negocio. Además se consideran en este dominio los cambios y mantenimiento en los sistemas existentes.

Entrega y Soporte. Este dominio se refiere a la entrega real de los servicios requeridos, los cuales abarcan desde las operaciones tradicionales, aspectos de seguridad y continuidad, hasta el entrenamiento y la capacitación. Este dominio incluye además el procesamiento real de los datos por los sistemas de aplicación de la empresa.

Monitoreo. Todos los procesos de tecnología de información requieren ser analizados de manera regular con el fin de determinar la calidad de su desempeño y el cumplimiento de los requerimientos de control.

En el gráfico de la página siguiente se presenta la interrelación entre estos dominios.

LOS CUATRO DOMINIOS DEL COBIT



COBIT - Control Objectives for Information and related Technology

PROCESOS DE TECNOLOGIA DE INFORMACION EN LOS CUATRO DOMINIOS

Dominio : Planeamiento y Organización
PO1 Definir un plan estratégico de tecnología de información
PO2 Definir la arquitectura de información
PO3 Determinar la dirección tecnológica
PO4 Definir la organización y las relaciones
PO5 Administrar las inversiones
PO6 Comunicar los objetivos y dirección de la gerencia
PO7 Administrar los recursos humanos
PO8 Asegurar el cumplimiento con los requerimientos externos
PO9 Evaluar los riesgos
PO10 Administrar proyectos
PO11 Administrar calidad

Dominio : Adquisición e Implementación
AI1 Identificar soluciones automatizadas
AI2 Adquirir y mantener software de aplicación
AI3 Adquirir y mantener la infraestructura tecnológica
AI4 Desarrollar y mantener procedimientos
AI5 Instalar y acreditar sistemas
AI6 Administrar los cambios

Dominio : Entrega y soporte
DS1 Definir niveles de servicio
DS2 Administrar los servicios de terceros
DS3 Administrar el rendimiento y la capacidad
DS4 Asegurar un servicio continuo
DS5 Asegurar la seguridad de los sistemas
DS6 Identificar y atribuir costos
DS7 Educar y entregar a los usuarios
DS8 Asistir a los clientes
DS9 Administrar la configuración
DS10 Administrar problemas e incidentes
DS11 Administrar datos
DS12 Administrar equipos e instalaciones
DS13 Administrar operaciones

Dominio : Monitoreo
M1 Monitorear los procesos
M2 Evaluar la adecuación del control interno
M3 Obtener aseguramiento independiente
M4 Obtener una auditoría independiente

Además de los 34 procesos identificados, el proyecto COBIT identificó entre 4 a 18 objetivos de control asociados a cada uno de los procesos. Los objetivos de control establecen declaraciones de resultados o propósitos deseados a ser alcanzados mediante la implementación de procedimientos de control específicos dentro de las actividades que forman parte de alguno de los procesos de tecnología de información identificados.

Así por ejemplo, los objetivos de control asociados al primer proceso del dominio "Planeamiento y Organización", son los siguientes:

Dominio: Planeamiento y Organización
Proceso: Definir un plan estratégico de tecnología de información

Objetivos de control asociados:

1. La gerencia general es responsable de desarrollar e implementar planes de largo y corto plazo que permitan alcanzar la misión y las metas de la organización. Al respecto, la gerencia general debe asegurarse que tanto los temas relacionados con la tecnología de información, así como las oportunidades que ésta brinda son evaluadas adecuadamente y consideradas en los planes de la organización de largo y corto plazo.

2. La gerencia de sistemas es responsable de desarrollar regularmente planes de largo plazo relacionados al uso de la tecnología de información en la empresa, de tal manera que se soporte el logro de la misión y las metas de la organización. En tal sentido, la gerencia de sistemas debe implementar un proceso de planeamiento de largo plazo del uso de tecnología de información, utilizar un enfoque estructurado y metodológico, y establecer una estructura estandarizada del plan.

3. La gerencia de sistemas debe asegurarse que exista un proceso para modificar oportunamente el plan de largo plazo del uso de tecnología de información, con el fin de adecuarse a los cambios en el plan de largo plazo de la organización, y cambios en el entorno de tecnología de información.

4. La gerencia de sistemas debe asegurarse que el plan de largo plazo del uso de tecnología de información es traducido regularmente en planes de corto plazo. Tales planes de corto plazo deben asegurar que los recursos de tecnología de información son utilizados de manera consistente con el plan de largo plazo.

De esta manera, se han identificado en conjunto más de 300 objetivos de control, cada uno de los cuales se encuentra asociado a alguno de los 32 procesos de tecnología de información identificados. Este conjunto de objetivos de control brinda una referencia de buenas prácticas que permite guiar el desarrollo de una adecuada política de control en los procesos de tecnología de información.

Debe señalarse, además, que siguiendo el esquema proporcionado por el COBIT, el riesgo en los sistemas de información se produce cuando un objetivo de control asociado a alguno de los procesos de tecnología de información identifcado no es alcanzado. En tal sentido, el esquema del COBIT, siguiendo las técnicas del control interno y del estándar COSO, sugiere implementar actividades de control que permitan asegurar que los objetivos de control sean cumplidos y, como consecuencia de ello, mitigar los riesgo existentes.

Guías de Auditoría de COBIT

El COBIT proporciona asimismo un conjunto de Guías de Auditoría, que consiste en una estructura de controles de auditoría basados en prácticas generalmente aceptadas, que permite evaluar la adecuación y cumplimiento de los controles establecidos para cada uno de los 32 procesos identificados en el esquema general del COBIT.

La guía establece que los procesos de tecnología de información deben ser auditados mediante los siguientes pasos:

a) *Obtener un entendimiento* de los riesgos relacionados a los requerimientos del negocio, así como de las medidas de control relevantes.
b) *Evaluar la adecuación* de los controles establecidos.
c) *Evaluar el cumplimiento*, probando que los controles establecidos se estén cumpliendo, como se había definido, de manera consistente y continua.
d) *Sustentar el riesgo* de no alcanzar los objetivos de control, utilizando técnicas analíticas y/o fuentes alternativas de consulta.

6.3. La Metodología de Análisis de Riesgos en los Sistemas de Información de la Reserva Federal de Estados Unidos

La supervisión bancaria que se realiza en los Estados Unidos utiliza el concepto de *supervisión basada en el riesgo*, el cual se aplica en todas las actividades de supervisión realizadas, incluyendo la revisión de los sistemas de información de las empresas supervisadas. Este enfoque se utiliza para la selección de las entidades que serán visitadas, eligiendo aquellas con condiciones o perfiles de alto riesgo (por su dimensión o complejidad), y a la vez, es utilizado para desarrollar la estrategia de supervisión para cada entidad.

Análisis de riesgos

Con el fin de aplicar el concepto de supervisión basada en riesgo en el diseño de la estrategia de supervisión para una entidad en particular, se realiza previamente un análisis de riesgos. Este análisis incluye la evaluación de cuatro aspectos relacionados al *riesgo de transacción* (riesgos asociados a la distribución de servicios de información para soportar los procesos operativos de negocio y los procesos de toma de decisiones). Estos aspectos son los siguientes:

Cantidad de riesgo.- Se refiere al nivel o volumen de riesgo presente. Está relacionado con el volumen de transacciones y la complejidad de los sistemas de información. Este puede ser alto, moderado o bajo.

Calidad de la administración del riesgo.- Se refiere a qué tan bien los riesgos son identificados, entendidos y controlados. La evaluación previa determina si esta calidad es débil, aceptable o fuerte.

Riesgo agregado.- Esta evaluación es un resumen que incorpora los dos aspectos anteriores: la cantidad de riesgo y la calidad de la administración del riesgo. Permite al examinador ponderar la importancia relativa de cada factor para una institución dada y dirigir actividades específicas y recursos de acuerdo a la estrategia de supervisión. Sus categorías son: alto, moderado y bajo. Esto puede apreciarse de mejor manera con una Matriz de Riesgo Agregado:

Calidad de la administración del riesgo	Bajo	Moderado	Alto
Débil	Moderado	Alto	Muy Alto
Aceptable	Bajo	Moderado	Alto
Fuerte	Muy Bajo	Bajo	Moderado

Cantidad de Riesgo

Dirección.- Este aspecto refleja la visión del examinador acerca de los cambios probables del perfil de riesgo de la empresa hasta el siguiente ciclo de supervisión.

La dirección puede ser expresada como descendente, estable o ascendente. Una dirección descendente indica que el examinador anticipa, basado en información actual, que el riesgo agregado disminuirá en los siguientes 12 meses. Una dirección estable indica que el examinador anticipa que el perfil de riesgo agregado se mantendrá sin cambios, mientras que una dirección ascendente indica que el examinador anticipa que dicho perfil aumentará en los siguientes 12 meses.

Este análisis de riesgos permite diseñar la estrategia de supervisión específica para cada entidad. El diseño de esta estrategia incluye la definición de los objetivos y los planes de trabajo a ser ejecutados durante la revisión, los cuales deben enfatizar aquellas áreas donde la empresa se encuentre más expuesta a los riesgos de transacción.

Areas funcionales de Sistemas de Información y su calificación

Las revisiones de sistemas de información incluyen la determinación de una calificación para cuatro áreas funcionales de sistemas de información: Auditoría, Gerencia, Desarrollo y Programación de Sistemas, y Operaciones. La calificación global varía de 1 a 5, donde 1 representa la mejor calificación, y 5 la peor. Para determinar esta calificación global, se consideran las interrelaciones y la importancia relativa de las cuatro áreas funcionales señaladas. Ocasionalmente, pueden existir factores que no se encuentren debidamente reflejados en las cuatro áreas y que, sin embargo, sean importantes para la determinación de la calificación global. En estos casos, se incluyen estos aspectos directamente sobre la calificación global con las notas explicativas correspondientes.

Cada área funcional es de igual manera calificada de 1 a 5, donde 1 es la calificación más alta y 5 la más baja. Cada calificación tiene el siguiente significado:

Calificación: 1 - Desempeño fuerte
El desempeño del área funcional es significativamente mayor que el promedio.

Calificación: 2 - Desempeño satisfactorio

El desempeño del área funcional se encuentra en el promedio o ligeramente superior, y es adecuado para el funcionamiento sólido y seguro del Area de Sistemas de Información

Calificación: 3 - Desempeño regular

El desempeño del área funcional es considerado de menor nivel que el promedio.

Calificación: 4 - Desempeño insatisfactorio

El desempeño del área funcional se encuentra significativamente por debajo del promedio y si se deja sin revisión, puede convertirse en una debilidad que amenace la integridad de los datos procesados y el funcionamiento adecuado del Area de Sistemas de Información

Calificación: 5 - Desempeño riesgoso

El desempeño del área funcional es críticamente deficiente y requiere ser atendido de inmediato. Este desempeño amenaza el funcionamiento apropiado del Area de Sistemas de Información.

Los principales aspectos que se revisan en cada área funcional son los siguientes:

Auditoría	**Gerencia**	**Desarrollo y Prog. de Sistemas**	**Operaciones**
• Visión • Independencia y Personal • Actividades de auditoría interna/externa • Seguimiento • Documentación	• Efectividad • Corrección de Deficiencias • Cump. Normativo • Planeam. y Dirección • Programa Corporativo de Seguridad de Información	• Organización • Personal • Estándares y Procedimientos • Documentación • Controles Internos • Seguridad Física	• Organización • Personal • Estándares y Procedimientos • Operaciones

• Software	• Planeamiento Corporativo de Contingencias • Estándares y Procedimientos • Controles Internos • Seguridad Física • Sistemas de Información Gerencial • Condición Financiera		

La revisión de cada área funcional se realiza siguiendo una guía de procedimientos detallada denominada 'Workprogram', en la cual se señalan los ítems específicos que deben ser considerados en dichas revisiones. Así por ejemplo, para la revisión del rubro 'Independencia y Personal' dentro del área de Auditoría deben considerarse tres ítems:

Independencia y Personal

1. Determinar si el orden jerárquico de la función de auditoría de sistemas es independiente en apariencia y en realidad, revisando el grado de control que las personas fuera de la función de auditoría tienen en el Directorio o en el Comité de Auditoría.
2. Revisar la estructura organizativa de la unidad auditoría interna y determinar la independencia y claridad de responsabilidades de la unidad.
3. Determinar si el personal de auditoría de sistemas es adecuado en número y tiene competencia técnica para cumplir sus funciones:
   a. Revisar las calificaciones del personal y compararlo con las habilidades requeridas para el puesto.
   b. Determinar si la competencia del personal es adecuada con la tecnología usada en la institución.
   c. Revisar el presupuesto asignado a las labores de auditoría de sistemas y discutir con la gerencia de auditoría la adecuación de los niveles actuales de personal, rotación y capacitación.

6.4. El Modelo MAGERIT del Consejo Superior de Informática de España

El Consejo Superior de Informática de España ha elaborado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, MAGERIT, cuya utilización promueve, como respuesta a la dependencia creciente de las instituciones públicas (y en general de toda la sociedad) respecto a la tecnología de información. El desarrollo de MAGERIT ha tomado como referencia:

- Los Criterios ITSEC (Information Technology Security Evaluation Criteria) de la Comunidad Europea.
- Los Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información, elaborados por la Unión Europea, Estados Unidos y Canadá.

La metodología contiene dos tipos de elementos:

- Un conjunto de Guías, compuesto básicamente por:
  - Guía de Aproximación
  - Guía de Procedimientos
  - Guía de Técnicas
  - Guía para Desarrolladores de Aplicaciones
  - Guía para Responsables del Dominio protegible
  - Referencia de Normas legales y técnicas
- Un panel de herramientas de apoyo, con sus correspondientes Guías de Uso y con la Arquitectura de Información y Especificaciones de la Interfaz para el Intercambio de datos.

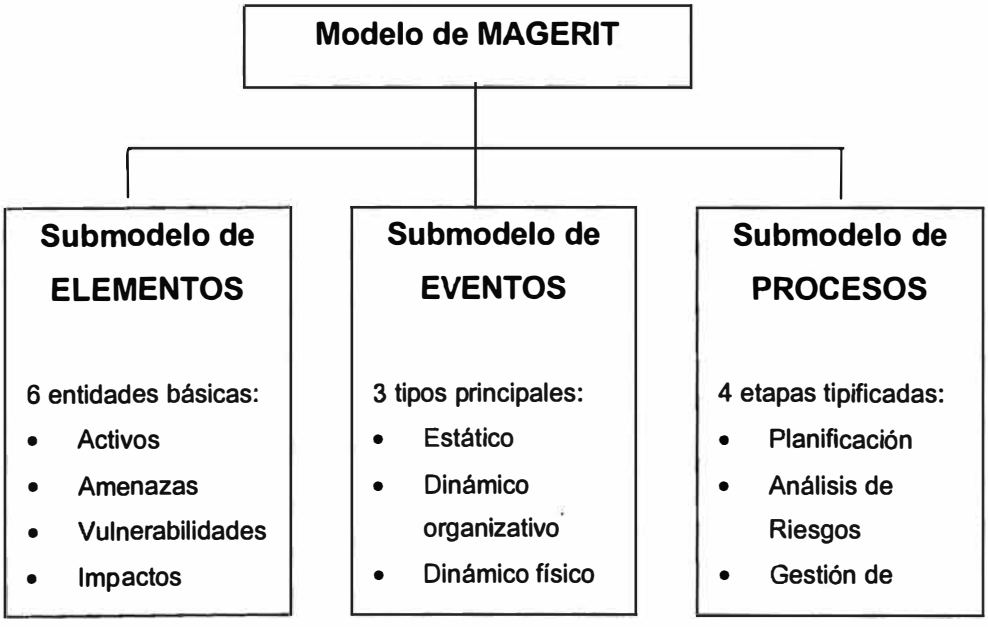
Esta estructura de MAGERIT permite realizar:

- El **análisis de los riesgos** para identificar las amenazas, a las que se encuentran expuestos los distintos componentes pertenecientes o relacionados con los sistemas de información (conocidos como 'activos'); para determinar la vulnerabilidad de los sistemas ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

- La **gestión de los riesgos**, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Componentes del Análisis y Gestión de Riesgos según MAGERIT

El modelo sobre el cual se ha desarrollado MAGERIT comprende tres submodelos, los cuales son señalados en el siguiente esquema:



Submodelo de Elementos

MAGERIT contiene 6 entidades básicas (cada una dotada de ciertos atributos y relacionadas con las otras). Estas entidades son los activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.

Activos.- Son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Incluye el entorno del sistema de información necesario para su funcionamiento (instalación física, infraestructura de comunicaciones, suministros, personal, etc.), el sistema de información en sí (hardware, sistemas operativos, utilitarios, aplicaciones, etc.), la propia información, las funcionalidades de la organización que dan finalidad a la existencia de los sistemas de información y activos intangibles.

Amenazas.- Son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en los activos de la empresa.

Vulnerabilidad.- Es la de potencialidad de materialización (ocurrencia real) de una amenaza sobre un activo. Es el mecanismo de paso desde la amenaza a la agresión materializada.

Impacto.- Es el daño producido a la organización por un posible incidente y es el resultado de una agresión sobre el activo. El impacto puede ser cuantitativo (si representa pérdidas cuantitativas monetarizables directas o indirectas), cualitativo con pérdidas orgánicas y cualitativo con pérdidas funcionales.

Riesgo.- Es la posibilidad de que se produzca un impacto dado en la organización. Es un indicador resultante de la combinación de la vulnerabilidad y el impacto que procede de la amenaza actuante sobre el activo. Este riesgo calculado permite

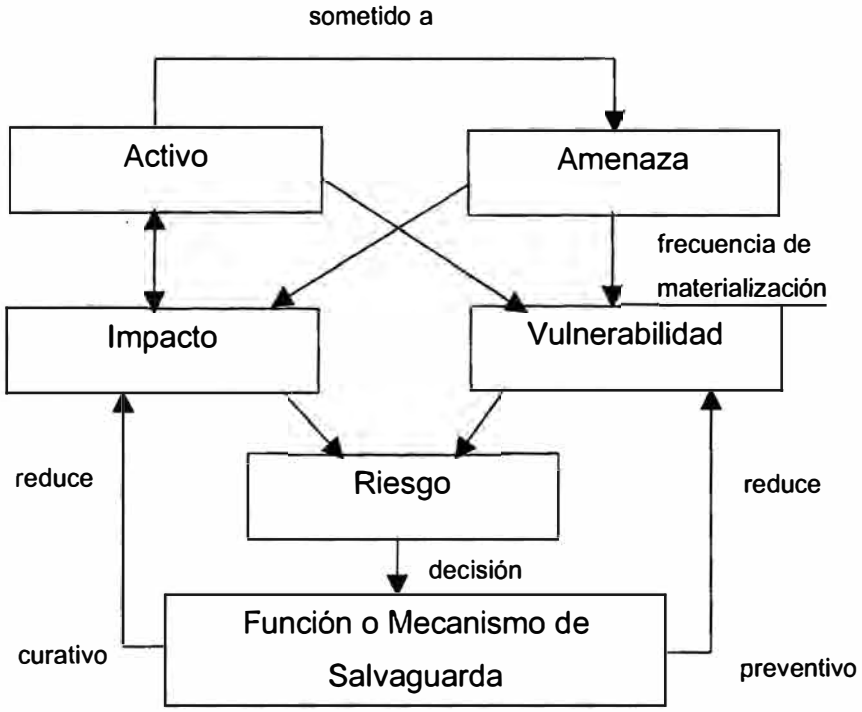
tomar decisiones racionales para cumplir con el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con un 'umbral de riesgo' definido por la organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un riesgo residual que se considera asumible.

Funciones y mecanismos de salvaguarda.- Una función o servicio de salvaguarda consiste en una acción destinada a reducir un riesgo de tipo actuación u omisión. Esta actuación se concreta en un mecanismo de salvaguarda que opera de dos formas:

- *La salvaguarda preventiva* ejerce acción sobre la Vulnerabilidad, 'neutralizando' otra acción, la materialización de la amenaza, antes de que actúe ésta.
- *La salvaguarda curativa* actúa sobre el Impacto, modificando el estado de seguridad del activo agredido y reduciendo el resultado de la agresión; o sea después de ésta.

Submodelo de Eventos

El submodelo de eventos, en su vista 'estática', contiene una representación de las relaciones generales existentes entre las 6 entidades reseñadas en el Submodelo de Elementos, como se puede ver en la figura siguiente.



Submodelo de Procesos de Seguridad

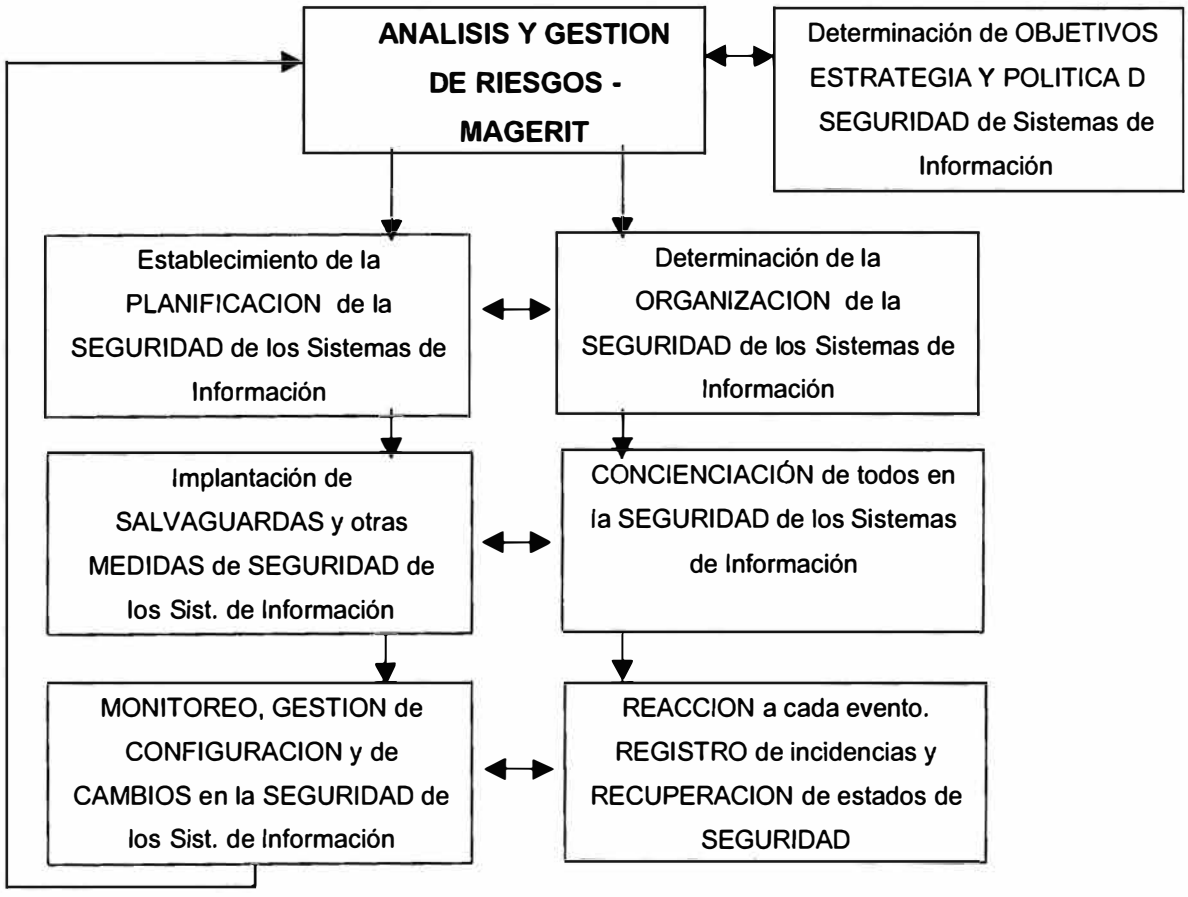
Este submodelo comprende cuatro etapas:

a. ***Planificación del Proyecto de Riesgos.-*** Se definen los objetivos que ha de cumplir y el ámbito que abarcará el proyecto, se planifican los medios materiales y humanos para su realización, entre otras actividades.
b. ***Análisis de riesgos.-*** Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
c. ***Gestión de riesgos.-*** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones.

d. ***Selección de salvaguardas.-*** Se prepara el plan de implantación de salvaguarda elegidos y los procedimientos de seguimiento para la implantación.

Gestion Global de la Seguridad de un Sistema de Información

Siguiendo el esquema planteado por MAGERIT, la gestión global de la seguridad de un sistema de información es una acción permanente, cíclica y recurrente (es decir, se ha de reemprender continuamente debido a los cambios en el sistema y en su entorno), que se descompone en diferentes fases, tal como se grafica en el diagrama siguiente:



6.5. Otras fuentes metodológicas

Además de las fuentes metodológicas descritas en las secciones anteriores, debe señalarse que las cinco compañías de consultoría de negocios más importantes a nivel mundial (conocidas como las 'Big-Five') han desarrollado sus propias metodología de análisis de riesgos en los sistemas de información, las cuales son utilizadas en los servicios de consultoría que ofrecen estas empresas alrededor del mundo. Estas cinco empresas son: Arthur Andersen, Deloitte and Touche, Ernst & Young, KPMG y PriceWaterhouseCoopers. Las metodologías desarrolladas por estas empresas, sin embargo, no son públicas, dado que constituyen parte de su know-how, y como tal determinan en cierta medida su ventaja competitiva al ofrecer estos servicios.

A pesar de ello, describiremos brevemente la naturaleza de los servicios ofrecidos por tres de estas consultoras, a partir de la información publicada en sus respectivos sitios web.

A. Arthur Andersen - Computer Risk Management **(http://www.arthurandersen.com/crm)**

Considerando la importancia de entender y administrar proactivamente el conjunto de riesgos de negocio derivados del uso de la tecnología de información, Arthur Andersen constituyó la unidad de Computer Risk Management, a través de la cual ofrece servicios de consultoría para el análisis de dichos riesgos, y permite a las organizaciones mejorar el desempeño de sus procesos de negocio. Los servicios específicamente ofrecidos por esta consultora incluyen las siguientes áreas:

a. Seguridad de Redes y de la Información
b. Planeamiento de la Continuidad del Negocio
c. Administración del Riesgo de Sistemas de Negocio

d. Administración de Recursos de Infraestructura
e. Minería de Información de Negocio
f. Consultoría en Riesgos del Comercio Electrónico
g. Computación Cliente/Servidor

B. PriceWaterhouseCoopers - Operational & Systems Risks Management Solutions

(http://www.pwcglobal.com)

A través de la Unidad de *Global Risk Management Solutions*, PriceWaterhouseCoopers ofrece un conjunto de servicios de consultoría para asistir a las empresas en la administración de los riesgos a los que se encuentran expuestas. Uno de estos servicios está relacionado con la administración de riesgos operacionales y de sistemas (*Operational & Systems Risks Management Solutions*), área en la cual se ofrecen los siguientes servicios:

A. *Servicios de Control y Aseguramiento.*- Incluye tanto el diseño e implementación de controles en proyectos de implementación de sistemas de información integrales (p.ej. un sistema ERP como SAP), como también en la provisión de controles independientes con el fin de confirmar que los controles actuales se encuentren operando normalmente.
B. *Servicios de Análisis de Riesgos Operacionales.*- Incluye servicios de Planeamiento de la Continuidad del Negocio, Administración y Medición de Riesgos Operacionales, Revisión de los Procesos Financieros, Administración del Valor de la TI, entre otros.
C. *Servicios de Análisis de Riesgo Tecnológico.*- Incluye servicios de Protección de Recursos, Redes y Telecomunicaciones, y Soporte Técnico en Comercio Electrónico.
D. *Servicios de Desarrollo (Deployment Services).*- Incluye servicios de Selección e Implementación de Paquetes, así como de Administración de Datos. Este último

servicio se encuentra mayormente dirigido hacia la recolección y procesamiento de grandes cantidades de información crítica para la empresa.

C. Deloitte & Touche - Enterprise Risk Services

(http://www.us.deloitte.com/risk)

La Unidad de *Enterprise Risk Services* de Deloitte & Touche ofrece un conjunto de servicios a las empresas relacionadas con el análisis de riesgos de negocio a las cuales se encuentran expuestas. Algunos de estos servicios, se encuentran relacionados con los riesgos en los sistemas de información. Así por ejemplo, se ofrecen los siguientes servicios:

a. Planeamiento de la Continuidad del Negocio
b. Seguridad en Negocios Electrónicos
c. Infraestructura para Computación Distribuida
d. Aseguramiento de la Calidad en Proyectos

Al igual que en las demás consultoras, Deloitte & Touche ofrece estos servicios a nivel mundial, y publica en su sitio web algunos documentos de interés sobre estos temas, sin embargo la metodología desarrollada para sus estudios de consultoría no es publicada.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El estudio realizado con el objetivo de diseñar una metodología de análisis de riesgos en los sistemas de información para una empresa bancaria, nos ha permitido concluir lo siguiente:

1. Las empresas bancarias hacen un uso cada vez más intensivo de la tecnología de información, en sus diferentes aplicaciones. Durante el estudio se identificaron cuatro grandes aplicaciones de esta tecnología:

    a. La automatización de las operaciones bancarias (Captaciones, colocaciones, tesorería, administración de agencias, etc.).
    b. El soporte a la toma de decisiones tácticas y estratégicas, a través de herramientas OLAP (análisis multidimensional), la construcción de almacenes centralizados de datos (data warehouse), técnicas de minería de datos, sistemas de información gerencial, entre otras herramientas.
    c. El desarrollo de la banca electrónica, que ha permitido generar nuevos canales de distribución de servicios bancarios (cajeros automáticos, puntos de venta, banca telefónica, banca por Internet, etc.)
    d. El comercio electrónico, que constituye una aplicación de uso muy reciente, y que en el Perú aún se encuentra en su etapa inicial.

2. El uso cada vez más intensivo de la tecnología de información ha traido como consecuencia una creciente dependencia de las empresas bancarias en la

confiabilidad de sus sistemas de información para el procesamiento de sus operaciones diarias. Esta dependencia significa que las empresas bancarias se encuentran expuestas de manera significativa a los riesgos asociados al uso de la tecnología de información (o riesgos en los sistemas de información). Estos riesgos pueden significar finalmente importantes pérdidas financieras o reducción en las utilidades de la empresa debido, por ejemplo, a robo de información confidencial, accesos no autorizados a sus sistemas de cómputo centrales, fraudes electrónicos, importantes proyectos de desarrollo e implementación de sistemas de información fracasados, paralización de operaciones debido a problemas en su computador central, etc.

3. Frente a esta posibilidad, es necesario contar con una metodología que permita analizar de manera sistemática los riesgos en los sistemas de información a los que se encuentra expuesta la empresa, e identificar posibles deficiencias y vulnerabilidades que deben ser corregidas y subsanadas adecuadamente.

4. Se ha identificado diez áreas de riesgo en los sistemas de información en las empresas bancarias, las mismas que han sido agrupadas en 4 dominios. Estas áreas de riesgo se detallan a continuación:

Dominio I: Planeamiento y Organización	**Dominio II: Adquisición, Desarrollo e Implementación**	**Dominio III: Operaciones**	**Dominio IV: Monitoreo y control interno**
• Planeamiento estratégico • Organización del departamento de SI	• Adquisición e implementación • Desarrollo y mantenimiento • Implementación de SI integrales	• Seguridad de información • Continuidad operacional • Banca electrónica y el uso de Internet	• Control de Gerencia • Revisiones de Auditoría Interna y Externa

El modelo de análisis elaborado considera asimismo que cada una de estas áreas de riesgo se encuentra asociada a un proceso genérico de tecnología de información. El riesgo en los sistemas de información se encuentra directamente asociado al incumplimiento de los objetivos de estos procesos. Frente a ello, deben implementarse actividades de control que permitan administrar adecuadamente estos riesgos.

5. La metodología diseñada toma como base este modelo de análisis y considera seis fases para el análisis y evaluación de los riesgos en los sistemas de información de la empresa. Estas seis fases son las siguientes:
    a. Inicio
    b. Identificación de riesgos
    c. Evaluación de actividades de control
    d. Medidas correctivas
    e. Calificación
    f. Reporte final

6. Un estudio de análisis de riesgos en los sistemas de información de una empresa bancaria debe iniciarse con la obtención de información general de la empresa, que permita identificar aspectos significativos de la estrategia de negocio de la empresa, así como de su infraestructura tecnológica (*Fase I: Inicio*). Estos aspectos incluyen :

    a. Principales líneas de negocio de la empresa.
    b. Procesos críticos de negocio
    c. Puesto en el ranking del sistema bancario por colocaciones, depósitos y patrimonio
    d. Número de agencias y distribución de las mismas
    e. Hechos de importancia ocurridos en la empresa durante los últimos 6 meses (cambios en la estrategia de negocio, desarrollo de nuevos

productos financieros, cambios en el directorio y/o en gerencias, posibles fusiones o adquisiciones por ser realizadas, etc.)

f. Infraestructura tecnológica de la empresa, (hardware, sistemas operativos, manejadores de bases de datos, lenguajes de programación utilizados)
g. Arquitectura de sistemas de información que soporta los procesos de negocio de la empresa.
h. Dispositivos de banca electrónica utilizados y arquitectura tecnológica que lo soporta.
i. Organización del departamento de sistemas de información de la empresa y su ubicación dentro del organigrama general de la empresa.

7. Luego de obtener información general de la empresa, el análisis de riesgos en los sistemas de información debe continuar por la identificación de riesgos. Para la ejecución de esta actividad, se ha elaborado el modelo de análisis descrito en el numeral 4. Asimismo es necesario definir que áreas de riesgo serán evaluadas durante el estudio. Esta definición debe tomar en consideración que deberían destinarse más recursos durante la evaluación a aquellas áreas que representen un mayor riesgo para la empresa (*Fase II: Identificación de riesgos*).

8. Una vez definido el alcance del estudio, el análisis de riesgos debe continuar con la evaluación de las actividades de control implementadas por la empresa. Esta evaluación debe enfocarse en la adecuación y cumplimiento de dichas actividades de control, identificando posibles vulnerabilidades o deficiencias de control (*Fase III: Evaluación de actividades de control*).

9. Como resultado del análisis de riesgos efectuado deben proponerse medidas correctivas para la adecuada administración de los riesgos en sistemas de información, de acuerdo a las deficiencias de control identificadas (*Fase IV: Medidas correctivas*).

10. El análisis de riesgos debe concluir con una calificación del riesgo en los sistemas de información a nivel de la empresa. La utilidad de esta calificación es que permite resumir en un solo calificativo los resultados de la evaluación efectuada en la empresa (*Fase V: Calificación*).

11. Se ha identificado tres metodologías internacionales sobre el tema en estudio, que han servido como fuentes de referencia importantes para el diseño de la metodología propuesta. Estas tres metodologías son las siguientes:

    a. Modelo COBIT de la Asociación ISACA (Information Systems Audit and Control Association).
    b. MAGERIT (Metodología de Análisis y Gestión de Riesgos en los Sistemas de Información) del Consejo Superior de Informática de España.
    c. Modelo de Análisis de Riesgos en Sistemas de Información de la Reserva Federal de Estados Unidos.

12. En particular, el COBIT constituye un esfuerzo importante emprendido por la Asociación Internacional de Auditores de Sistemas de Información (ISACA), con el fin de elaborar un estándar para el control en los procesos de tecnología de información.

Recomendaciones

Luego de haber desarrollado el presente estudio, que tuvo como resultado la elaboración de una Metodología de Análisis de Riesgos en los sistemas de información de una empresa bancaria, se proponen las siguientes recomendaciones:

1. Cualquier estudio de análisis de riesgos en sistemas de información debe considerar la naturaleza de la empresa evaluada, su estrategia de negocio, las características de su organización y del sector al cual pertenece.

2. El uso de la metodología propuesta por los Gerentes o Auditores de Sistemas de las empresas bancarias, permitirá una mejor administración de los riesgos asociados a los sistemas de información, a los que se encuentran expuestas estas empresas. En el primer caso, permitirá una auto-evaluación y la identificación de medidas correctivas y áreas de mejora. En el segundo caso permitirá igualmente la identificación de deficiencias de control y de las medidas correctivas correspondientes.

3. Se recomienda adicionalmente el uso de la Metodología propuesta por los supervisores bancarios. Los procedimientos de supervisión bancaria propuestos por el Comité de Basilea se encuentran orientados bajo la denominada Supervisión por Riesgos, la cual se basa en dirigir los esfuerzos de supervisión hacia los riesgos del negocio bancario, entre los que se incluyen los riesgos tecnológicos o riesgos asociados al uso de la tecnología de información. En ese sentido, la Metodología propuesta se encuentra orientada bajo esta perspectiva y permitiría guiar a los supervisores bancarios en las revisiones de los sistemas de información de las empresas bancarias que se realizan en sus exámenes ordinarios y especiales.

4. Si bien la metodología planteada se ha desarrollado para empresas bancarias, existen muchos aspectos que pueden ser utilizados para empresas de otros sectores económicos. La mayoría de las áreas de riesgo identificadas existen en cualquier empresa industrial, comercial o de servicios. Con un esfuerzo adicional de adaptación, la metodología propuesta puede ser aplicada en dichas empresas.

5. La identificación y evaluación de riesgos es un proceso dinámico, y debe ser retroalimentado no solo con los resultados del análisis efectuado, sino sobretodo considerando las condiciones cambiantes del entorno empresarial. En tal sentido, la importancia que se asigne a cada una de las áreas de riesgo identificada debe ser evaluada continuamente. Inclusive podrían surgir nuevas áreas de riesgo, o algunas subdividirse, de acuerdo a su importancia en el negocio. En particular, el comercio electrónico debería derivar en una nueva área de riesgo, conforme la cantidad de transacciones realizadas en número de clientes y monto transado sean lo suficientemente importantes.

6. El esquema de calificación propuesto en la Metodología se basa principalmente en el criterio del analista, el cual debe proponer una calificación en base a los resultados del análisis. Sin embargo, es posible desarrollar un esquema semi-automático de calificación basado en puntajes. Así por ejemplo, para un área de riesgo determinada, podría establecerse que cada uno de los criterios propuestos en la Guía de evaluación respectiva otorgue un determinado puntaje. La suma ponderada de puntajes, daría el puntaje del área, y a través de un esquema de rangos, se obtendría la calificación del área. Una de las ventajas de este esquema es que no se dependería excesivamente del criterio del analista.

BIBLIOGRAFIA

AMBROSINI, David

1997 **Introducción a la banca.**
Lima, Universidad del Pacífico. 1ª.ed.

ARANGO SOFTWARE INTERNATIONAL

1997 **Soluciones Financieras Integradas**
Panamá, 1ª.ed.

BASLE COMMITTEE ON BANKING SUPERVISION

1998 **Framework for the evaluation of internal control systems**
Basle - Suiza, 1998

1998 **Risk management for electronic banking and electronic money activities**
Basle - Suiza, 1998

BLACHARSKI, Dan

1998 **Network security in a mixed environment**
IDG Books Worldwide, Inc. USA 1998.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

1998 **Assesment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations**
Washington, D.C. SR 98-9. Abril 1998.
http://www.bog.frb.fed.us/boarddocs/SRLETTERS/1998/SR9809.htm

BRINKWORTH, John W.O.

1992 **Software Quality Management. A pro-active approach.**
Prentice Hall International Ltd. 1992. pp.139-158

CONSEJO SUPERIOR DE INFORMATICA DE ESPAÑA

1995 **MAGERIT versión 1.0 - Guía de Aproximación a la Seguridad de los Sistemas de Información**
Consejo Superior de Informática - Ministerio de Administraciones Públicas. Madrid, España.

CORDERO ROSADO, Antonio y Luis VALENCIA PALACIOS

1996 **Aspectos de seguridad en los servicios bancarios por Internet**
Trabajo de Investigación preparado para la Primera Feria de Tecnología organizada por la Universidad Privada de Santa Cruz de la Sierra - Bolivia.
Lima, Noviembre 1998.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATIONS COUNCIL

1997 **FFIEC Information Systems Examination Handbook**
1996 Edition. Washington, D.C.

GARCIA-CANTERA, José A.

1996 **Peruvian Banking System. It's a new game...Who's prepared?**
Salomon Brothers

GOLDFINGER, Charles

1996 **Electronic Money in the United States: Current Status, Prospects and Major Issues**
European Commission - Electronic Commerce Team.
Bruselas, Setiembre 1996.
http://www.ispo.cec.be/infosoc/eleccom/elecmoney.html

IBM BANKING SOLUTION CENTRE

1996 **Banking Data Warehouse Description**
Banking Solution Centre - IBM Ireland

IBM DEL PERU

1996 **Seguridad en Sistemas de Información**
Departamento de Educación - IBM del Perú.

IBM CORP. INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

1998 **Smart Cards: A Case Study**
IBM Corp. 1ª.ed.

IBM SOFTWARE GROUP

1996 **Business Intelligence Guide**
IBM Software Group. New York.

INFORMATION INFRASTRUCTURE TASK FORCE

1997 **A Framework for Global Electronic Commerce**
http://www.iitf.nist.gov/eleccomm/ecomm.htm
http://www.whitehouse.gov/WH/New/Commerce/index.html

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION - ISACF

1996 **COBIT Framework**

1996 **COBIT Control Objectives**

1996 **COBIT Audit Guidelines**
The Information Systems Audit and Control Foundation.
Illinois, USA.

MARION, Larry.

1990 **Feeding the Beast. ERP Success from Smart Change Management**
ERP News 1990.
http://www.erpnews.com/erpnews/erp905/02get.html

MCNAMEE, David

1996 **Assessing Risk Assessment**
MC2 Management Control Concepts, USA.
http://www.mc2consulting.com/riskart2.htm

OLAP COUNCIL

1997 **OLAP Council White Paper**
OLAP Council. 1997.
http://www.olapcouncil.org/research/whtpaply.htm

OFFICE OF THRIFT SUPERVISION

1997 **Regulatory Bulletin - Subject: Information Technology**
Section: 341 RB32-6 Octubre 1997.

RODRIGUEZ ULLOA, RICARDO

1994 **La sistémica, los sistemas blandos y los sistemas de información**
Lima, Universidad del Pacífico. 1ª.ed.

SAUNDERS, Anthony

1997 **Financial Institutions Management: A Modern Perspective**
Irwin / McGraw-Hill. 2ª.ed.

SENN, James A.

1992 **Análisis y diseño de sistemas de información**
México D.F., McGraw-Hill Interamericana de México. 2ª.ed.

SISTI, Frank J. y Sujoe JOSEPH

1994 **Software Risk Evaluation Method Version 1.0**
Technical Report CMU/SEI-94-TR-19.
Software Engineering Institute.
Carnegie Mellon University. Pittsburgh, Pennsylvannia 15213

SIYAN, Karanjit y Chris HARE.

1997 **Firewalls y la Seguridad en Internet.**
México D.F. Prentice-Hall Hispanoamericana. 2ª.ed.

STONER, James A.F. y R.Edward FREEMAN

1994 **Administración**
México. Prentice-Hall Hispanoamericana.

SUPERINTENDENCIA DE BANCA Y SEGUROS

1998 **Información Financiera Mensual al 30 de Abril de 1999.**

1996 **Ley General del Sistema Financiero y de Seguros y Orgánica de la Superintendencia de Banca y Seguros. Ley N° 26702.**

S.W.I.F.T.

1999 **S.W.I.F.T at a glance**
http://www.swift.com/

TAPSCOTT Don y Art CASTON

1995 **Cambio de paradigmas empresariales**
Versión en español de: "Paradigm Shift.The New Promise of Information Technology" (1993).
McGraw-Hill Interamericana S.A. 1ª.ed. Bogotá 1995.

THE UNIVERSITY OF TEXAS SYSTEM

1998 **Control Self-Assessment Workshop**
The University of Texas System - System Audit Office
http://iron.utsystem.edu/home/AUD/Resource/1ses2of2.htm

UNITED STATES GENERAL ACCOUNTING OFFICE (GAO)

1992 **Information Technology: An Audit Guide for Assessing Acquisition Risks**
United States General Accounting Office - Information Management and Technology Division. GAO/IMTEC - 8.1.4. Diciembre 1992.

UNIVERSITY OF WATERLOO - INTERNAL AUDIT DEPARTMENT

1997 **Internal Controls**
University of Waterloo. Ontario, Canada.
http://www.adm.uwaterloo.ca/infoia/intcontr.html

VAN SCOY, Roger L.

1992 **Software Development Risk: Opportunity, Not Problem**
Technical Report CMU/SEI-92-TR-30.
Software Engineering Institute.
Carnegie Mellon University. Pittsburgh, Pennsylvannia 15213

VISA INTERNATIONAL

1999 **VisaCash**
http://www.visalatam.com/cgibin/vee/s_newtech/visacash/main.html
Comercio Electrónico
http://www.visalatam.com/s_newtech/commerce/main.html

APENDICES

APENDICE A

LOS RIESGOS DERIVADOS DEL PROBLEMA INFORMATICO DEL AÑO 2000

Aspectos generales

- Los alcances del problema informático del año 2000 han demostrado el grado de dependencia de las empresas con respecto al normal funcionamiento de sus sistemas de información. En particular, enfrentar esta problemática ha constituido un reto para las empresas bancarias, considerando la complejidad de sus sistemas de información, su dependencia en el uso de estos sistemas para el procesamiento normal de sus operaciones diarias, el desarrollo de la banca electrónica, así como la creciente interconexión entre los sistemas de información de las empresas del sector.

Este problema consiste básicamente en la posibilidad de un procesamiento inadecuado de las transacciones que manejen fechas durante el cambio al año 2000 y otras fechas críticas relacionadas. En todos aquellos programas o aplicaciones que manejan la fecha con un formato de 6 dígitos (dd-mm-aa), se asume que las dos primeras cifras del año son '19'. En tal sentido, llegado el 1 de enero del 2000 (01-01-00), esta fecha podría ser entendida como el 1 de enero de 1900, lo cual ocasionaría un procesamiento inadecuado de las transacciones que manejan fechas, o posibles fallas en los equipos de hardware, sistemas operativos o aplicaciones que soportan los procesos críticos de negocio de la empresa.

Un elemento adicional en esta problemática es que el año 2000 es bisiesto, lo cual podría no ser reconocido por muchos programas, dado que en muchos de ellos, sólo se han considerando las dos primeras reglas de del algoritmo del año bisiesto, según las cuales son bisiestos aquellos años múltiplos de 4, pero que no sean múltiplos de 100. En muchos programas no se considera la tercera regla del año bisiesto, la cual señala que cumpliéndose las dos reglas anteriores, son bisiestos los años múltiplos de 400.

Estrategias de solución

Una de las principales estrategias de solución del problema informático del año 2000, denominada *técnica de expansión*, consiste en expandir los datos de fecha de un formato de 6 a 8 dígitos (dd-mm-aaaa). Si bien esta estrategia proporciona una solución definitiva al problema, su implementación requiere la modificación de todos los archivos y bases de datos de la empresa que contengan datos fecha, además de los programas que manejan estos datos.

Otra estrategia, denominada *técnica de ventaneo*, consiste en incluir algoritmos que permitan interpretar los dos primeros dígitos del año de acuerdo a una determinada ventana de tiempo. Así por ejemplo, podría indicarse lo siguiente:

Año (aa)	Interpretación
50-99	1950-1999
00-49	2000-2049

La implementación de esta estrategia no requerirá mayores cambios a los archivos y bases de datos de la empresa (aunque sí será necesario en caso las fechas formen parte de un campo clave o índice). El problema de esta estrategia de solución es que se trata de una solución temporal, por lo que la empresa deberá definir que estrategia seguirá conforme la ventana de tiempo definida vaya llegando a su fin.

Características particulares del problema

Si bien es cierto, las estrategias de solución son ampliamente conocidas y, en la mayoría de los casos, sencillas de implementar, el problema informático del año 2000 tiene ciertas características particulares que aumentan su complejidad. Así por ejemplo:

1. Alcanza a todos los componentes de tecnología de información instalados en la empresa: aplicaciones internas, aplicaciones mantenidas por terceros, bases de datos y archivos, sistemas operativos, paquetes, equipos de hardware y de comunicaciones, e incluso otros equipos no informáticos con chips empotrados (bóvedas, controladores de asistencia, aire acondicionado, ascensores, etc.).

2. Tiene un plazo fijo e improrrogable para su solución. El problema debe ser solucionado y dicha solución probada y estabilizada antes del 1 de enero del 2000. Este proyecto no admite prórrogas.

3. Como todo proyecto de desarrollo o mantenimiento de sistemas de información, a pesar de la intensidad de las pruebas realizadas, es posible que existan errores que sólo puedan ser identificados en las fechas críticas reales. Frente a ello, es necesario diseñar e implementar medidas de contingencia que permitan asegurar la continuidad operativa de la empresa en caso ocurra algún problema relacionado con el tratamiento informático del cambio al año 2000.

4. Alcanza aspectos no técnicos por lo cual es necesaria la participación de las Areas de negocio de la empresa. Estos aspectos conocidos como *Riesgos de negocio*, incluyen: un incremento del riesgo crediticio de los clientes corporativos, posibles contingencias legales, riesgos de imagen y de reputación, riesgos por la variabilidad de precios en la cartera de inversión negociable de la empresa, riesgos de liquidez, etc.

5. Afecta a todas las empresas cuyos procesos de negocio se encuentran soportados por sistemas informáticos. En particular, afecta a aquellas empresas que forman parte de la cadena de valor de la organización: proveedores de servicios críticos, socios de negocio, clientes corporativos, etc.

6. Si bien es un problema de origen informático, su alcance abarca a toda la empresa, por lo cual es necesario contar con el apoyo y compromiso de la Alta Gerencia.

Etapas en un Proyecto de Adecuación al Año 2000

A través de diversos organismos internacionales, se han logrado determinar las mejores prácticas para un proyecto de adecuación de los sistemas de información de una empresa para el año 2000. En particular, el esquema propuesto por el Comité de Supervisión Bancaria de Basilea (organismo que agrupa a las principales entidades de regulación y supervisión bancaria del mundo) ha influido en muchos de los esquemas dictaminados por los supervisores bancarios y aplicado en las principales empresas bancarias del mundo.

Dicho esquema comprende las siguientes etapas y actividades:

Etapa I : Identificación y Planeamiento

- Realizar un inventario y un análisis de impacto de todos los componentes de tecnología de información instalados en la empresa: aplicaciones internas, aplicaciones mantenidas por terceros, bases de datos y archivos, computación de usuario final, paquetes, sistemas operativos, equipos de hardware, equipos con microprocesadores empotrados, interfases con entidades externas, etc.
- En base a los resultados del análisis de impacto es posible determinar el alcance, dimensión, recursos y tiempos necesarios para la ejecución del

proyecto de adecuación al año 2000, lo cual permitirá elaborar el Plan de Acción correspondiente, el cual debe incluir:

a. Estrategia de adecuación a seguir por la empresa
b. Cronograma de actividades con asignación de responsables e hitos de control
c. Prioridades definidas de acuerdo a la criticidad de los componentes para la continuidad del negocio.
d. Presupuesto necesario
e. Directivas de control y monitoreo de la ejecución del Plan
f. Participación de Auditoría Interna

Etapa II: Conversión y/o Renovación

- Conversión de aquellos componentes de tecnología de información impactados por el problema del año 2000 de acuerdo a la estrategia definida por la empresa.
- Renovación o sustitución de aquellos componentes afectados, cuya conversión resulte costosa o no viable, de acuerdo al análisis costo/beneficio realizado por la empresa.

Etapa III: Pruebas

- Definir la estrategia de pruebas a ser utilizada por la empresa
- Elaborar un plan de pruebas, considerando los tipos de pruebas a ser realizadas (unitarias, integrales y con aceptación de usuario) y los recursos disponibles, entre otras consideraciones.
- Ejecución del plan de pruebas, el cual debe incluir una simulación de las condiciones del año 2000 (pruebas integrales).
- En el caso de las empresas bancarias, se recomienda la ejecución de pruebas sectoriales en las cuales pueda validarse la compatibilidad con el año 2000 de las interfases informáticas entre las empresas bancarias, así como su interrelación con proveedores de servicios críticos como telecomunicaciones, suministro de energía eléctrica, transporte de valores, etc.

Etapa IV: Implementación

- Implementar (pasar a producción) los componentes de tecnología de información cuya compatibilidad con el año 2000 ha sido validada exhaustiva y exitosamente.

Control de Reincidencias y 'congelamiento'

Además del Proyecto de adecuación al año 2000, normalmente existen otros proyectos de desarrollo y/o mantenimiento de sistemas de información que se ejecutan en forma paralela, así como adquisiciones de equipos y/o paquetes requeridos por diversos departamentos de la empresa. En el primer caso, la empresa debe definir procedimientos y estándares que permitan asegurar que en dichos proyectos paralelos no se vuelvan a introducir problemas año 2000. Esto puede lograrse, por ejemplo, estableciendo un conjunto de pruebas que deben ser superadas por los nuevos aplicativos desarrollados o las modificaciones realizadas a los sistemas de información, antes de su pase a producción. De manera similar, los nuevos equipos y paquetes adquiridos deberían pasar previamente por un conjunto de pruebas año 2000, adicionalmente a la declaración por escrito del proveedor acerca de la compatibilidad con el año 2000 del equipo o paquete adquirido, otorgando las garantías y soporte técnico requerido en caso de problemas.

Un tema adicional que se sugiere es efectuar un 'congelamiento' en los proyectos de sistemas de información durante los tres meses anteriores y posteriores al cambio de fecha al año 2000 (Octubre 1999 - Marzo 2000). Este 'congelamiento', posterior a la implementación de todos los componentes de tecnología de información compatibles con el año 2000 (finalización de la Etapa IV), significa que la empresa debe evitar realizar nuevos pases a producción, que impliquen cambios en sus sistemas de información ya compatibles, de tal manera que se minimice la posibilidad de introducir nuevos problemas año 2000 en sus sistemas de información.

Plan de Contingencia

En su aspecto tecnológico, el Proyecto de Adecuación al año 2000 se convierte en un gran proyecto de mantenimiento de sistemas de información, que abarca a todos los componentes de tecnología de información de la empresa. Sin embargo, como todo proyecto de desarrollo o mantenimiento de sistemas de información, no existe una certeza absoluta que los sistemas convertidos y validados no presenten absolutamente ningún problema durante el cambio de fecha al año 2000. En tal sentido, resulta necesario elaborar un Plan de Contingencia específico que permita mantener la continuidad operativa de la empresa, en caso alguno de los componentes informáticos que soportan sus procesos críticos experimente problemas ocasionados por el cambio al año 2000.

Dicho Plan debería considerar, entre otros aspectos, los siguientes:

a. Identificación de los procesos críticos de negocio de la empresa, así como de los activos (sistemas de información, equipos de hardware, equipos no informáticos, etc.), que soportan dichos procesos.
b. Identificación de los proveedores de servicios críticos para la empresa.
c. Identificación de escenarios de fallas originadas por el problema del año 2000, que incluyan fallas en los activos que soportan los procesos críticos de negocio, así como fallas en proveedores críticos.
d. Evaluación de la probabilidad de ocurrencia e impacto de los escenarios de falla identificados.
e. Evaluación de alternativas de mitigación de riesgos.
f. Definición de procedimientos especiales de respaldo de información crítica.
g. Elaboración de procedimientos de recuperación para cada escenario de falla identificado, teniendo como objetivo la recuperación rápida y oportuna de los procesos críticos de negocio afectados.

h. Definición de procedimientos de restauración al modo normal de operaciones, en caso haya finalizado la contingencia.
i. Definición del equipo de trabajo que laborará durante la contingencia, asignando claramente responsabilidades y líneas de reporte.
j. Definición de un programa de entrenamiento y capacitación para el personal.
k. Conformación de un equipo de emergencia con la autoridad y responsabilidad de resolver situaciones no previstas durante la contingencia.
l. Establecer medidas de comunicación externas acerca de las medidas que adoptará la empresa en caso de activación del Plan.
m. Definición de criterios de activación, es decir, las condiciones bajo las cuales el plan entra en ejecución.

Con la finalidad de asegurar que el Plan de Contingencia elaborado permitirá asegurar de manera efectiva la continuidad de los procesos críticos de negocio de la empresa, en caso de una contingencia, dicho Plan debe ser adecuadamente validado. La validación del Plan de Contingencia puede realizarse a partir de una simulación de los escenarios de falla, frente a los cuales las personas designadas deben declarar la activación del Plan y monitorear su correcta ejecución.

Riesgos de negocio derivados del problema informático del año 2000

Si bien el problema del año 2000 tiene un origen informático, sus repercusiones alcanzan todos los demás riesgos de negocio a los que se encuentran expuestas las empresas bancarias, tal como detallamos a continuación:

El riesgo crediticio derivado del año 2000 significa que los principales clientes tomadores de fondos (banca empresarial o corporativa) pueden experimentar problemas operativos debido al problema del año 2000, los mismos que pueden traducirse finalmente en problemas financieros o en su flujo de caja, aumentando su

riesgo crediticio. En tal sentido, las empresas bancarias deben monitorear el riesgo año 2000 de sus principales clientes, como un elemento adicional en su evaluación de riesgo crediticio.

Los riesgos legales derivados del año 2000 significan las posibles contingencias legales que puedan originarse como consecuencia del problema informático del año 2000. Así por ejemplo: demandas judiciales de clientes que puedan sentirse 'afectados' por el problema, contratos de servicios con proveedores críticos, contratos de garantías, pólizas de seguros contratados, entre otros instrumentos legales. En este aspecto, se recomienda que las empresas bancarias realicen una revisión exhaustiva de todos los contratos firmados con clientes, proveedores y socios de negocio, con el fin de evaluar los posibles riesgos año 2000, a los que se encuentra expuesta debido a dichos contratos.

El riesgo de mercado derivado del año 2000 significa que las empresas emisoras de títulos-valores (bonos, acciones, etc.) pueden experimentar dificultades operativas debido al problema de año 2000. En el caso de los bonos, esto puede incrementar el riesgo de no pago (default risk) de la empresa emisora. En el caso de las acciones, los problemas operativos y financieros que la empresa emisora pueda experimentar constituye información que es recogida por el mercado de capitales e influye directamente sobre la cotización de las acciones de estas empresas. Esto puede determinar finalmente variaciones importantes en la valorización de la cartera de inversiones negociables de la empresa bancaria, frente a lo cual debería incrementarse el nivel de capital existente para cubrir dichas variaciones.

El riesgo de imagen o *reputación derivado del año 2000* significa que la empresa bancaria puede verse expuesta a publicaciones tendenciosas acerca de su preparación frente al problema informático del año 2000, dañando su reputación e imagen. Esto puede causar inseguridad en sus depositantes y posibles problemas de liquidez, como se describe en el párrafo siguiente. Frente a este riesgo, se recomienda que las empresas bancarias manejen adecuadamente una política de

comunicaciones destinadas a brindar confianza al público acerca de su preparación frente al problema del año 2000.

El riesgo de liquidez derivado del año 2000 se refiere al posible incremento en la demanda de efectivo que pueden experimentar las empresas bancarias debido a expectativas negativas de los depositantes y del público en general, acerca de la adecuación de la empresa con respecto al problema del año 2000. Este aspecto resulta especialmente importante, debido a que una inadecuada política de comunicaciones puede exponer a la empresa a posibles retiros masivos de sus depositantes, originando problemas de liquidez que pueden traducirse finalmente en problemas de solvencia de la institución.

Plan de acción durante la transición al año 2000 (Rollover Plan)

La empresa debe definir asimismo un esquema especial de organización, denominado Centro de Control, para las fechas críticas de la transición al año 2000 (del 30-12-1999 al 04-01-2000), con la autoridad suficiente para tomar decisiones rápidas, y administrar adecuadamente los posibles eventos que pudieran ocurrir durante el período de transición al año 2000. Debe considerarse además de los aspectos tecnológicos internos, el desempeño de los principales proveedores de servicios, y las expectativas del público en general. Esto debería incluir asimismo un esquema de validación con hitos de control definidos que permita asegurar que las transacciones de negocio han sido procesadas correctamente durante la transición.

APENDICE B

EL ESTANDAR ITSEC DE LA COMUNIDAD EUROPEA

Aspectos generales

ITSEC (Information Technology Security Evaluation Criteria) o Criterios de Evaluación de la Seguridad en Tecnología de Información, consiste en un conjunto de criterios estándares, reconocidos por la Comunidad Europea, para la evaluación de la seguridad en los sistemas y productos de tecnología de información, realizada en forma independiente de sus proveedores, con el fin de identificar posibles vulnerabilidades lógicas en estos productos. El resultado de esta evaluación se expresa en grados de rigor conocidos como Niveles de Seguridad (Assurance Levels). Se emiten certificados de productos en base a este esquema de evaluación, señalando el Nivel de Seguridad alcanzado.

Los criterios estándares incluidos en el esquema ITSEC han sido recogidos como resultado de la homogeneización y unificación de los criterios de evaluación definidos por Gran Bretaña, Alemania, Francia y Holanda para sus respectivos países. La versión actual de ITSEC es la versión 1.2 y fue publicada en Junio de 1991. Actualmente los certificados emitidos en base al esquema ITSEC son reconocidos en todos los países de la Comunidad Europea, reduciendo la necesidad de evaluación de productos o sistemas en cada país.

Asimismo en años recientes se han logrado unificar los criterios de evaluación definidos por ITSEC, los criterios definidos por Canadá (CTCPEC) y aquellos definidos por Estados Unidos (Federal Criteria - FC), en un solo conjunto de criterios

denominado *Criterios Comunes para la Evaluación de la Seguridad en Tecnología de Información* (Common Criteria - CC). La propuesta final de este conjunto de Criterios Comunes fue publicada en Diciembre de 1997, y se encuentra en proceso de evaluación por la ISO (Organización de Estándares Internacionales) para su aceptación formal como estándar internacional.

La Premisa

El desarrollo de criterios estándares para la evaluación de la seguridad en tecnología de información (TI) se basa en la siguiente premisa:

Los usuarios de los sistemas de información requieren tener confianza en la seguridad del sistema que están usando. Además necesitan contar con una medida estándar para comparar las características de seguridad ofrecidas por los productos de tecnología de información que se piensan adquirir. A pesar que los usuarios pueden confiar en las indicaciones de los fabricantes o proveedores de los sistemas y productos sobre este aspecto, es más probable que la mayoría de los usuarios prefieran confiar en los resultados de una evaluación imparcial realizado por una empresa independiente. Para ello, se requiere contar con criterios de evaluación objetivos y bien definidos, así como la existencia de una entidad certificadora que pueda confirmar que la evaluación fue realizada apropiadamente.

El Modelo de Evaluación

El Modelo de Evaluación implícito en los Criterios propuestos por el estándar ITSEC considera los siguientes aspectos:

Cada sistema o producto de tecnología de información evaluado se denomina Objeto de Evaluación (*Target of Evaluation - TOE*). Con el fin que un TOE alcance sus objetivos de seguridad, debe incorporar funciones apropiadas de reforzamiento de seguridad (*security enforcing functions*) que cubran áreas como, por ejemplo,

control de acceso, auditoría y recuperación a partir de errores. Estas funciones deben ser implementadas a través de mecanismos específicos de seguridad. Este esquema jerárquico de tres niveles se resume de la siguiente manera:

- Objetivos de Seguridad. *(¿Por qué se requiere la funcionalidad?)*
- Funciones de Reforzamiento de Seguridad. *(¿Cuál es la funcionalidad realmente proporcionada?)*
- Mecanismos de Seguridad. *(¿Cómo se proporciona la funcionalidad?)*

Una vez identificadas estas funciones y mecanismos debe evaluarse cual es el nivel de confianza o aseguramiento (*assurance*) que dichas funciones permitan alcanzar los objetivos de seguridad definidos para un determinado TOE.

Esta evaluación distingue entre la confianza en la **corrección** de la implementación de las funciones de reforzamiento de seguridad y la confianza en su **efectividad**.

La ***evaluación de la efectividad*** determina si las funciones de reforzamiento de seguridad proporcionados en el TOE realmente satisfacerán los objetivos de seguridad establecidos, considerando los siguientes aspectos:

a. La adecuación de las funciones de reforzamiento de seguridad del TOE para mitigar las amenazas a la seguridad del TOE.
b. La integración y soporte de las funciones y mecanismos de reforzamiento de seguridad del TOE.
c. La habilidad de los mecanismos de seguridad del TOE para enfrentar un ataque directo.
d. Considerar si las vulnerabilidades de seguridad existentes en la construcción del TOE pueden comprometer la seguridad del TOE.
e. Considerar si el TOE no puede ser configurado o usado de una manera insegura, pero que el administrador o usuario final del TOE crea razonablemente que es segura.

f. Considerar si las vulnerabilidades de seguridad en la operación del TOE pueden comprometer la seguridad del TOE.

La ***evaluación de la corrección*** determina si las funciones de reforzamiento de seguridad se encuentran implementadas correctamente. Para ello se han definido siete niveles de evaluación denominados E0 a E6, los cuales constituyen niveles ascendentes de confianza en la corrección, de la siguiente manera:

Nivel E0	Este nivel representa una confianza inadecuada.
Nivel E1	En este nivel debe existir un objetivo de seguridad definido y una descripción informal del diseño de la arquitectura del TOE. Las pruebas funcionales deben indicar que el TOE satisface su objetivo de seguridad.
Nivel E2	Además de los requerimientos del nivel E1, debe existir una descripción informal del diseño detallado. Debe evaluarse la evidencia de las pruebas funcionales. Debe existir además un sistema de control de la configuración y un procedimiento de distribución aprobado.
Nivel E3	Además de los requerimientos del nivel E2, el código fuente de los programas y los dispositivos de hardware que correspondan a los mecanismos de seguridad, deben ser evaluados. Además deben evaluarse las pruebas de dichos mecanismos.
Nivel E4	Además de los requerimientos para el nivel E3, debe existir un modelo formal subyacente de política de seguridad que soporte el objetivo de seguridad. Las funciones de reforzamiento de seguridad, el diseño de la arquitectura y el diseño detallado deben ser especificados en un estilo semiformal.

Nivel E5	Además de los requerimientos planteados por el nivel E4, debe existir una correspondencia cercana entre el diseño detallado, el código fuente y los diagramas de hardware de la empresa.
Nivel E6	Además de los requerimiento planteados en el nivel E5, las funciones de reforzamiento de seguridad y el diseño de la arquitectura deberían encontrarse especificados siguiendo un estilo formal. Asimismo debe ser consistente con el modelo formal implícito de la política de seguridad de la emrpesa.

La corrección es evaluada desde el punto de vista de la construcción del TOE, cubriendo tanto el proceso de desarrollo como el entorno de desarrollo, y la operación del TOE.

Referencias adicionales

Mayor referencia sobre el esquema ITSEC puede encontrarse en el sitio web dedicado a este tema por el gobierno del Reino Unido: http://www.itsec.gov.uk. En este sitio web se encuentran guías introductorias sobre el esquema ITSEC, así como documentación formal sobre el mismo tema, las cuales pueden ser descargadas libremente.