UNIVERSIDAD CATÓLICA ANDRÉS BELLO
DIRECCIÓN DE POSTGRADO
AREA DE CIENCIAS ECONÒMICAS
ESPECIALIZACIÓN EN ECONOMIA EMPRESARIAL

TRABAJO DE ESPECIALIZACIÒN:

FRAUDE DESDE LA OPTICA SOX

Asesor: Profesor Daniel Lahoud

Trabajo especial, realizado por:
Lic. Vásquez R. Nelly E.
Caracas, Noviembre 2010

INDICE

INTRODUCCIÓN

El siguiente trabajo de especialización busca entender y conocer el por qué se ha experimentado la crisis financieras de las empresas, a través del tiempo, se han conocido diversas razones que han generado esta situación, tales como malas inversiones, políticas económicas o monetarias no adecuadas, malas praxis en las operaciones financieras, sobre endeudamiento público o privado, entre otras, factores generan desequilibrios en las instituciones financieras debido a la fragilidad del sistema y la complejidad de las operaciones.

Adicionalmente, otro de los factores que genera crisis en las entidades, son los riesgos a los cuales está propenso las actividades de las empresas, entre ellas el fraude (operativo y financiero), pero que se plantea bajo la metodología SOX y que son factores que generan cambios en los estados financieros y dependiendo del impacto podría afectar a un sector de la economía.

Es por ello, que se decide estudiar el desarrollo de la metodología SOX, basado mediante el modelo COSO, que se enfoca desde el riesgo y los controles que mitigan esos riesgos, que está enfocado en los procesos y funciones de las empresas.

Debido a esta situación, las entidades financieras poseen peligro de fraudes y escándalos corporativos que representan un riesgo de fraude económico y a su reputacional en el mercado, es por ello, que mediante la metodología de control interno establecen los aspectos legales tanto políticas internas como aquellas emitida por los entes reguladores para todas las operaciones financieras, también cabe destacar que son basadas por el Gobierno Nacional de la República Bolivariana de Venezuela con la finalidad de fomentar la prevención de actividad delictiva.

CAPITULO I

1.1.- ANTECEDENTES.

Es importante conocer el origen de la ley “SOX”, a fin de identificar en el desarrollo del trabajo sus riesgos y los impactos que genera este tipo de actividades en las instituciones financieras, y a su vez, qué impactos generan en las actividades económicas. Es por ello que se ha realizado una serie de investigaciones documentales para poder entender porque surge esta ley o norma.

De acuerdo a lo antes comentado a continuación se menciona algunos hechos históricos, que explican en cierta manera como surge la Ley SOX.

Después de la declaración de bancarrota de Worldcom y el escándalo financiero de Enron, el Congreso Americano aprobó el proyecto de ley de la Cámara de Representantes No. 3763 firmada por el Presidente Bush y convertida en ley de forma inmediata.

> “La ley Sarbanes-Oxley, garantiza la creación de mecanismos de auditoría y seguridad confiables en las empresas, incluyendo aún reglas para la creación de comités encargados de supervisar sus actividades y operaciones, de modo a mitigar riesgos a los negocios, evitar la ocurrencia de fraudes o asegurar que haya medios de identificarlas cuando ocurren, garantizando la transparencia en la gestión de las empresas”. (http://es.wikilingue.com/pt/Ley_Sarbanes-Oxley).

La creación de esta ley fue en el año 2002, surgió por la necesidad de normar las leyes y controlar los procesos internos de las empresas, pues se realizaban auditorias y controles contables para garantizar la fiabilidad de los estados financieros, sin embargo, se presentaron fraudes financieros en empresas importantes y de envergadura. Es por ello que dicha ley supone lo siguiente: constituye un nuevo organismo supervisor de la contabilidad, nuevas reglas de independencia del auditor, una reforma de la contabilidad corporativa, la

protección del inversor y aumenta las penas criminales y civiles por las violaciones al mercado de valores.

Con la creación de la Ley Sarbanes-Oxley, reflejan los dos artículos más importantes, que son la sección 302 “Responsabilidad Corporativa” y la sección 404 “Desgloses Financieros de Mejor Calidad”, por lo que al profundizar el desarrollo del tema se explicará en detalle su aplicación en las instituciones financieras.

Se realizó una investigación de los temas desarrollados por el sector académico y que se encuentran asociados al “Fraude desde la óptica SOX” aplicado en las instituciones financieras. Cabe destacar que este tema es relativamente nuevo, sin embargo, se pudo conocer el desarrollo de una tesis en la Universidad de los Andes, relacionado a “Evaluación del Control Interno Administrativo Bajo Procesamiento Electrónico de Datos Basados en el Modelo COSO en la Dirección de Hacienda de la Alcaldía del Municipio Urdaneta del Estado Trujillo”, este se basa en función de un modelo corporativo de control interno en el cual se fundamenta en las mejores prácticas internacionales contenidas en el “Enterprise Risk Management – Integrated Framework de COSO (Comité of Sponsoring Organizations of the Treadway Comisión), de acuerdo al autor, expresa que fue realizada con la necesidad observar que todas las instituciones públicas garanticen un adecuado control interno en sus funciones y actividades, para ser más eficientes y eficaz.

Adicionalmente, otra tesis de la Universidad de los Andes “Análisis de la Eficiencia y Eficacia del Sistema de Control Interno Tributario de Impuesto Sobre la Renta, Caso: Distribuidora Santa Inés C.A. (Año de Evaluación 2008) “, en donde su principal objeto fue el análisis de la eficiencia y eficacia del sistema de control interno tributario de Distribuidora Santa Inés C.A.

Sin embargo, se observan que estas tesis solo argumentan la eficiencia y eficacia de los controles internos a fin de garantizar el buen funcionamiento de las

empresas, en si esta es la filosofía del Control Interno, sin embargo, esta investigación que se está desarrollando va enmarcada desde las normas internacionales y corporativas, a fin de reducir el riesgo de fraudes operativos y financieros de la banca.

1.2.- PLANTEAMIENTO DEL PROBLEMA

Al analizar el "fraude desde la óptica SOX" en las instituciones financieras de Venezuela, se debe entender que este tema aplica únicamente a las empresas corporativas y que se encuentran registradas bajo la SEC (Security Exchange Comision) para poder ejercer sus operaciones a nivel internacional, pues es el ente encargado de garantizar el funcionamiento adecuado de las empresas en el cual está regido bajo una certificación contable SOX de los procesos internos de las empresas.

El problema que surge, en gran medida por los escándalos financieros de las grandes empresas, es que a pesar de realizar auditorías contables y de sistemas (internas, externas, corporativos) y obtener de ellas un dictamen limpio, surgen fraudes financieros que no habían sido detectado durante dichas auditorias, es por ello que se encuentra la necesidad de investigar y analizar el por qué ocurren estos eventos, los riesgos y controles asociados, adicionalmente conocer las normas que rigen estos procesos corporativos de certificación contable.

Su principal fuente de información es la documental, para luego llevarla a la práctica, en donde se podrán exponer los eventos que podrían generar fraudes operativos y/o financieros, y que generan impactos en las instituciones financieras. A su vez, es importante conocer las medidas de prevención que poseen las instituciones financieras para protegerse o disminuir los riesgos que puede ocasionar esta actividad.

1.3.-JUSTIFICACIÓN E IMPORTANCIA.

Dado el incremento de las actividades ilícitas en el mundo y que también involucra a Venezuela, en el cual las organizaciones delictivas utilizan el sistema financiero como intermediario para realizar actividades con ánimos de lucros, que involucran a las personas externas a la institución y a la misma en sí. Debido a que a través del fraude interno o externo, generan desestabilización en un sector de la economía. Es por ello, que se decidió estudiar el fraude desde la óptica SOX, es decir, conocer la metodología para reducir el riesgo del fraude externo (u operativo) y el fraude interno (financiero), en donde se mitigue el evento mediante controles específicos y adecuados.

A continuación se comentan algunos casos que generaron gran controversia a nivel internacional, y se ha convertido en un problema globalizado, nació a raíz de los escándalos financieros, de las empresas ENRON, WORLDCOM, MADOFF, STANFORD BANK, PARMALAT (Italia). Estos casos fueron muy conocidos, pues generaron debacles financieras afectando un sector económico dentro de un país, adicionalmente generaron e incurrieron en riesgos reputacional (prestigio de las empresas, confianza) y riesgo de credibilidad (aceptabilidad de las empresas) en las instituciones de cara a los potenciales inversionistas y clientes.

Las instituciones financieras, han tenido que lidiar con los fraudes operativos y mejorar los controles a fin de hacerlos más eficientes, sin embargo, se había dejado a un lado el control de los procesos internos y financieros dentro de las empresas, en las cuales pudiera existir políticas, normas y procesos de control de las actividades.

Esta investigación ha surgido por la necesidad de dar a conocer el fraude desde la óptica SOX en las instituciones financieras, sus impactos, riesgos y sus controles.

Para esto se debe conocer el modelo de control interno (SOX y no SOX), la tipología del riesgo y los controles, esto está enfocado en los procesos internos de las empresas. Adicionalmente, referenciar las normas que anteceden a la Ley SOX, tales como Basilea I y II, para entender la evolución de los controles de los procesos en las empresas financieras, sin embargo, Basilea se enfoca en disminuir y controlar los riesgos operativos, es decir, capacidad de absorción de pérdidas y de protección ante quiebra en las instituciones, el control interno desde la óptica SOX, se basa en los riesgos y controles que lo mitigan, cumpliendo una metodología; está asociada con el objetivo de indagar los impactos que genera el fraude financiero y operativo a las entidades financieras, así como su afectación a la economía

Se busca dar respuesta a los objetivos específicos definidos al inicio del trabajo, detectando así las operaciones más sensibles a los fraudes financieros y operativos, qué medidas de control son consideradas para su detección. Es por ello, que se desea conocer cuáles son las normativas legales que protegen al sistema financiero a nivel nacional e internacional y su efectividad en la aplicación.

Debido a lo antes comentado, se desea analizar y explicar detalladamente los riesgos a los cuales están expuestas las instituciones financieras a través del Fraude desde la óptica SOX. Los impactos que generan dentro de ellas y en las economías de los países que se encuentran expuestos a este factor de riesgo ejercidas por las fuerzas externas e internas.

1.4.- OBJETIVO.

A continuación se definen los objetivos del trabajo, en donde se plantean los objetivos generales que expresan lo que se pretende lograr, esto se logra a través del objetivo general y de los objetivos específicos que se irán cumpliendo en cada una de las fases y cuyos logros colaboraran en el alcance o en el logro de los objetivos generales.

1.4.1 OBJETIVO GENERAL

Descubrir la metodología SOX.

1.4.2 OBJETIVOS ESPECÍFICOS

- ✓ Analizar los riesgos que genera el fraude financiero y fraude operativo en las instituciones financieras.
- ✓ Identificar las principales operaciones que son más vulnerables en presentar fraudes operativos o financieros.
- ✓ Determinar los métodos de control que se aplican en las instituciones para evitar los fraudes financieros y operativos desde la óptica SOX.

1.5.- ALCANCE Y LIMITACIONES.

1.5.1 Alcance

- ✓ Conocer los riegos que impactan de forma negativa a las instituciones financieras, originada por el fraude desde la óptica SOX-
- ✓ Cuáles son los principales riesgos que posee un país y sus bancos; y sus consecuencias económicas.
- ✓ Dar a conocer las operaciones bancarias más vulnerables en el fraude SOX y cuáles son los métodos de protección para evitarlas.

1.5.2 Limitaciones

- ✓ Insuficiente información certera en relación a las cifras financieras provenientes de pérdidas que se generan en las instituciones financieras en Venezuela, a raíz de los fraudes operativo o financiero en base a las normas SOX.

CAPITULO II

MARCO TEORICO.

2.1.- Origen de la Ley Sarbanes– Oxley (SOX).

El 25 de Julio del 2002, las cámaras del Congreso de los Estados Unidos se ponen de acuerdo para aprobar el convenio de Sarbanes Oxley, para proporcionar una reforma corporativa eficaz, con el objetivo de fortalecer la confianza en los mercados de capitales.

Dicha ley fue propuesta por un Senador y un Diputado, ambos de los Estados Unidos, ellos son: Paul Sarbanes y Michael Oxley, detectaron que existía una debilidad en las empresas y realizaron un trabajo de investigación y observaron que el problema se originaba esencialmente en los procesos de las empresas. Es por ello que la finalidad de la creación de dicha ley, es la protección a los inversionistas que interactúan en el mercado y no propiciar desestabilización en algunos sectores del mercado.

La Ley Sarbanes-Oxley, origina que todas las agrupaciones o empresas que cotizan en la Bolsa de Valores de los Estados Unidos de América, certifique la efectividad y funcionamiento apropiado de controles internos en las diversas zonas geográficas donde operan, todo esto con el propósito de certificar la transparencia de sus procedimientos. (Gutierrez, 2004)

Para el 30 de julio del 2002, se convierte en ley “Sarbanes-Oxley”, una vez que el Presidente Bush firmó dicho acuerdo.

La ley “Sarbanes-Oxley, aporta claridad y confianza en los siguientes temas:

Crea un organismo autónomo de inspección a tiempo completo, Consejo de Supervisión de Contabilidad de Empresas Públicas (PCAOB), destinado a los participantes en el mercado de capitales; la SEC (Securities and Exchange Commission) controla a dicho Consejo.

1. Instaura responsabilidades nuevas a los comités de auditorias y ejecutivos corporativos.

2. Solicita nuevos requerimientos de información a las empresas públicas.
3. Presta servicios de “no auditoría” que las firmas auditoras pueden facilitar a sus clientes:
4. Impide ciertos servicios a los clientes auditados, específicamente en la externalizarían de la auditoría interna y el diseño e ejecución de los sistemas de información financieros.
5. Permite la prestación del resto de los servicios, sujeto a la pre aprobación del comité de auditoría (el Consejo de Supervisión de Contabilidad de Empresas Públicas podrá establecer otros servicios de “no auditoría” prohibidos).
6. Mejorar los controles asociados a los riesgos de fraudes corporativos.
7. Requerir reglas sobre los conflictos de intereses de los empleados o colaboradores.
8. Incrementa explicativamente las responsabilidades y el presupuesto de la SEC (Securities and Exchange Commission).

Esta ley, se basa en la interpretación de los procedimientos de la regulación SEC (Securities and Exchange Commission) y del Consejo de Supervisión de Contabilidad de Empresas Públicas. (Touche, 2008).

2.2.- Principales Ámbitos de Aplicación.

La Ley “Sarbanes-Oxley, posee un extenso impacto y afecta a diversos participantes y sectores del mercado, tales como: La administración de compañías públicas, Comités de Auditoría, Firmas Auditoras, y entre otros: Reguladores y “fijadores de normas”, Inversionistas, Bancos de inversión y Abogados.

2.3. –Problemas que generaron la creación de la “Ley Sarbanes Oxley” y el Objetivo.

Los principales problemas que motiva el surgimiento de la Ley Sarbanes-Oxley (SOX), son los siguientes: creación de información alterada, precios abultados de las acciones, modificación de las cifras de los estados financieros y sociedades delictuosas con las compañías contables (firmas de auditorias). Es por ello, que se generan los desastres financieras en grandes empresas, y a pesar de que se les realizaban procesos de auditorias, no se detectó es ningunos de estos dificultades.

Como consecuencia el objetivo de esta Ley “Sarbanes-Oxley (SOX)” se basa principalmente de crear o mejorar el ambiente del control interno de las empresas y concretar y establecer responsabilidades sobre su cumplimiento al CEOs (chief executice officer), CFOs (chief financial officer) y auditores financieros.

2.4.- Elementos claves y definiciones.

Certificación: los gerentes de las empresas deben certificar los reportes anuales, trimestrales y algunos reportes periódicos, debido a que se hacen responsables del establecimiento y el mantenimiento de los controles internos, en cuento a su efectividad y que la información material relacionada a los controles internos se ha dado a conocer, esto será publicado en informes periódicos, luego de la fecha de evaluación.

Informe de controles internos: en cada informe de la administración deberá revelar que los controles internos se encuentran evaluados y mitigados los riesgos. Adicionalmente, los auditores internos deben dar fe del informe emitido por la administración sobre la evaluación de los controles internos.

Nuevos requerimientos de revelación de información: la información deberá estar en tiempo real, veras y que cumpla con los principios contables generalmente aceptados (“GAAP”), los ejecutivos que posean al menos el 10% del capital de una empresa tiene un nuevo exigencia de información sobre los cambios en su tenencia de títulos.

Reforma de "Corporate governance": las empresas deben tomar un nuevo código de ética para los altos ejecutivos, se recomienda la firma del gerente general (CEO - chief executice officer) en la declaración de impuestos, no se consiente préstamos personales a los altos ejecutivos, limitaciones en las transacción en periodos de blackout de los fondos de pensiones.

Nuevos castigos: prohibición de intervenir indebidamente en las firmas auditoras y nuevas penas delictivas.

Incrementa en la revisión por parte de la SEC de los registros de información.

Interacción con los auditores: el comité de auditoria es responsable de la designación, pre-aprobación, compensación y revisión de la firma de auditoria, incluyendo las diferencias entre la gerencia y el auditor en relación a los informes financieros.

Independencia y conocimientos del comité de auditoria: los miembros de las compañías no deben tener relaciones con las empresas, es decir, estar asociada o afiliadas, debe tener un carácter de independencia. Adicionalmente, no recibir ningún pago o compensación aparte del establecido por el comité de dirección de auditoria con la compañía.

Quejas y recomendaciones anónimas: el comité de auditoria debe establecer procedimientos para la recepción, retención, y tratamiento de quejas recibidas por las empresas asociadas a la contabilidad, controles internos o auditorias. Así como también en el tratamiento de información confidencial de la compañía.

Pre-aprobación: La ley "Sarbanes –Oxley" faculta a los comités de auditorias a encargar la auditoria de la pre-aprobación a uno o más miembros independientes, sujetos a la siguiente revisión por parte del comité de auditoría.

Establecimiento del consejo de supervisión de contabilidad de empresas públicas: para inspeccionar la auditoria de sociedades publicas y salvaguardar los intereses de inversionistas.

Servicios prohibidos de "no auditorias": los siguientes servicios están prohibidos a ser prestados por las firmas auditoras:

Contabilidad, diseño e implementación de sistemas de información financiera, servicios de valoración y tasación, servicios actuariales, externalizarían de servicios de auditorias interna, intermediación, recomendaciones de inversión o servicios de banca de inversión, servicios legales y servicios especializados no relacionados con auditoria.

Rotación de socios: el socio auditor líder y el que efectúa las segunda revisión no pueden estar al servicio de un cliente auditado por más de 5 años fiscales continuos.

Informe de comité de auditoria: El auditor debe informar al comité de auditoria lo siguiente: todas las políticas contables y practicas criticas empleadas por el emisor, todos los tratamientos de información financiera en GAAP que hayan sido discutidos con la gerencia, así como los tratamientos alternativos o sugeridos por los auditores.

Conflictos de interés: no es legal que una empresa auditora audite a una empresa si el CEOs (chief executice officer), CFOs (chief financial officer), "Controller", "CAO", u otra persona que sirva en esa empresa es una posición equivalente, haya sido empleado por la firma auditora y participado en la auditoria de dicha empresa durante un año antes del periodo.

Estudio de la obligación de rotación de la firma auditora: un estudio de rotación de la firma auditora se llevara a cabo por la oficina de contabilidad general.

Destrucción de documentos: la destrucción de documentos de trabajos de auditorias puede acarear multas o hasta penas de cárcel hasta de diez años o ambas. (Deloitte&Touche, 2008). **Visión General de la Ley "Sarbanes-Oxley".**

2.5.- La Ley "Sarbanes –Oxley".

La ley SOX está conformada por 11 títulos y múltiples secciones, estableciendo diversos aspectos e incluyendo a las gerentes de las empresas, directorio, gobiernos corporativos, comités de auditorías, agentes de valores, corredores de bolsa, clasificadoras de riesgos y firmas auditoras.

En el Titulo I, plantea el “Public Company Accounting Oversight Board”, destacado como PCAOB que es la junta de supervisión de firmas de contabilidad pública y que se iniciar a aplicar en el mes de abril del 2003. Su función principal es llevar el registro de las firmas auditoras, observar su trabajo y validar que cumplan con los lineamientos de control de calidad y principios éticos. El PCAOB aplicar sanciones y medidas disciplinarias.

El Titulo II, SOX se relaciona con la independencia de los auditores. Este capítulo determina los servicios que las firmas pueden ejercer a sus clientes de auditoría y detalla las actividades que requieren ser certificadas previamente por el comité de auditoría. Es por ello, que queda prohibido prestar a los clientes de auditorías servicios de contabilidad y otros asociados con la preparación de las cuentas anuales; diseñar y/o preparar sistemas de información financiera; suministrar servicios actuariales o de auditoría interna; servicios gerenciales y de recursos humanos, de consultorías de inversión, servicios legales, outsorcing auditoría interna y cualquier otro servicio que la PCAOB establezca. En cuanto al servicio de asesoría tributaria solo y únicamente podrá prestarse cuando este sea aprobado por el comité de auditoría.

Por consiguiente, las secciones más relevantes de la ley está dirigida a la sección 302 “Responsabilidad Corporativa” y 404 “Responsabilidad de la administración”, será detallada a continuación.

En la sección 302, se establece la “Responsabilidades Corporativas para el Reporte Financiero”, en el cual se determina los lineamientos en los cuales los CEOs (chief executice officer) y CFOs (chief financial officer) deberán certificar anualmente el control interno de las compañías, por la CEOs deberán, cumplir lo siguiente:

Responsabilizarse por la certificación de controles y procedimientos; Diseño y la supervisión de la certificación de los controles, con la finalidad de asegurar que se conozca el diseño de los controles y de la información contenida en los mismos; Evaluación de la eficacia de los controles, procedimientos y cambios importantes realizados en el control interno para la emisión de los estados financieros; Exponer sus conclusiones en relación a la efectividad del

control interno; Informar al Comité de Auditoría y a los Auditores Externos sobre las deficiencias en el control interno, debilidad material y algunos actos de fraude que involucren a la Gerencia o a otros empleados que realicen actividades asociadas con el control interno e indicar cualquier cambio que se haya efectuado y a su vez sea significativo en los controles internos.

En la sección 404 “Evaluación Gerencial del Control Interno” constituye obligaciones por parte de la Gerencia de la compañía, en cuanto a emitir un informe anual sobre la evaluación del control interno de cada uno de los procesos de negocio y como se garantiza la adecuada emisión de los reportes financieros de las empresas, es por ello que al ser emitido el informe debe estar conformado de las siguiente manera: una declaración de que la gerencia de las empresas sea hace responsable por el diseño, aplicación y mantenimiento de un control interno eficiente y eficaz para la realización de los estados financieros; una declaración de la razonabilidad de los controles internos en la generación de los reportes de los estados financieros; una declaración de debilidades materiales detectadas durante la evaluación de los controles internos en la generación de los estados financieros; una evaluación relacionada al diseño y la garantiza la efectividad del control interno de las empresas sobre la emisión de los estados financieros; un informe efectuado por los auditores externos en el cual se comente la efectividad de los controles internos de la empresa para la generación de los estados financieros.

Adicionalmente las empresas no solo deberán garantizar el buen funcionamiento de los controles internos, asimismo tendrán que facilitar y suministrar a los auditores externos la documentación soporte necesaria para respaldar la evaluación y la decisión definitiva de la alta gerencia sobre el control interno.

La ley establece que se debe resguardar y tener disponilidad de los documentos por un lapso de diez años, por lo cual no se pueden modificar en los siguientes aspectos:

Almacenamiento: debe conservarse en las bases de datos sea en cintas, disco óptico y magnéticos para conservar la información.

Aplicaciones: debe abarcar detalles como protección de documentos, clasificación en línea y capacidad de auditorías.

Políticas y procedimientos: se definen opciones de cómo serán modificados, movidos y almacenados, así como también se especificara el personal capacitado y autorizado a efectuar dichos cambios. (UCES Auditoria de Sistemas y Software).

2.6.- Marco integral para el control y prevención del fraude.

El marco de control interno recomendado, para desempeñar los lineamientos determinados en la ley SOX, que es el creado por el Comite of Sponsoring of Treadway Comision (COSO). El Committee of Sponsoring Organization of Treadway Commission fue fundado en el año 1985 con el objetivo de estudiar los factores que permitían la emisión fraudulenta de reportes financieros. Luego en los inicios de los años 90, el comité conjunto con la asesoría de PrincewaterhouseCoopers, realizó un estudio detallado sobre los controles internos, donde el resultado fue los lineamientos del control internos COSO.

El COSO está compuesto por cinco componentes los cuales, al ser conformados en las unidades de negocio de la organización, favorecen a lograr los objetivos de control, que se categorizan en las siguientes áreas: eficiencia y efectividad de las operaciones para alcanzar los objetivos del negocio, preparación de cuentas financieras confiables y el cumplimiento de leyes y regularizaciones. (UCES Auditoria de Sistemas y Software)

Los cinco (5) componentes de Control Interno según COSO

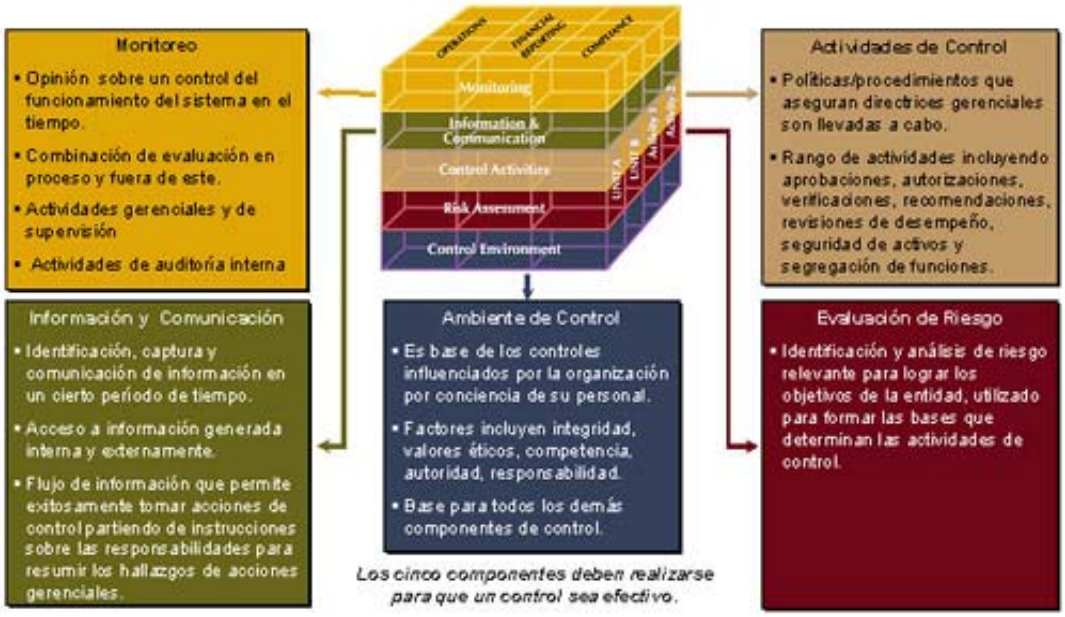


Gráfico 1. Modelo COSO. UCES, Auditorias de Sistemas y Software, trabajo práctico Ley Sarbanes –Oxley, www.megapuntes.com.ar (consultado: 09-05-2010).

2.7.- Fraude

Para poder conocer el fraude desde la óptica SOX, debemos conocer el significado del "fraude" principalmente, esta palabra proviene del latin Fraud, que no es más, que la habilidad de la simulación con propósito de engañar o lesionar a otro.

Una definición más formal, es que existió ánimo de lucro cuando la persona que realiza la tarea persigue un beneficio personal ilícito (obtención de provecho o enriquecimiento para sí mismo o para un tercero). (Rios Alfonso, 2009)

El fraude desde la óptica SOX, se divide en un fraude externo y un fraude interno, esta particularidad es originada debido a que surge de situaciones distintas y que su vez afectan a la empresa.

El *fraude externo*, es necesario evaluar la intencionalidad con que se han realizado las acciones que desencadenaron el error, diferenciados si existe o no ánimo de lucro. Si existió ánimo de lucro cuando la persona que comete la acción persigue un beneficio personal ilícito (obtención de provecho o enriquecimiento para sí mismo o para un tercero, en perjuicio de la entidad).

Sin embargo, si ha existido intención de provocar un daño sin ánimo de lucro el evento se clasificará en desastres, riesgos tecnológicos, etc.…

Estos eventos se pueden presentar de la siguiente manera: uso fraudulentos de tarjetas, robos y atracos, otros fraudes externos (falsificación de documentos, uso de fraudulentos de cheques, transferencias, pagarés y efectos, suplantación de la personalidad, estafas, uso y divulgación de información confidencial, espionaje industrial, extorsión y sobornos, secuestros y rescates), violación de la seguridad informática (utilización inadecuada de claves de accesos y fraudes a través de ordenadores (hackers, crakers, etc.)).

El fraude interno se precisa la colaboración probada de una persona vinculada en la empresa. Cuando la acción persiga el lucro de las personas que ejecuta la acción se clasifica en la subcategorìa de “robos u fraudes”. En caso de que se haya realizado sin ánimo de lucro se clasificará en el grupo denominado “actividades no autorizadas”. Se considerará existe ánimo de lucro cuando la persona que comete la acción persigue un beneficio ilícito (obtención de provecho o enriquecimiento para sí mismo o para un tercero, en perjuicio de la entidad).

En este caso se puede reconocer los siguientes eventos: robos y atracos (contempla los delitos ocasionados por el personal interno dentro de la institución o empresa), estas actividades son: falsificación de documentos, vulnerabilidad del sistema de identificación, uso y divulgación de información sensible, espionaje industrial, extorsión y sobornos, banca paralela. Dentro de las actividades no autorizadas, se encuentra el uso indebido de poderes y limites, divulgación de información sensible, manipulación de la contabilidad de gestión e inexistencias o deficiencias en el circuito de fijación de facultades.

De acuerdo a lo explicado anteriormente es donde hacemos la separación entre la visión del fraude operativo y el fraude desde la óptica SOX, básicamente es el origen del fraude, en si el fraude operativo proviene de actividades realizadas por personas ajenas a la entidad, en la cual puede realizar desfalco de empleados, autorizaciones de créditos con documentación fraudulenta, falsificación y clonación de tarjetas, cheques y estafas, falsificación de documentos.

En cuanto a la óptica SOX, se puede presentar de la siguiente manera: reconocimiento de ingresos ficticios, aplicación inconsistente de PCGA, transacciones significativas inusuales, que afectan tanto a ingresos como a gastos, estimaciones significativas en el cierre contable e incentivos y presiones para obtención de resultados.

2.7.1 Los Riesgos que corre las entidades.

Se refleja en la desconfianza de los inversores, re-evaluación de los riesgos de auditoría por posibilidades de errores materiales y pérdidas de empleados que ejecutan actividades de control relacionadas al reporting financiero.

2.7.2 Prevenir el Fraude.

A continuación se mencionaran observaciones que las entidades deben tener presentes para evitar el riesgo del fraude, los cuales son:

Segregar las funciones asociadas al efectivo, desembolsos, generación de cheques, firmas de autorización y conciliaciones bancarias. El hecho de concentrar estas actividades en un solo colaborador la empresa está asumiendo un alto riesgo.

La información confidencial de las empresas deberá presentarse de forma bien sellada a fin de que llegue a las manos de la alta gerencia, quien deberá analizarlo con detalle a fin de identificar alguna posibilidad de fraude.

La gerencia deberá revisar la emisión y autorización de los cheques generados, en especial las firmas y el endoso, con el objetivo de identificar si efectivamente está teniendo su fin y a su vez validar que se encuentren solo las personas autorizadas para ello.

Efectuar revisiones independientes de las conciliaciones de las cuentas y las bancarias, realizado por un experto en la materia. Se podría identificar algunas operaciones o transacciones irregulares.

Realizar un chequeo de los empleados sobre todo los de los nuevos, para identificar alguna irregularidad.

Efectuar periódicamente capacitación en los empleados relacionados con el fraude y sus aspectos perjudiciales, por los cual el personal estaría más dispuestos a colaborar a controlar la ocurrencia del fraude.

Los empleados que no se sienten bien remunerados pueden generar mayor riesgo o motivos que se generen situaciones irregulares, así como en insistir que los empleados tomen sus días de vacaciones, poder realizar la revisión de los papeles de trabajo del mismo.

La gerencia debe obtener información importante sobre posibles fraudes realizando preguntas no intimidadora a sus colaboradores.

Cuando se sospeche de fraudes o actividades irregulares podría la gerencia solicitar una revisión por auditoria interno o externa detallada.

El acceso a los registros debe estar autorizado y facultado de acuerdo a los perfiles y funciones, adicionalmente obtener claves de accesos, tanto para los PC como las bases de datos.

Los sistemas informáticos deben dejar un seguimiento de las personas que utilizaron la información, así como también los cambios que se efectúen., adicionalmente la base de datos de los proveedores debe conservar documentación soporte que respalde la actividad realizada, y a su vez tengo un adecuado nivel de segregación de funciones desde la elaboración, aprobación y autorización. (Daniel, 2005)

2.7.3 Indicadores de avisos sobre el fraude.

Las señales o alarmas que indican actividades irregulares que afectarían a las empresas, se encuentran las siguientes:

Inconvenientes financieros no resueltos, estilos de vida muy elevados de acuerdo a la posibilidad del empleado, propensos a las apuestas y los juegos de azar, alcohol y el exceso de drogas, relaciones estrechas con los proveedores y se preste para el fraude, no tomar vacaciones, trabajar hasta altas horas todo los días y disponer una actitud secreta y exagerada en cuanto al trabajo. (Daniel, 2005)

2.7.4 Como se debe controlar el Fraude SOX.

Es por ello que en una auditoria SOX, el auditor evaluará si los controles existentes cubren suficientemente los riesgos de error material por fraude y si gestionan el riesgo de manipulación intencionada de los propios controles.

Es por ello que para que los controles se cumplan y sean eficientes, es fundamental: que se establezcan controles sobre las transacciones significativas inusuales, particularmente aquellas que desembocan en apuntes manuales de última hora o inusuales, controles sobre apuntes manuales y ajustes realizados durante el proceso de cierre de la información financiera, controles relacionados con estimaciones de importancia de la gerencia, controles que mitigan incentivos y presiones sobre la gerencia para falsificar o gestionar inapropiadamente los resultados de los estados financieros y controles sobre el valor razonable y el análisis del deterioro de los activos.

CAPITULO III

MARCO LEGAL.

En relación con el marco legal, se puede conocer que desde la Ley General de Bancos y Otras Instituciones Financieras, hasta llegar a la políticas internas de las instituciones financieras; con el objetivo de resguardar a las instituciones financieras y la economía del país, asociadas con las actividades propensas al fraude financiero u operativo. En este caso se podrá conocer la norma de interna de prevención contra el fraude y debilidades de los controles internos de las entidades, que lo refleja de una manera general sin entrar en el detalle del modelo de control interno (COSO).

A continuación se mencionan las bases legales de prevención y control de las operaciones que poseen un riesgo implícito y se pueden detectar a través de los controles internos de las entidades (sean preventivos o detectivos), en las cuales se pretende protegen y velar por el buen funcionamiento del sistema financiero.
De acuerdo a lo comentado, se muestra las normativas asociadas a nivel nacional con las normativas legales vigentes:

3.1. - Resolución de la Superintendencia de Bancos y Otras Instituciones Financieras No. 136.03, de fecha 29 de mayo de 2003 “Normas para una adecuada Administración Integral de Riesgos”.

Artículo 1: La presente Resolución tiene por objeto, establecer los lineamientos básicos, que deberán observar las instituciones financieras en la implementación de un proceso de administración integral de riesgos.

En cuanto al artículo 2, se mencionan diversos tipos de riesgos, sin embargo, se mencionan los más resaltantes en donde el riesgo de legitimación de capitales se puede presentar, a continuación se presentan:

Riesgo: Posibilidad de que se produzca un acontecimiento, que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las instituciones financieras.

Riesgo operacional: Es la probabilidad de daños potenciales y pérdidas motivados a las formas de organización y a la estructura de sus procesos de gestión, debilidades en los controles internos, errores en el procesamiento de operaciones, fallas de seguridad e inexistencia o desactualización en sus planes de contingencias del negocio. Así como, la potencialidad de sufrir pérdidas inesperadas por sistemas inadecuados, fallas administrativas, eventos externos, deficiencias en controles internos y sistemas de información originadas, entre otros, por errores humanos, fraudes, incapacidad para responder de manera oportuna o hacer que los intereses de la institución financiera se vean comprometidos de alguna u otra manera.

Riesgo legal: Es la contingencia de pérdida que emana del incumplimiento de la institución financiera con las leyes, normas, reglamentos, prácticas prescritas o normas de ética de cualquier jurisdicción en la que lleva a cabo sus actividades.

Riesgo de reputación: Es la opinión negativa ocasionada por la afectación de la imagen de una institución financiera, al verse involucrada involuntariamente en transacciones o relaciones de negocios ilícitos con clientes, así como por cualquier otro evento externo.

Artículo 3: La **administración integral de riesgos** debe asegurar la homogeneidad de las herramientas, estructuras organizativas, procesos y sistemas adecuados a la dimensión de la institución financiera; que permita facilitar la gestión global de todos los riesgos que se asuman en cualquier actividad o área geográfica, para ello la unidad de administración integral de riesgos observará las técnicas básicas que a continuación se señalan:

Identificación: En un proceso dinámico y productivo aparecen nuevos y variados riesgos. Su descubrimiento es un precursor esencial de la acción.

Medición: Cuantifica los riesgos financieros, a través de la estimación de la probabilidad de ocurrencia y severidad de los eventos.

Control: Permite velar por el cumplimiento de las políticas de riesgo. Por tanto, dicha Unidad deberá contar con por lo menos los Manuales que más adelante se detallan, debidamente aprobados por su Junta Directiva y ser de uso obligatorio de la institución financiera, los cuales deben contener como mínimo lo siguiente: (SUDEBAN, 2003)

1. **Manual de organización y descripción de funciones**: Detalla la organización funcional de la unidad de administración integral de riesgos de la institución financiera, así como, las funciones, cargos y responsabilidades de ella y de los funcionarios y demás trabajadores vinculados a la unidad.
2. **Manual de políticas y procedimientos:** Contiene las políticas y procedimientos establecidos por la institución financiera para la identificación, medición, control, adecuación, seguimiento y administración de todos los riesgos de la institución financiera; así como, de las acciones correctivas a ser implementadas y del seguimiento de las instrucciones impartidas, según sea el caso. Contempla, entre otros, los sistemas preventivos para detectar los riesgos a que pudiese estar expuesta la institución financiera y los mecanismos de vigilancia a los fines de no exceder los límites por riesgo para las actividades u operaciones que ésta realiza. El contenido de este Manual debe ser constantemente revisado y actualizado.
3. **Manual de sistemas de organización y administración:** Permite la instauración de una adecuada estructura organizativa y administrativa que delimite claramente las obligaciones, responsabilidades y el grado de dependencia e interrelación existente entre el área de sistemas y las distintas áreas de la institución financiera, las cuales deben estar englobadas en el respectivo Manual de organización y descripción de funciones.
4. **Manual de sistemas de información:** Incluye los mecanismos dispuestos para elaborar e intercambiar información, tanto interna como externa y los procedimientos necesarios para identificar, desarrollar, administrar y

controlar los riesgos de la institución financiera. Debe comprender las acciones previstas para la difusión de las actividades que corresponden a los diferentes niveles directivos y al personal sobre el control de sus tareas e incluir, adicionalmente, las políticas y procedimientos contemplados para la utilización de los sistemas informáticos y las medidas de seguridad, así como los planes a ser implementados para afrontar las contingencias que pudieran presentarse en dichos sistemas.

CAPITULO IV

MARCO METODOLOGICO

4.1.- Tipo De Investigación

El tipo de investigación en el cual se desarrolla el trabajo de grado es de tipo documental, es conocer el modelo de control interno enfocado en la metodología SOX, en nuestro caso en particular, está enfocado en una institución financiera la cual se plantea todo el marco teórico del control interno, que explica los eventos y los controles que mitigan los posibles riesgos a los que se encuentran las actividades o funciones de una empresa o institución.

Se plantea una investigación documental, motivado al estudio del problema con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos. La originalidad del estudio se refleja en el enfoque, criterios, conceptualización y, en generalmente, el pensamiento del autor. (Yaselli, 2003).

Es por ello que dicha investigación, se considera documental basado en un estudio de desarrollo teórico y con revisiones criticas del estado del conocimiento, pues se ha basado en estudio anteriores y de casos ocurridos en otros países e instituciones bancarias o de empresas, y que ha afectado el desarrollo de las mismas, generando desestabilización financiera y pérdida en la credibilidad de sus clientes, asociado al riesgo reputacional de las entidades.

Adicionalmente, la investigaciòn esta basada en la informaciòn disponible en la web, libros, articulos especificos, normas internas o politicas contables que enfoca el tema del control interno basado en la ley SOX y su metodologia, el objetivo primordial del trabajo de grado es descubrir la metodologia SOX, y secuencialmente, analizar lor riesgos que genera el fraude desde la òptica SOX en las instituciones financieras, identificar las principales operaciones que son màs

vulnerables en presentar fraudes internos y externos; asi como tambièn determinar la metodologia de control interno que se aplican en las instituciones para reducir los eventos de riesgos. Cabe destacar que el control interno basado en la ley SOX, proviene de una metodologia que es homogeneizada con las empresas que deben certificar bajo el marco SOX, para las empresas que deban certificar en la bolsa de valores de los Estados Unidos.

Es por ello, que se dará a conocer como se protegen las entidades, inclusive todo el proceso que debe efectuarse para cumplir con las normas internacionales, esto con el objetivo de mitigar el riesgo que se encuentran presente en toda las funciones que ejecutan las empresas.

Para dar a entender el tema, se tomo una institución financiera, de capital accionario extranjero y nacional, a su vez se detallará el proceso de control interno bajo la metodología SOX, enfocado de acuerdo a lo indicado por grupo financiero al cual pertenece.

4.2.- Diseño De La Investigación.

El diseño señala al investigador lo que debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se ha planteado y analizar la certeza de la (s) hipótesis formuladas en el contexto en particular. (Roberto, Carlos, & Pilar, 1991).

Para el desarrollo de la investigación que se está desarrollando “Descubrir la metodología SOX”, se usara una investigación no experimental del tipo “diseño transeccionales correlaciónales/causales” que tiene como objetivo describir relaciones entre dos o más variables en un momento determinado. Se trata también de descripciones, pero no de variables individuales sino de sus relaciones, sean estas puramente correlaciónales o relaciones causales (Roberto, Carlos, & Pilar, 1991).

Debido a lo antes mencionado, se toma en consideración este tipo de diseño de investigación bibliográfico, ya que la investigación se ha basado en la investigación de libros, artículos, presentaciones, políticas interna, manuales para

la implementación de metodología SOX, en una institución financiera reconocida en Venezuela.

El análisis de la investigación corresponde a variables causa- efecto que genera las actividades del modelo de control interno (basado en la ley SOX) y el fraude desde esta óptica, dentro de las entidades privadas y los impactos que genera en un sector de la economía.

4.3.- Población y Muestra.

La población se define como el conjunto de todos los casos que concuerdan con una serie de especificaciones (Selltiz, 1974).

La muestra es “en esencia un subgrupo de la población. Básicamente se categorizan a las muestras en dos grandes ramas: las muéstrales no probabilísticas y las muestras probabilísticas. En estas últimas todos los elementos de la población tienen la misma posibilidad de ser escogidos”. (Roberto, Carlos, & Pilar, 1991).

Para el descubrimiento del modelo SOX, se requiere delimitar la población en donde se especificará aquellos que claramente poseen características similares, es por ello que para este caso, se toma en cuenta las entidades financieras que deben certificar SOX anualmente, siempre y cuando, coticen en la bolsa de valores a nivel internacional que a su vez, es regularizada por la SEC (securiti Exchange commission), en donde la propuesta es evaluar los riesgos y los controles que hacen posible la mitigación de los mismos, enfocado en el modelo control interno, por lo que da respuesta a uno de los objetivo específicos que es el fraude desde la óptica SOX.

Cuando se dice que una muestra es representativa indicamos que reúne las características de la población que son significativos para la investigación, para la misma se tomo en consideración las entidades que cotizan de la bolsa de valores internacional.

A nivel nacional, se tomo una institución financiera que posee una composición accionaria de un 55% de capital extranjero y el 45% de capital nacional, en donde es un Banco Universal, es por ello que debe cumplir con una

serie de regularizaciones nacionales e internacionales, dentro de ella está la emisión de la certificación de control interno SOX y No SOX.

Se detallará todo el proceso del modelo de control interno, el perímetro en el cual se marcará los riesgos, de acuerdo a los macroprocesos, procesos y subprocesos luego se incorporaran los riesgos y se determinaran los controles que mitigan los riesgos, el objetivo del modelo de control interno (SOX y NO SOX) es garantizar que las cifras reflejadas en los Estados Financieros se encuentren razonables y adecuados, es decir, son eficaces y efectivos.

4.4.- Técnicas e Instrumentos de recolección de datos.

"Toda medición o instrumento de recolección de los datos debe reunir dos requisitos esenciales: confiabilidad y validez. La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo sujeto u objeto, produce iguales resultados". (Roberto, Carlos, & Pilar, 1991).

Como técnica de recolección de datos se selecciona la recolección de investigación documental, basado principalmente en las leyes y normas regulatorias tanto de políticas internas de las instituciones financieras como de sus entes reguladores, en este caso la SUDEBAN y la casa matriz (nivel corporativo) mediante la ley Sarbanes Oxley. Es por ello, que las instituciones emplean indicadores para medir la evolución económicas, que a la final se basa en los rubros de los estados financieros, que están conformados por cuentas contables, en donde se traducen a nivel cuantitativo los riesgos que se materializaron, es decir, cuentas en donde se registra los fraudes operativos.

En el caso de los fraudes financieros, no existen datos que cuantifiquen estos eventos, sin embargo, existen muestras documentales donde se garantiza el buen funcionamiento de las instituciones y normas que garantizan el buen desempeño de las mismas. Más allá de una norma o política, se refleja a través de las revisiones por parte de los entes supervisoras que dan fe del adecuado funcionamiento de las entidades en Venezuela.

La evaluación del Modelo de Control es uno de los elementos que se utiliza periódicamente para concluir sobre la calidad del ambiente de control cierto en las diferentes unidades del Banco y cierra el proceso que garantiza que los instrumentos de control establecidos previamente se ejecuten de forma eficaz.

4.5.- Validez De La Investigación

"La validez de contenido es compleja de obtener. Primero, es necesario revisar como ha sido utilizada la variable por otros investigadores. Y en base a dicha revisión elaborar un universo de ítems posibles para medir la variables y sus dimensiones (el universo tiene que ser la más exhaustivo que sea factible).

Posteriormente, se consulta con investigadores familiarizados con las variables para ver si el universo es exhaustivo". (Roberto, Carlos, & Pilar, 1991).

El estudio realizado, posee validez, debido a la investigación el instrumento aplicado fue a través de una investigación documental reforzado con el desarrollo que se realiza en una institución financiera que debe aplicar la metodología SOX y a su vez, realizar la certificación de los controles que mitigan los riesgos.

Esto se efectúa de acuerdo a los lineamientos corporativos y para dar cumplimiento a las normas internacionales, por lo que se lleva mediante los procesos, riesgos y controles, que mitigan los riesgos y a nivel financiero, se establece los controles en los procesos contables, que a la final se reflejan en las cuentas contables que su fin es reflejado en los Estados Financieros.

CAPITULO V

PRESENTACIÒN Y ANALISIS DE LOS RESULTADOS.

La institución financiera BBVA Banco Provincial, perteneciente al grupo BBVA Banco Provincial, ha implementado un Modelo de Control Interno que se enmarca dentro de la Gestión Integral de Riesgos, el cual es un proceso que involucra al consejo de administración, el comité de direcciones y a todo el personal del banco. Esto con el fin de identificar los riesgos potenciales a los que se enfrenta la institución y gestionarlo dentro de lo establecido, a fin de asegurar de manera razonable los objetivos del negocio.

5.1- El modelo de control interno del BBVA Banco Provincial, se fundamenta en los siguientes objetivos:

- Dar a conocer a toda la organización el modelo del control, los principios, la estructuras y la organización en que se concreta, contribuyendo de esta manera a promocionar la "cultura del control interno" y establecer la responsabilidad de todo el grupo.
- Constituir un ámbito de actuación de la unidad de control interno unidad de riesgo operacional cumplimiento normativo, auditoría interna, dirección financiera, servicios jurídicos, y las áreas transversales.
- Garantizar que el ambiente de Control de las empresas del grupo BBVA Banco provincial, esta en cuanto a la salvaguarda de los activos, calidad de las operaciones y procesos, el control del reporting financiero y el cumplimiento de las leyes y regulaciones Nacionales o Internacionales que nos afecten. (BBVA BANCO PROVINCIAL, 2008)

5.2.- Alcance del modelo del control interno BBVA Banco Provincial.

Se fundamenta en las mejores prácticas internacionales contenidas en los documentos ARIS "Arquitecture of Integrated Information Systems"- Integrated Framework de COSO (Comité of Sponsoring Organizations of the Treadway Comisión) y el Framework for internal Control Systems in Banking Organizations del BIS (Bank for International Setlement). Estos documentos han servido de guía para el desarrollo del Modelo de Control Interno del BBVA Banco Provincial y sus empresas filiales. El Modelo involucra en el control y en la mitigación de los riesgos a toda la plantilla y muy especialmente, a los responsables de Control Interno y Riesgo Operacional (CIROs) quienes son piezas importantes. (BBVA BANCO PROVINCIAL, 2008).

5.3.- Taxonomía del modelo de control interno.

En el modelo del control interno del grupo BBVA Banco Provincial, se establece en procesos, macroprocesos, subprocesos, riesgos y controles, en los cuales se entienden por "procesos", el conjunto de actividades, especificadas funcionalmente y relacionadas entre sí, que ejecutan los procedimientos o normativa interna preestablecidos, o que debieran estarlo sobre la base de la evaluación de riesgos previamente realizada por las unidades especializadas que correspondan. No obstante la información de los procesos debe ser capaz de satisfacer cualquier requerimiento del regulador o de gestión. (BBVA BANCO PROVINCIAL, 2008).

El riesgo, está basado en el comité COSO en su "Marco de gestión integral de riesgos" (ARIS - Arquitecture of Integrated Information Systems) , en el cual se establece "los riesgos son futuros eventos inciertos, los cuales pueden influir el cumplimiento de los objetivos de las organizaciones, incluyendo sus objetivos estratégicos, operacionales, financieros y de cumplimiento", adicionalmente, el riesgo también se entiende como una medida de la potencial de pérdida económica o lesión en términos de la probabilidad de ocurrencia de un evento no

deseado junto con la magnitud de las consecuencias. El riesgo esta medido por la criticidad y ocurrencia, está basado bajo la nota nro. 3, determinado a nivel corporativo. (BBVA Banco Provincial, 2009).

Los controles, se entiende como cualquier actividad o tarea que permite conocer, gestionar, seguir, reducir o mitigar el riesgo al cual esta expuesto la entidad. Para el caso del BBVA Banco Provincial esta diseñado por un esquema corporativo de controles en base a su naturaleza y criticidad.

Para poder documentar los procesos se debe establecer un mapa de procesos, en este caso el mapa de proceso viene dado por casa matriz, el cual está conformado diversos niveles, los cuales son: procesos de alto nivel (PAN), Diagramación del proceso (DAF) y por último las Variantes. Entiéndase como proceso de alto nivel que es un macroproceso, la diagramación del proceso es el proceso y la variante es el subproceso; este cambio de taxonomía surge por mejoramiento de la herramienta. Cada uno de estos niveles se encuentra segregado por sociedades (Banco y filiales) y países en una única matriz. (Ver anexo I).

El mapa de riesgo, está determinado por el nivel corporativo se ha identificado un listado completo de riesgos para influir directa o indirectamente en los procesos, en el cual se segrega en los siguientes niveles, I. categoría de riesgos: clasificación general según la naturaleza del riesgo, II. Tipos de factores de riesgos: desglose en función de las causas generadoras del riesgo, III. Sub. Factores de riesgos: desglose detallado por causas generadoras de riesgos concretas. (Ver anexo II).

El modelo del control interno se basa fundamentalmente en lograr y mantener estos tres objetivos, garantizar la salvaguarda de los activos contra adquisiciones, uso o disposiciones no autorizadas, garantizar el cumplimiento de las leyes y regularizaciones Nacionales e Internacionales y cumplir con la normativa del reporting financiero SOX.

5.4.- La evaluación del modelo.

El modelo de control interno se separa en dos procesos de revisión, que está conformado por el perímetro SOX y No SOX (control interno), este último corresponde a las procesos que no se encuentran considerados de alto impacto y mayor ocurrencia, se encuentran catalogados como riesgos con menor criticidad (menores a 4), en el caso del perímetro SOX son riesgos con mayor criticidad (superior a 4). (BBVA Banco Provincial, 2008)

Adicionalmente, se debe destacar que de acuerdo a la determinación del riesgo atachada a las variantes, diagramación de procesos, procesos de alto nivel, cuando se levantan los controles (indicado por el área responsable) se determina la frecuencia del control (se refiere a cada cuanto tiempo se realiza la actividad), este es determinante, porque dicha información se emplea para tomar la muestra y meses a validar. (BBVA Banco Provincial, 2008) .

- **Cuadro Nº 1** Frecuencia de la muestra

		Inherent Risk > 4	Inherent Risk = 4
Naturaleza del control	**Frecuencia de realización**	**Número mínimo selecciones**	**Número mínimo selecciones**
Manual	Por operación	25	5
Manual	Diaria	15	3
Manual	Semanal	5	1
Manual	Mensual / Quincenal	2	1
Manual	Trimestral	1 por trimestre	1 por trimestre
Manual	Anual	1	1
Automático	Verificar una actividad por cada control automático		

Fuente: nota 2 2008 Perímetro SOX y plan de pruebas. BBVA Banco Provincial Corporativo.

- **Cuadro Nº 2** Criticidad del Perímetro

Frecuencia de realización	Selección de elementos por periodicidad y Inherent Risk > 4
Por operación	Primera del mes anterior y las sucesivas hasta alcanzar 17 muestras. Si no hubiera suficientes hasta completar las 17, continuar con las inmediatamente anteriores a la primera seleccionada. Adicionalmente, tomar las 8 restantes con el mismo criterio, a partir de la primera del tercer mes anterior a la fecha de testing. Ejemplo: Testing en Octubre. 17 muestras de Septiembre y 8 de Julio.
Diaria	Último viernes hábil del mes anterior al Testing, ese día y los anteriores, hasta alcanzar 10 muestras. Adicionalmente, tomar las 5 restantes con el mismo criterio a partir del último viernes hábil del tercer mes anterior al testing. Ejemplo: Testing en Octubre. A partir del 28 de Septiembre, tomar 10 muestras - ese día y los anteriores. A partir del 27 de Julio, tomar 5 muestras – ese día y los anteriores.
Semanal	Última semana del mes anterior al Testing, esa semana y las anteriores, hasta alcanzar 3 muestras. Adicionalmente, tomar las 2 restantes con el mismo criterio a partir de la última semana del tercer mes anterior al Testing. Ejemplo: Testing en Octubre. A partir de la semana del Lunes 24 de Septiembre, tomar 3 muestras – esa semana y las anteriores. A partir de la semana del 23 de Julio, tomar 2 muestras – esa semana y las anteriores.
Quincenal	Última quincena mes anterior al Testing. Esa quincena y las anteriores.
Mensual	Mes anterior a la fecha del Testing. Ese mes y los anteriores
Trimestral	El último anterior a la fecha del Testing.
Anual	El último anterior a la fecha del Testing.
Aperiódico	Se considerará como un control “Por operación”.

Cuadro Nº 2 (Cont.)

Frecuencia de realización	Selección de elementos por periodicidad y Inherent Risk = 4
Por operación	Primera del mes anterior y las sucesivas hasta alcanzar 3 muestras. Si no hubiera suficientes hasta completar las 3, continuar con las inmediatamente anteriores a la primera seleccionada. Adicionalmente, tomar las 2 restantes con el mismo criterio, a partir de la primera del tercer mes anterior a la fecha de testing. Ejemplo: Testing en Octubre. 3 muestras de Septiembre y 2 de Julio.

Frecuencia de realización	Selección de elementos por periodicidad y Inherent Risk = 4
Diaria	Último viernes hábil del mes anterior al Testing, ese día y los anteriores, hasta alcanzar 2 muestras. Adicionalmente, tomar la restante con el mismo criterio a partir del último viernes hábil del tercer mes anterior al testing. Ejemplo: Testing en Octubre. A partir del 28 de Septiembre, tomar 2 muestras - ese día y los anteriores. A partir del 27 de Julio, tomar 1 muestra.
Semanal	Última semana del mes anterior al Testing.
Quincenal	Última quincena mes anterior al Testing.
Mensual	Mes anterior a la fecha del Testing.
Trimestral	El último anterior a la fecha del Testing.
Anual	El último anterior a la fecha del Testing.
Aperiódico	Se considerará como un control "Por operación".

Fuente: nota 2 2008 Perímetro SOX y plan de pruebas. BBVA Banco Provincial Corporativo.

5.4.1. - Perímetro SOX

La definición del perímetro se efectúa todos los años, durante los meses de abril y mayo, bajo la coordinación del área de Control Interno y todos los gestores CIRO de las unidades, en función de la criticidad de los riesgos y aplicando los criterios mínimos para todos los riesgos pertenecientes ha:

- Procesos críticos: incluye procesos masivos (actividades que incorporan una importante fuente de pérdidas para la unidad), procesos externalizados y tecnológicos, entre otros.
- Que estén sometidos a una regulación especial.
- Relacionados con recomendaciones de auditoría interna y externa.

Además de estos riesgos, las unidades incluyeron aquellos que consideraron más relevantes. La evaluación del perímetro de Control Interno permite centrar la atención en los riesgos que realmente son relevantes para las áreas. El objetivo de esta evaluación es definir aquellos controles asociados a los riesgos que

incorporen un mayor riesgo en el ámbito de actuación de cada una de las unidades de negocio y soporte, dando prioridad a las actuaciones que aporten mayor eficacia en el cumplimiento de las metas fijadas.

La definición del perímetro, como todos los años, tiene dos alcances:

- Perímetro SOX: definido de forma centralizada por el área Financiera Corporativa.
- Perímetro CI: responsabilidad de las unidades y gestores CIRO locales.

El perímetro SOX es determinado por casa matriz, a través de Control Interno Información Financiera Corporativo (CIIFC), que luego es comunicada a cada país, en este caso Control Interno de Información Financiera Venezuela (CIIFV) y se realiza en función a la materialidad del importe establecido en los estados financieros, específicamente del balance general y sus rubros y los mismos serán objeto de revisión SOX, donde se va a involucrar todo el proceso mediante el cual se llega al importe reflejado en las cifras de los estados financieros. (BBVA Banco Provincial, 2009).

Una vez obtenido la materialidad que abarcará el perímetro se procede a marcar en la herramienta ARIS "Arquitecture of Integrated Information Systems", tomando en consideración los procesos de alto nivel que se encuentran dentro del perímetro, esto con la finalidad de marcar los riesgos y controles que son de alto riesgos y mayores impactos de ocurrencia. Para posteriormente poder realizar el testeo de los controles, en el cual se certifica la efectividad del control en donde se mitiga el riesgo, generando la certificación de SOX.

5.4.2. El Testing SOX y NO SOX

El proceso de revisión SOX y No SOX (Control Interno), tienen los mismos procedimiento, está conformado por las revisiones de control interno financiero y control interno riesgo país, auditoría interna y auditoría externa.

Anualmente se realiza el testing, la actividad principal es probar los controles que mitigan los riesgo, esto de acuerdo al trabajo efectuado en la

herramienta ARIS “Arquitecture of Integrated Information Systems”, en el cual cada proceso de alto nivel, posee n cantidad de diagramación de procesos y los mismos poseen n cantidad de variantes, que a su vez poseen riesgos y controles que lo mitigan, en dicha herramienta se realiza el marcaje de los riesgos y controles SOX y No SOX.

Primero se inicia con la revisión SOX, para el mes de julio, realizada por control interno financiera y control interno riesgo país (ambas áreas en Venezuela), luego el testing control interno No SOX, se realiza en el mes de Septiembre. Una vez efectuada la revisión por los sectores de control interno se efectúa un informe en el cual se coloque las observaciones de los controles testeados y es informado a los responsables de las áreas para su adecuada corrección y modificación.

Luego, para el período de Noviembre, entra la revisión de auditoría interna del banco para realizar la revisión de los controles SOX y No SOX, la diferencia en este testing es la amplitud de la muestra, considerando distintos meses, a la final los controles y riesgos son los mismo testeados en el mes de Julio y Septiembre por los sectores de control interno.

En el mes de Diciembre, entra la revisión de auditoría externa, en el cual realizan el re-testing de los controles y riesgos que fueron revisados anteriormente, igualmente la muestra puede variar, lo que sigue siendo igual es la evidencia, pues el objetivo es certificar la efectividad de los controles de la entidad financiera, en esta certificación se reflejará si existe alguna debilidad.

Una vez, realizada la certificación en borrador por auditoria externa, la Unidad de Contabilidad de la Vicepresidencia Financiera efectúa reunión con la Directiva de la firma (auditores externos), en el cual se exponen las conclusiones obtenidas y posibles aspectos a mejorar de la institución en cuestión. Se efectúa la reunión con la unidad de Contabilidad, ya que es la unidad responsable de los controles que mitigan los riesgos SOX.

Se procede por parte de la firma realizar la certificación definitiva SOX, en la cual es firmada por todo los responsables del proceso SOX.

CONCLUSIONES.

En el trabajo de especialización desarrollado el objetivo general es descubrir la metodología del modelo del control interno, es por ello que la evaluación del modelo de control es uno de los mecanismos que se utiliza recurrentemente para concluir sobre la calidad del ambiente de control existente en las diferentes unidades del Banco y cierra el proceso que garantiza que los instrumentos de control establecidos previamente se ejecuten de forma eficaz.

La evaluación se debe realizar en virtud de la criticidad de los procesos y riesgos de cada unidad, y se aborda con carácter periódico (anual) mediante la realización de un *testing* durante el segundo semestre de cada año, el cual es aplicado por el área de Control Interno, luego auditoría interna y por último auditoría externa.

Previo a la ejecución del *testing* es necesario que cada unidad, a través de los propietarios de los procesos y los gestores CIRO, determine el perímetro de evaluación y de gestión para cada año.

Por lo antes señalado, se concluye que la metodología del control interno es anticiparse a los posibles riesgos que siempre se encuentra latente en todas las actividades que se realizan en las empresas y a su vez, repercute en la imagen y estabilidad de las mismas. Adicionalmente, esta ley ha permitido establecer los niveles de responsabilidades por parte de las personas que conforma una organización, desde los niveles de responsabilidad de las instituciones y a su vez de los entes revisores, que en estos casos señalan a las firmas de auditorías. Esto con la finalidad de prevenir el fraude desde la óptica SOX, pues involucra una serie de procesos que se deben desarrollar para garantizar el buen funcionamiento de las instituciones, en especial las actividades financieras.

Se ha detectado que mediante esta metodología, se han identificado controles con fallas en diseño y por ende no mitigan los riesgos, así como la falta de dichos controles en algunos procesos o los mismos son débiles o no son suficientes para mitigar los riesgos; por lo que es una metodología útil y que garantiza la estabilidad de las instituciones a nivel de procesos.

RECOMENDACIONES.

- Las empresas que deseen generar un modelo de control interno, debe establecer principalmente una adecuada segregación de funciones y así como también una estructura organizativa formalizada, motivado al que modelo de control interno se fundamenta bajo la normativa SOX y por ende está enfocado a los procesos de las organizaciones, que obtienen como resultado el reflejo en los estados financieros y sus operaciones diarias. En caso, contrario no se podría determinar los procesos, variantes (subprocesos), riesgos y controles, donde puedan existir riesgo y menos determinar los niveles de responsabilidad.
- De ser necesario se recomienda implementar **n** cantidad de controles que mitiguen los riesgos, de ser requeridos y a su vez se encuentren adecuadamente diseñados, con el objetivo de garantizar la eficiencia y efectividad de los mismos.

BIBLIOGRAFIA

Textos.

BBVA BANCO PROVINCIAL. (2008). Modelo de control interno del grupo BBVA Banco Provincial nro. 00.30.009. Caracas: Banco Provincial S.A.

BBVA Banco Provincial. (2009). Nota 3 - 2009 . Caracas.

Roberto, S., Carlos, C., & Pilar, L. (1991). Metodologia de la Investigacion. (p. 505). Mexico: Mc Graw Hill.

Yaselli, M. B. (2003). Manual de trabajos de grado de especialización y maestrias y tesis doctorales. In M. B. Yaselli, Manual de trabajos de grado de especialización *y maestrias y tesis doctorales* (p. 215). Caracas: FEDUPEL.

Tesis:

Briceño, M. (2010, Mayo). *Evaluacion del control interno administrativo bajo procesamiento electrónico de datos basado en el modelo COSO en la Direccion de hacienda de la alcaldia Municipio Urdaneta del Edo. Trujillo.* Retrieved mayo 11, 2010, from biblioteca.universia.net: http://biblioteca.universia.net

Castillo, D. (2010). *biblioteca.universia.net.* Retrieved Mayo 11, 2010, from http://biblioteca.universia.net

Rios Alfonso, C. R. (2009, Marzo). *Instituto politecnico nacional, Escuela superior y administraciòn, Unidad Tepepan*. Fraude como fenomeno economico. Retrieved junio 05, 2010, from http//itzamna.bnct.ipn.mxc

Pàginas web.

Daniel, C. (2005, Septiembre). *Normaria Boletin del Comite de Normas del Instituto de Auditores Internos de Argentino Nro. 20* . Retrieved Mayo 09, 2010, from www.nor-mas.iaia.org.ar

Deloitte&Touche, D. &. (2008, septiembre 3). ley sarbanes-Oxley. Retrieved mayo 17, 2010, from deloitte & touche: htt//www.deloitte.com/sarbanes

5.555, G. O. (2001). *Ley General de Bancos y Otras Instituciones Financieras.* Caracas.

Gutierrez, H. (2004). *auditoria y seguridad informática*. Retrieved 05 30, 2010, from http://www.auditoria.com: http://www.auditoria.com.mx

http://es.wikilingue.com/pt/Ley_Sarbanes-Oxley. (s.f.). Recuperado el Mayo de 2010

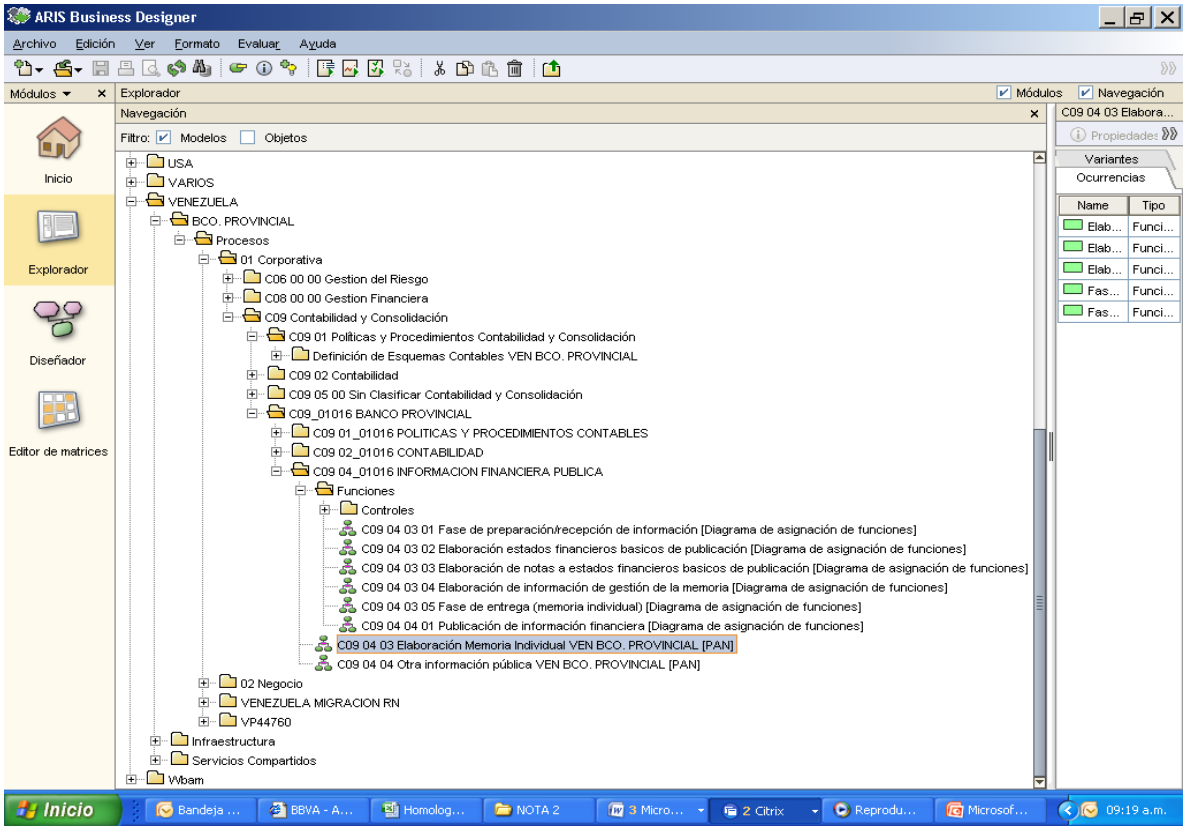
Iturbide, F. (2005). *Economia y negocio*. Retrieved 05 30, 2010, from http://www.economiaynegocios.uahurtado

UCES Auditoria de Sistemas y Software. (n.d.). Retrieved mayo 09, 2010, from Trabajo pràctico: ley de Sabarnes - Oxley: www.megapuntes.com.ar

SUDEBAN. (2003, 05 29).Resolucion 136.03 SUDEBAN.gov.ve. Retr abril 15, 2010, from www.sudeban.gov.ve

ANEXO I

MATRIS DE CONTROL INTERNO
Herramienta ARIS “Arquitecture of Integrated Information Systems”


ARIS Business Designer
Archivo Edición Ver Formato Evaluar Ayuda
Módulos
Explorador
Navegación
Módulos Navegación
Inicio
Explorador
Diseñador
Editor de matrices
Navegación
Filtro: Modelos Objetos
USA
VARIOS
VENEZUELA
BCO. PROVINCIAL
Procesos
01 Corporativa
C06 00 00 Gestion del Riesgo
C08 00 00 Gestion Financiera
C09 Contabilidad y Consolidación
C09 01 Políticas y Procedimientos Contabilidad y Consolidación
Definición de Esquemas Contables VEN BCO. PROVINCIAL
C09 02 Contabilidad
C09 05 00 Sin Clasificar Contabilidad y Consolidación
C09_01016 BANCO PROVINCIAL
C09 01_01016 POLITICAS Y PROCEDIMIENTOS CONTABLES
C09 02_01016 CONTABILIDAD
C09 04_01016 INFORMACION FINANCIERA PUBLICA
Funciones
Controles
C09 04 03 01 Fase de preparación/recepción de información [Diagrama de asignación de funciones]
C09 04 03 02 Elaboración estados financieros basicos de publicación [Diagrama de asignación de funciones]
C09 04 03 03 Elaboración de notas a estados financieros basicos de publicación [Diagrama de asignación de funciones]
C09 04 03 04 Elaboración de información de gestión de la memoria [Diagrama de asignación de funciones]
C09 04 03 05 Fase de entrega (memoria individual) [Diagrama de asignación de funciones]
C09 04 04 01 Publicación de información financiera [Diagrama de asignación de funciones]
C09 04 03 Elaboración Memoria Individual VEN BCO. PROVINCIAL [PAN]
C09 04 04 Otra información pública VEN BCO. PROVINCIAL [PAN]
02 Negocio
VENEZUELA MIGRACION RN
VP44760
Infraestructura
Servicios Compartidos
Wbam
C09 04 03 Elabora...
Propiedades
Variantes
Ocurrencias
Name Tipo
Elab... Funci...
Elab... Funci...
Elab... Funci...
Fas... Funci...
Fas... Funci...
Inicio
Bandeja ...
BBVA - A...
Homolog...
NOTA 2
3 Micro...
2 Citrix
Reprodu...
Microsof...
09:19 a.m.

ANEXO II

MODELO DEL RIESGOS PROYECTO SOX

MODELO DE RIESGOS PROYECTO SOX

10 PROCESOS

Se incluyen en esta categoría todos los errores ocasionados por el procesamiento de operaciones o en la gestión de procesos, así como de relaciones *con contrapartes comerciales y proveedores".*

En consecuencia, se encuadrará dentro de este grupo todos los errores originados por un evento en el que concurran las siguientes condiciones:

- El error haya sido provocado por acción u omisión en la ejecución de operaciones, errores involuntarios cometidos en la operativa y gestión de procesos.
- Que no haya supuesto un beneficio directo para la entidad.

101 errores en la operativa

Este grupo recogerá todos los eventos que no tengan cabida en el resto de los apartados de esta categoría. Es decir la asignación se realizará por exclusión.

En particular, se incluirán todos los eventos que supongan un error directo para la entidad, como consecuencia de:

- errores en la introducción y mantenimiento de datos,
- ejecución deficiente de procedimientos de control,
- comunicaciones realizadas a otras contrapartidas y corresponsales y,
- en general, cualquier fallo en el funcionamiento de los procesos habituales de la entidad no contemplados en las siguientes subcategorías.

101O1	en órdenes de clientes
	Errores ocasionados por deficiencias en la ejecución de órdenes de clientes a consecuencia de falta de diligencia en la tramitación o deficiente interpretación de las mismas. (Órdenes de compra/venta de Valores, suscripciones... órdenes de transferencias – individuales, masivas y permanentes– operaciones de Cuentas Personales, Préstamos, Medios de Pago, Fondos, etc.).
101O2	en la operativa (entrada datos, duplicidades, retrasos, caja, etc.)
	Errores o duplicidad en la entrada de datos. Afecta a todo tipo de datos (límites, importes, plazos, referencias,etc.) en toda clase de operaciones (operativa de Caja, cobros, pagos, liquidaciones, extravío de remesas de moneda nacional o divisas, liquidación de impuestos y seguros sociales, extranjero, etc.).
101O3	en las comunicaciones a clientes
	Errores involuntarios en el suministro de información obligatoria (en contenidos y plazos de entrega) que deba remitirse a: - Clientes - Inversores - Organismos e instituciones. etc; cualquiera que sea el medio por el que se cursen, excepto la la transmisión mediante sistemas telemáticos, en cuyo caso, la pérdida se clasificará como "Riesgo Tecnológico".
101O4	en modelos de precios/riesgos
	Implantación o funcionamiento deficiente de modelos de valoración, de riesgos, de determinación precios, etc.
101O5	en liquidaciones de operaciones y contratos.
	Errores originados en la liquidación de contratos de productos de Activo, Pasivo y Servicios.
101O6	divulgación involuntaria de información sensible
	Divulgación no intencionada de información privilegiada, etc.
101O7	errores y omisiones en el diseño de procedimientos/circuitos
	Deficiencias en el diseño y/o implantación de productos, sistemas, elaboración y divulgación de tareas y procedimientos, etc.
101O8	en el planteamiento de procesos judiciales
	Incorrecto planteamiento o enfoque en litigios, demandas, reclamaciones de deuda, recursos, oferta de servicios, mandatos de asesoramiento, etc.
101O9	Incorrecto reflejo en contabilidad de la operativa
	Errores directos en el reflejo contable de las cuentas patrimoniales, transitorias, de orden etc.
1011:0	Diferencias en inventarios
	Errores cometidos en los cuadres y conciliaciones periódicas.
1011:1	Errores en la verificación de firmas y/o poderes (Por tratarse de una deficicincia en un control este riesgo no será de aplicación)
	Deficiencias en la validación e intervención de documentos.
1011:2	Errores en el control ficheros externos (RAI, ASNEF, CIRBE, ETC ...)
	Errores u omisiones registradas en el acceso a sistemas externos de calidad del crédito, listas "Robinson", etc.

103 Incumplimiento de la normativa

Riesgo que tiene su origen en el incumplimiento o errónea interpretación de normas de todo tipo, excepto laborales, que deban ser aplicadas por la Entidad, y tanto si se debe a procesos defectuosamente diseñados como a errores de ejecución de los mismos.
Cuando los incumplimientos estén relacionados con la normativa laboral, se clasificarán en la categoría de "**Recursos Humanos**".

10301 legal general (Código Comercio, ley S.A., etc...)

Multas y sanciones derivadas de infracciones cometidas en el cumplimiento de obligaciones societarias, en general no incluidas en los subgrupos siguientes.

10302 Ley de Protección de Datos

Incumplimiento de la LOPD. Pérdidas por reclamaciones relacionadas con información errónea facilitada a organismos, instituciones, registros de calidad de crédito (ASNEF, RAI, etc.), medios de comunicación, etc.

10303 fiscal

Penalizaciones por infracciones cometidas en el cumplimiento de obligaciones tributarias, impago o evasión de impuestos y otras contingencias de carácter fiscal.

10304 reguladores nacionales (BdE, CNMV, DGS, etc..)

Multas y sanciones impuestas por organismos supervisores a consecuencia del incumplimiento en la presentación (plazos y contenidos) de cualquier tipo de información, de obligaciones formales frente a clientes, etc.

10305 reguladores internacionales (Fed, Sec, etc..)

Multas y sanciones impuestas por organismos supervisores internacionales a consecuencia del incumplimiento de otras normas de obligado cumplimiento.

10306 registros públicos

Otras multas, sanciones y recargos originados por la falta de diligencia en el registro de documentos en general.

10307 normativa de edificios

Multas, sanciones y recargos satisfechas a organismos: Comunidades autónomas, ayuntamientos, etc., relacionadas con el incumplimiento de normativa de seguridad, de mantenimiento, de publicidad, etc., en edificios propiedad de la entidad o alquilados cuando sanción recaiga por la omisión en el cumplimiento de obligaciones del arrendatario.

10308 En la elaboración de estados financieros

Incumplimiento de normas relacionadas con la obligación del reporting financiero. Informes financieros inexactos, fuera de plazo, etc.

104 Errores en la gestión y administración de cuentas de clientes

Se recogen en esta subcategoría las errores provocados por la ejecución inadecuada o negligente **tratamiento de instrucciones y órdenes impartidas por clientes**, ocasionados por el uso indebido de la cuenta del cliente, la ejecución errónea de cualquier tipo de instrucciones, la demora en su tramitación, etc.

Cuando el error sea consecuencia de fallos en los procesos internos, normalmente tendrán repercusión sobre un amplio colectivo de clientes. En este caso el evento se clasificará en la subcategoría "**Errores en la operativa**".

Si el control y ejecución de estas instrucciones reside en los sistemas de información de la entidad, el error rovocado por un defecto en su funcionamiento se clasificará como "**Riesgo Tecnológico**".

10401 en circuitos de notificación y recepción de instrucciones

Errores en las Comunicaciones emitidas. Pérdidas ocasionadas por deficiencias en las comunicaciones remitidas a clientes.

10402 errores u omisiones en el ejercicio de derechos del cliente

Errores causados en la gestión y administración de activos por falta de diligencia u omisión en el ejercicio de los derechos de un cliente, en la administración de depósitos, gestión de carteras, aportaciones a fondos, custodia de valores, fiducias y otros vehículos de inversión.

MODELO DE RIESGOS PROYECTO SOX

10 PROCESOS

Se incluyen en esta categoría todos los errores ocasionados por el procesamiento de operaciones o en la gestión de procesos, así como de relaciones *con contrapartes comerciales y proveedores".*

En consecuencia, se encuadrará dentro de este grupo todos los errores originados por un evento en el que concurran las siguientes condiciones:

- El error haya sido provocado por acción u omisión en la **ejecución de operaciones, errores involuntarios** cometidos en la operativa y gestión de procesos.
- Que no haya supuesto un **beneficio** directo para la entidad.

101 errores en la operativa

Este grupo recogerá todos los eventos que no tengan cabida en el resto de los apartados de esta categoría. Es decir la asignación se realizará por **exclusión.**

En particular, se incluirán todos los eventos que supongan un error directo para la entidad, como consecuencia de:

- errores en la introducción y mantenimiento de **datos,**
- ejecución deficiente de procedimientos de **control,**
- **comunicaciones** realizadas a otras contrapartidas y corresponsales y,
- en general, cualquier **fallo en el funcionamiento de los procesos** habituales de la entidad no contemplados en las siguientes subcategorías.

101O1	en ordenes de clientes
	Errores ocasionados por **deficiencias en la ejecución de órdenes de clientes** a consecuencia de falta de diligencia en la tramitación o deficiente interpretación de las mismas. (Órdenes de compra/venta de Valores, suscripciones... órdenes de transferencias - individuales, masivas y permanentes- operaciones de Cuentas Personales, Préstamos, Medios de Pago, Fondos, etc.).
101O2	en la operativa (entrada datos, duplicidades, retrasos, caja, etc.)
	Errores o duplicidad en la entrada de datos. Afecta a todo tipo de datos (límites, importes, plazos, referencias,etc.) en toda clase de operaciones (operativa de Caja, cobros, pagos, liquidaciones, extravío de remesas de moneda nacional o divisas, liquidación de impuestos y seguros sociales, extranjero, etc.).
101O3	en las comunicaciones a clientes
	Errores involuntarios en el **suministro de información obligatoria** (en contenidos y plazos de entrega) que deba remitirse a: - Clientes - Inversores - Organismos e instituciones. etc; cualquiera que sea el medio por el que se cursen, excepto la la transmisión mediante sistemas telemáticos, en cuyo caso, la pérdida se clasificará como **"Riesgo Tecnológico".**
101O4	en modelos de precios/riesgos
	Implantación o funcionamiento deficiente de modelos de valoración, de riesgos, de determinación precios, etc.
101O5	en liquidaciones de operaciones y contratos.
	Errores originados en la liquidación de contratos de productos de Activo, Pasivo y Servicios.
101O6	divulgación involuntaria de información sensible
	Divulgación no intencionada de información privilegiada, etc.
101O7	errores y omisiones en el diseño de procedimientos/circuitos
	Deficiencias en el diseño y/o implantación de productos, sistemas, elaboración y divulgación de tareas y procedimientos, etc.
101O8	en el planteamiento de procesos judiciales
	Incorrecto planteamiento o enfoque en litigios, demandas, reclamaciones de deuda, recursos, oferta de servicios, mandatos de asesoramiento, etc.
101O9	Incorrecto reflejo en contabilidad de la operativa
	Errores directos en el reflejo contable de las cuentas patrimoniales, transitorias, de orden etc.
1011:0	Diferencias en inventarios
	Errores cometidos en los cuadres y conciliaciones periódicas.
1011:1	Errores en la verificación de firmas y/o poderes (Por tratarse de una deficicincia en un control este riesgo no será de aplicación)
	Deficiencias en la validación e intervención de documentos.
1011:2	Errores en el control ficheros externos (RAI, ASNEF, CIRBE, ETC ...)
	Errores u omisiones registradas en el acceso a sistemas externos de calidad del crédito, listas "Robinson", etc.

20 FRAUDE EXTERNO

Para poder calificar un evento de fraude externo es necesario evaluar la intencionalidad con que se han realizado las acciones que desencadenaron el error, diferenciando si existe o no ánimo de lucro.
Si existió ánimo de lucro cuando la persona que comete la acción persigue un beneficio personal ilícito (obtención de provecho o enriquecimiento para sí mismo o para un tercero, en perjuicio de la entidad).
Sin embargo, si ha existido intención de provocar un daño sin ánimo de lucro el evento se clasificará en **Desastres, Riesgo Tecnológico, etc...**

201 uso fraudulento de tarjetas

En esta subcategoría se incluyen los fraudes cometidos sin intervención de personal vinculado a la entidad, por clientes o terceras personas, mediante la utilización de instrumentos de medios de pago o a través de cualquiera de los sistemas implantados para su administración y gestión.

20101	**uso indebido por terceros (falsificación, clonación, etc...)**
	Demoras en la tramitación de órdenes de cancelación de tarjetas robadas/extraviadas, tanto de débito como de crédito, suplantación de personalidad, etc.
20102	**utilización por el titular**
	Utilización fraudulenta de este instrumento de pago por el/los titular/es del contrato (cuando la pérdida no sea imputable a riesgo de crédito).

202 robos y atracos

Robos y atracos perpetrados contra activos de la Entidad.

20201	**robos y atracos (oficinas, cajeros automáticos, etc..)**
	Se trata de pérdidas ocasionadas por el robo, hurto o atraco mediante el cual se produce la pérdida de activos materiales o financieros propiedad de la entidad.

203 otros fraudes externos

Se clasificarán en este grupo aquellas pérdidas originadas por el resto de actividades delictivas realizadas por personas ajenas a la entidad, mediante alguno de los medios que se detallan en los siguientes apartados.

20301	**uso fraudulento de cheques, transferencias, pagarés y efectos**
	Pérdidas por pagos contra documentos sin fondos cuando no pueda ser considerado Riesgo de Crédito.
20302	**falsificación de documentos**
	Quebrantos originados por la manipulación en cualquier tipo de operación (activo, pasivo y servicios), de documentos mercantiles, contractuales e informativos: Contratos, poderes, Efectos de Comercio, Cheques, Billetes, Cartas de Pago, etc.
20303	**suplantación de la personalidad**
	Fraudes comtidos mediante esta modalidad.
20304	**estafas**
	Pérdidas por estafas sufridas por la entidad.
20305	**uso y/o divulgación de información sensible**
	Pérdidas por ocasionadas por el uso y/o divulgación cualquier información por personas no vinculadas a la entidad que hayan tenido acceso a este tipo de información .
20306	**espionaje industrial**
	Robo de información propiedad de la entidad. (p.e. Base de datos de clientes, información confidencial, etc.).
20307	**extorsión y soborno**
	Pérdidas originadas a consecuencia de este tipo de delitos.
20308	**secuestros y rescates**
	Pérdidas por gastos y pagos satisfechos como consecuencia de secuestros de empleados.

204 violación de la seguridad informática

Riesgos vinculados a la violación de los sistemas de seguridad lógica implantados por la entidad, por personas ajenas a la misma.

20401	**utilización inadecuada de claves de acceso**
	Vulneración de claves de acceso y/o niveles de autorización, independientemente del canal en que se produzcan: Banca Telefónica, Banca Electrónica, Banca Automática, Internet, etc.
20402	**fraudes a través del ordenador (hackers, crakers, etc...)**

Pérdidas directas y sanciones relacionadas con fraudes y otros delitos (ej. piratería informática, accesos no autorizados, sabotaje de datos críticos, virus introducidos, robo de información, etc.) a través del uso irregular de los sistemas del Banco.

30 FRAUDE INTERNO

Para que exista Fraude interno se precisa la participación o colaboración probada de una persona vinculada a la entidad

Cuando la acción persiga el lucro de la persona que ejecuta la acción se clasifica en la subcategoría de **"robos y fraudes"**. En caso de que se haya realizado sin ánimo de lucro se clasificará en el grupo denominado **"Actividades no autorizadas"**.

Se considerará existe ánimo de lucro cuando la persona que comete la acción persigue un beneficio personal ilícito (obtención de provecho o enriquecimiento para sí mismo o para un tercero, en perjuicio de la entidad).

301 robos y fraudes

Riesgo de pérdidas ocasionadas por actuaciones irregulares, comisión de hechos delictivos, infidelidades, abuso de confianza, etc. efectuadas con ánimo de dolo o lucro por parte del personal interno de la entidad.

30101	**falsificación de documentos**
	Por medio de la manipulación de documentos mercantiles, contractuales, informativos, etc.
30102	**vulneración de sistemas de identificación**
	mediante la utilización fraudulenta de las claves de acceso y/o niveles de autorización. Utilización fraudulenta de password por personas distintas al titular.
30103	**desfalco y malversación**
	Pérdidas causadas por la apropiación de activos del banco.
30104	**uso y/o divulgación de información sensible**
	Pérdidas por pérdidas directas, indemnizaciones y sanciones debidas al uso, con ánimo de lucro, de este tipo de información.
30105	**espionaje industrial**
	Robo de información propiedad de la entidad. (p.e. Base de datos de clientes, información confidencial, etc.).
30106	**extorsión y soborno**
	Pérdidas como resultado de pagos, multas o sanciones como consecuencia de delitos de esta naturaleza cometidos por personal vinculado a la entidad.
30107	**banca paralela**
	Pérdidas causadas por la apropiación de activos de clientes del banco.

302 actividades no autorizadas

Riesgo de pérdidas ocasionadas por el uso incorrecto de los poderes conferidos a cualquier miembro de la Entidad y por la realización de operaciones sin que existan atribuciones, independientemente del medio utilizado para realizar esas actividades: a través de sistemas informáticos (incluida utilización de password o claves de usuarios de otras personas), firma de documentos, autorizaciones, etc.

30201	**uso indebido de poderes/límites**
	Quebrantos producidos a consecuencia de la incorrecta utilización de facultades delegadas: Aprobación del riesgo en operaciones con clientes (préstamos, líneas de crédito, exceso de límites, etc.) y aplicación incorrecta de los criterios de consolidación de cifras de riesgo en grupos de empresa y, en general, incumplimiento de la política establecida en la concesión y realización de todo tipo de operaciones financieras. Autorización de precios no autorizados en cualquier tipo de operación: Activo, Pasivo o Servicios; transacciones con otros agentes económicos, etc.
30202	**divulgación de información sensible**
	Pérdidas relacionadas con la difusión de información, cuando no existe autorización para ello y se realiza sin ánimo de lucro.
30203	**manipulación de la contabilidad de gestión**
	Aplicación de criterios y procedimientos inadecuados en la elaboración de la contabilidad de gestión de la unidad.
30204	**inexistencia o deficiencia en el circuito de fijación de facultades**
	Pérdidas relacionadas con el abuso de facultades conferidas a causa de errores de interpretación respecto a los límites de las mismas.

40 TECNOLOGÍA

Se clasifica en esta categoría todos los riesgos asociados al uso y utilización de herramientas informáticas desde el punto de vista del usuario. Todos los riesgos tecnológicos relacionados con el diseño, mantenimiento y explotación de las explotaciones se encuentrarán recogidos los macroprocesos Ciclo Productivo de Infraestructura Tecnológica, Ciclo Productivo de Aplicaciones y Explotación de la Tecnología Se considera un "fallo en los sistemas informáticos" al deficiente funcionamiento del "hardware" o equipamiento (cualquiera que sea su ubicación) y al "software" cuyo desarrollo y mantenimiento sea competencia exclusiva de la Unidad de Sistemas de Información de la entidad.

401 funcionamiento inadecuado de la aplicación

En particular corresponderá a pérdidas asociadas a la ejecución de procesos concretos, deficiente funcionamiento de las líneas de comunicaciones, pérdidas de información en los dispositivos de respaldo, deficiente funcionamiento de aplicaciones por nos responder a las especificaciones del usuario, carencias en los sistemas de seguridad lógica, de la infraestructura tecnológica y del edificio de proceso de datos, etc.

40101	funcionamiento inadecuado de la aplicación (software)
	Errores originados por deficiencias en el nivel de servicio, provocadas por la ejecución incorrecta de procesos establecidos, incompatibilidad entre sistemas, módulos y/o aplicativos, falta de conectividad on line entre aplicativos o interfaces, errores (abend's) o demoras en procesos batch planificados, que retrasen la apertura del servicio on-line, pérdida de información por incorrecto funcionamiento de los sistemas de respaldo y seguridad, etc.
40102	Errores en el uso y/o administración por parte de los usuarios de los SI.
40103	degradación del rendimiento de los sistemas de infomación
40104	el nivel de servicio ofrecido por el software no cubre las expectativas de negocio por indefinición del mismo
40105	incapacidad en la medición del nivel de servicio ofrecido por el software (indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
40106	ineficiencia en la medición del nivel de servicio ofrecido por el software(indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
40107	degradación del rendimiento y la capacidad de los recursos software
40108	incumplimiento de los niveles de servicio del software definidos respecto a la cantidad y calidad del servicio ofertado
40109	Imposibilidad de utilización de las aplicaciones por parte de los usuarios, a causa de un inadecuado soporte de TI.
40110	problemas e incidentes software recurrentes y/o no resueltos
40111	ineficiencia en la operación de los sistemas de información
40112	errores en el proceso de operación
40113	pérdida de confiabilidad de los datos tras la ejecución de un proceso
40114	Pérdida de integridad transaccional del número de registros tratados en la ejecución de un proceso
	La operación masiva ejecutada no considera todos los registros de entrada que deben ser procesados y/o no da como resultado el número de registros adecuados. En la ejecución del proceso se puede incurrir en pérdida de: --> Unicidad: Cada registro que debe ser tratado es procesado una única vez.
40115	Inexactitud del proceso
	Los datos han sufrido modificaciones no esperadas durante el procesamiento porque no han sido captados, grabados y/o enviados/recibidos (por ejemplo, interfaces con otros sistemas / aplicaciones) correctamente en las aplicaciones. La operación no se ejecuta completamente (ha sido interrumpida).
40116	Inexactitud del cálculo
	El resultado obtenido tras la ejecución de la operación por el sistema de aplicación no es el deseado por el área usuaria.
40117	Errores de funcionamiento por mantenimiento inadecuado de la aplicación
	La aplicación/aplicaciones que soportan la ejecución de la operación no se mantienen cumpliendo con el modelo de control definido en el macroproceso de soporte "Ciclo Productivo de las Aplicaciones"

402 fallos en la implantación de sistemas

40201	desviación en coste de TI sobre lo presupuestado
40202	necesidades de inversión en TI no cubiertas por falta de presupuesto

	40203	ineficiencia en el control y seguimiento de los proyectos de TI
	40204	necesidades de TI demandadas por negocio no valoradas o atendidas con la celeridad requerida
	40205	incapacidad en la medición del la calidad ofrecida por el servicio de TI
	40206	definición de metodología que no está alineada con estándares internacionales o de la organización o no existencia de la misma
	40207	ineficiencia en la medición del la calidad ofrecida por el servicio de TI
	40208	desarrollo de software de aplicación que no soporte de manera efectiva los requerimientos del negocio o la normativa interna
	40209	Dificultad de mantenimiento de aplicaciones por no utilizar metodología en el desarrollo de las mismas.
	40210	Deficiente funcionamiento de las aplicaciones por errores en el diseño, construcción e implementación de las mismas
	40211	incorrecto funcionamiento de la tecnología (HW, Comunicaciones, SW Base, SW de seguridad)
	40212	falta de disponibilidad de la tecnología
	40213	pérdida de integridad de los datos
	40214	interrupciones en el servicio tras la realización de un cambio, consecuencia del incumplimiento o falta de procedimientos de control de cambios
	40215	el servicio de gestión de cambios no alineada con las necesidades de negocio. (la propia función de gestión de cambios no se adecua a los requerimientos de negocio, frecuencia de subidas,....)
	40216	alteraciones de información no deseadas en las aplicaciones tras la realización de un cambio, consecuencia del incumplimiento o falta de procedimientos de control de cambios
	40217	imposibilidad de medir y/o repercutir costes de TI al área de negocio
	40218	inadecuada imputaciones de costes de TI
	40219	uso inapropiado de la tecnología por parte de los usuarios a causa de una deficiente formación
	40220	inadecuado control de las versiones del sw base y de aplicación
	40221	incapacidad de regresar al punto de verificación despues de una modificación
	40222	uso de sw no autorizado en PC´s
	40223	entrada de datos no confiables a los sistemas de información
	40224	salida de datos no confiables de los sistemas de información
	40225	dificultad de mantenimiento de la tecnología por no utilizar procedimientos
403	fallos de hardware	
	40301	el nivel de servicio ofrecido por el hardware no cubre las expectativas de negocio por indefinición del mismo
	40302	incapacidad en la medición del nivel de servicio ofrecido por el hardware (indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
	40303	ineficiencia en la medición del nivel de servicio ofrecido por el hardware(indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
	40304	degradación del rendimiento y la capacidad de los recursos hardware
	40305	incumplimiento de los niveles de servicio hardware definido respecto a la cantidad y calidad del servicio ofertado
	40306	dimensionamiento de los recursos hardware no alineado con las necesidades reales
	40307	problemas e incidentes hardware recurrentes y/o no resueltos
404	arquitectura de sistemas inadecuada	
	40401	tecnología de información no alineada con los requerimientos de negocio
	40402	modelo de arquitectura de información inconsistente con las necesidades de negocio de la Organización
	40403	Incapacidad de adecuación y/o evolución de la infraestructura tecnológica ante nuevas necesidades
	40404	definición de la plataforma tecnológica que no cubra las necesidades de negocio
	40405	selección de soluciones tecnológicas que no soporten de manera efectiva los requerimientos de negocio o la normativa interna
	40406	Selección de soluciones Tecnológicas no homologados por la organización o incumpliendo la normativa interna
405	fallos en las comunicaciones y redes	
	40501	el nivel de servicio ofrecido por los sistemas de comunicaciones no cubre las expectativas de negocio por indefinición del mismo

40502	incapacidad en la medición del nivel de servicio ofrecido por el sistema de comunicaciones (indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
40503	ineficiencia en la medición del nivel de servicio ofrecido por los sistemas de comunicaciones (indicadores utilizados no significativos o indefinidos o no tengo herramientas de medición)
40504	degradación del rendimiento y la capacidad de los recursos de redes de comunicaciones
40505	incumplimiento de los niveles de servicio de las comunicaciones definidos respecto a la cantidad y calidad del servicio ofertado
40506	dimensionamiento de los recursos de redes de comunicaciones no alineado con las necesidades reales
40507	problemas e incidentes en las comunicaciones TI recurrentes y/o no resueltos
406 ausencia o deficiencia de planes de continuidad de sistemas	
40601	imposibilidad de garantizar la continuidad del servicio de TI ante una contingencia
407 deficiencia en los sistemas de seguridad informática	
40701	ausencia parcial o total de definición de los niveles de seguridad aplicables de los datos
40702	ausencia parcial o total de definición de los niveles de seguridad aplicables a la tecnología
40703	degradación de la seguridad del sistema de información
40704	imposibilidad de conocer la actividad realizada en el entorno de producción durante la administración de cambios
40705	parametrización de herramientas de seguridad que no garantiza el nivel de seguridad requerido
40706	falta de protección sobre los recursos a securizar por deficiente administración de seguridad
40707	ataques lógicos intrusivos a los sistemas de información
40708	acceso lógico indebido a los sistemas de información
40709	acceso y/o manipulación indebido a la información
40710	imposibilidad de recuperación de datos
40711	acceso físico no autorizado a las instalaciones donde se ubican los sistemas de información
40712	problemas e incidentes de seguridad recurrentes y/o no resueltos
40713	repudio
40714	ataques a terceros haciendo uso de aplicaciones de BBVA

50 RRHH

Riesgo asociado a la gestión de Recursos Humanos. Incluye todo lo relativo a incumplimientos de la normativa laboral y otras actuaciones que originen sanciones, multas, indemnizaciones, etc., relacionadas con la actividad laboral. Costes relacionados con eventuales demandas por incumplimientos laborales, políticas de selección y contratación, prácticas discriminatorias, multas e indemnizaciones satisfechas como consecuencia del incumplimiento de las condiciones de Seguridad e Higiene en el trabajo, etc.

501 gestión de recursos humanos

Pérdidas ocasionadas por litigios relacionados con las fórmulas de contratación y retribución utilizadas, contingencias derivadas de procesos de negociación sindical, etc.

50101	**deficiencias en la contratación de RRHH**
	Pérdidas originadas a cuasa de una deficiente gestión de cobertura de vacantes.
50102	**deficiencias en la política de retención de RRHH**
	Quebrantos ocasionados por la fuga de talento, conocimiento y experiencia o relacionados con la rotación inadecuada de plantilla, etc.
50103	**huelgas**
	Quebrantos ocasionados a causa de huelgas sectoriales y de empresa.
50104	**despidos improcedentes**
	Indemnizaciones pagadas por este motivo.
50105	**admisión forzosa de personal externo**
	Pérdidas originadas por la admisión forzosa de personal externo subcontratado.
50106	**retribución y beneficios sociales**
	Riesgos relacionados con la aplicación de criterios retributivos, compensación, bonus, errores de administración o de gestión de fondos de pensiones, etc.
50107	**carencia de planes de formación**
	Riesgos asociados a deficiencias en los planes de formación de la plantilla.
50108	**dependencia de recursos críticos**
50109	**dependencia de personal subcontratado/temporal**
50110	**gestión inadecuada de prejubilaciones**

502 incumplimiento normativa laboral

Multas y sanciones impuestas por las autoridades laborales relacionadas con el incumplimiento de las normas de Seguridad e Higiene en el trabajo.

50201	**incumplimiento normativa laboral**
	Multas y sanciones.

503 discriminación, acoso

Riesgo de indemnizaciones y sanciones relacionadas con la discriminación laboral.

50301	**difamación e invasión de la intimidad**
	Pérdidas como consecuencia de la divulgación, oral o escrita, de información que daña la reputación de una persona o de la la invasión ilegal de la intimidad de las personas.
50302	**discriminación**
	Pérdidas resultado de la discriminación (no respeto del principio de igualdad de oportunidades) por razón de la edad, estado civil, género, situación médica, filiación política, raza, creencias religiosas, orientación sexual, etc.
50303	**acoso personal, acoso moral, etc..**
	Verbal, físico, sexual, etc.

60 PRACTICAS COMERCIALES

En este grupo se integran "las riesgos derivados del incumplimiento involuntario o negligente de una obligación profesional frente a *clientes concretos* (incluidos requisitos fiduciarios y de adecuación) o de la naturaleza o diseño de un producto".

Esta categoría es complementaria de la denominada "10. Procesos". En general, recogerá todas las pérdidas originadas por sanciones, indemnizaciones y gastos ocasionados por:

- Litigios por infracciones de la normativa vigente y del marco jurídico existente.
- Reclamaciones de clientes que hayan sufrido un quebranto económico o se consideren perjudicados por la acción u omisión de la entidad en la comercialización de productos o servicios.

601 política comercial

En este apartado se integrarán los eventos que no pueden ser clasificados en el resto de los grupos de esta categoría.
En particular, se incluirán todos los eventos generados por reclamaciones de clientes en relación con el proceso de comercialización de productos o servicios por parte de algún componente individual de la fuerza de ventas.

60101	admisión inadecuada de cliente
	Pérdidas por sanciones y reclamaciones originadas por inadecuada admisión de clientes.
60102	publicidad engañosa
	Pérdidas por sanciones y reclamaciones originadas por publicidad engañosa o deficiencias en los mensajes comerciales.
60103	ventas agresivas
	Pérdidas por reclamaciones originadas por la información facilitada al cliente que tienen por objeto la persuasión de la bondad de determinados productos.
60104	relaciones con los medios de información
	Pérdidas por sanciones y reclamaciones originadas por información facilitada a los medios de comunicación.
60105	Discriminación del cliente
	Pérdidas por reclamaciones y sanciones originadas por acciones discriminatorias en la admisión de clientes.
60106	incumplimiento normativa del Banco de España sobre el blanqueo de capitales
	Pérdidas por sanciones y reclamaciones originadas por actividades relacionadas con el blanqueo de capitales.

602 asesoramiento deficiente a cliente

Dentro de este apartado se clasificará cualquier indemnización satisfecha a clientes como resultado del riesgo de pérdidas provocadas por recomendaciones erróneas y asesoramientos deficientes.

En particular, se incluirán en este apartado los riesgos de pérdidas originadas por la actividad de asesoramiento prestada, así como otras pérdidas originadas por reclamaciones de clientes perjudicados por las recomendaciones realizadas por la entidad en servicios tales como la tramitación de testamentarías, asesoramiento fiscal, etc...

60201	fallos en asesoría a clientes
	Riesgo de pérdidas por indemnizaciones y sanciones, etc., resultado de litigios por la diferente interpretación de las actividades de asesoría prestadas.

603 productos defectuosos

Riesgo de pérdidas ocasionadas por sanciones y penalizaciones a consecuencia de:
- La comercialización de productos sin la preceptiva autorización o las debidas a
- Reclamaciones de clientes perjudicados por la utilización de modelos de valoración erróneos, sistemas de análisis de riesgo defectuosos, etc. se incluirán dentro de esta subcategoría.

60301	diseño inadecuado de producto
	Pérdidas por indemnizaciones, sanciones o compensaciones como consecuencia del diseño inadecuado del producto en la aplicación de modelos de riesgos, políticas de precios...
60302	insuficiencia de medios de soporte
	Pérdidas por indemnizaciones a clientes como consecuencia de defectos en la implantación de nuevos productos a causa de la insuficiencia de medios para la correcta gestión de los mismos, etc.
60303	desconocimiento del producto por parte de los comerciales

Pérdidas ocasionadas en la comercialización de productos y servicios como consecuencia de la falta de conocimiento de los productos por parte de la fuerza de ventas.

6004 prácticas comerciales impropias

Pertenecen a este grupo todos los riesgos de pérdidas (multas, sanciones, indemnizaciones y gastos) originadas por infracciones de la regulación vigente.
En particular, se incluirán dentro de este grupo los eventos relacionados con:

- Prácticas ajenas a la competencia
- Utilización de **información privilegiada** en beneficio de la entidad;
- Comisión de actividades ilícitas en relación con actividades de blanqueo de dinero, evasión de capitales, etc.
- **Política de ventas agresivas**

60401	**incumplimiento normativa de la competencia**
	Multas y sanciones relacionadas con el Tribunal de Defensa de la Competencia y similares, participaciones societarias, fijación de precios, etc.
60402	**discriminación por precios, importes, etc...**
	Multas y sanciones originadas por la aplicación de políticas discriminatorias en la comercialización de productos y servicios o en la aplicación de la política de precios de los mismos.
60403	**dumping**
	Sanciones por aplicación irregular de precios en los productos de activo y pasivo.
60404	**sobreprecios**
	Pérdidas por denuncias originadas por la aplicación de tarifas abusivas, netamente superiores a las de mercado en: seguros, servicios, etc.
60405	**sobornos y comisiones ocultas**
	Pérdidas por multas, sanciones y compensaciones, resultado de pagos realizados para generar o retener negocio.
60406	**blanqueo de capitales**
	Sanciones por actividades de blanqueo llevadas a cabo tanto por personal interno como terceras personas.
60407	**venta engañosa**
	Pérdidas ocasionadas por la política de ventas implantada en orden a facilitar información parcial de los productos, ocultación de riesgos asociados, etc.

6005 transgresión de instrucciones de clientes

Formarán parte de este grupo todos los eventos cuyo riesgo de pérdidas hayan sido ocasionadas por reclamaciones de clientes que consideran se ha hecho un uso inadecuado de los poderes otorgados a la entidad en la gestión discrecional de patrimonios, en el cumplimiento de las restricciones o límites impuestos en la gestión fiduciaria y en la investigación previa necesaria para la realización de inversiones.

60501	**incumplimiento de perfiles/límites fijados por el cliente**
	Pérdidas por multas, sanciones e indemnizaciones como consecuencia del incumplimiento de las directrices y límites prefijados por el cliente.

70 DESASTRES

Incluye todos los riesgos de pérdidas originadas por daños sufridos en activos materiales de la entidad, excepto aquellos cuya causa determinante sea la de obtener un beneficio ilícito en cuyo caso se clasificarán como "Fraude interno" o "Fraude externo". Ejemplo: desperfectos ocasionados en robos, atracos, etc.

701 desastres y accidentes

Riesgo de pérdidas por acontecimientos externos, tanto naturales y accidentales (Incendios, inundaciones, rayos, terremotos, explosiones, etc.) como provocados (actos terroristas, sabotajes, guerras, tumultos, etc), que originen daños en activos físicos o la interrupción de la actividad de la empresa.

70101	interrupción de la actividad
	Pérdidas ocasionadas por la interrupción de la actividad comercial y servicios en general.
70102	daños en inmuebles
	Quebrantos vinculados a la pérdida de bienes inmuebles.
70103	daños en instalaciones, equipamiento, etc...
	Otras pérdidas relacionadas con el resto de los activos físicos.
70104	daños en vehículos
	Pérdidas ocasionadas por los siniestros que afecten a la flota de vehículos de la entidad para uso propio o en la actividad de renting.
70105	accidentes y daños personales
	Otros quebrantos relacionados con el efecto del desastre sobre las personas vinculadas a la entidad.
70106	ausencia o deficiencia de planes de contingencia
	Pérdidas adicionales que pueden producirse de no contar con planes de contingencia adecuados.
70107	carencias en la protección de documentación vital

80 PROVEEDORES

Con frecuencia, la realización de una parte de los procesos de la Entidad se subcontratan con empresas de servicios.
Cualquier interrupción o deficiencia en la actividad de un proveedor que tenga consecuencias negativas en la calidad de los servicios prestados o afecte al correcto funcionamiento de los procesos de la entidad se clasificará en la subcategoría **"101. Errores en la operativa"** o en cualquier otra categoría que pudiera corresponder en aplicación de los criterios de clasificación descritos.

En este grupo se clasificarán, exclusivamente, los eventos que ocasionen puedan ocasionar pérdidas derivadas de **litigios mantenidos con proveedores y distribuidores** en general.

801 proveedores

80101	**deficiencias en el servicio**
	Pérdidas imputables a deficiencias en los servicios del proveedor, que contractualmente pueden ser repercutidas a éste y que, a causa de la insolvencia, quiebra, suspensión de pagos u otros motivos deben ser asumidas por la entidad.
80102	**incumplimiento de contrato**
	Pérdidas vinculadas al incumplimiento de cualesquiera otras obligaciones contractuales por parte del proveedor.
80103	**corte de suministros**
	Otros quebrantos derivados de interrupciones del servicio del proveedor
80104	**dependencia excesiva de determinados proveedores**
	Otros riesgos relacionados con la eventual concentración de actividades o servicios estratégicos en uno o varios proveedores, que puedan poner en peligro la prestación del servicio en las condiciones previamente establecidas.

90 OTROS TIPOS DE RIESGOS

Los riesgos asociados a equivocaciones en la toma de una decisión no se consideran riesgos operacionales, salvo en el caso en que esta decisión pueda afectar directamente a los estados financieros.

901 otros tipos de riesgos

Existe un riesgo que hace referencia a las posibles equivocaciones que una persona puede tener (y que puedan afectar al Reporting Financiero), por el hecho de tomar una decisión.

90101	**Errores en la toma de decisión**
	Errores ocasionados por la inadecuada emisión de una opinión, juicio o interpretación y que puede llegar a tener o generar errores en los estados financieros de forma directa, es decir, en general aquellas circunstancias en las que se requiere un juicio por parte del empleado y este se puede llegar a equivocarse, afectando este error a la contabilidad.